ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería Eléctrica y Computación

"Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002 para el Área de Hardware en la Empresa Uniplex Systems S.A. en Guayaquil"

INFORME DE PROYECTO DE GRADUACION

Previo la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentada por:

Erick Abraham Lamilla Rubio

José Roberto Patiño Sánchez

GUAYAQUIL – ECUADOR

AÑO: 2009

A G R A D E C I M I E N T O

A todas aquellas personas que siempre han creído en nuestra fuerza de voluntad y carácter y a las cuales esperamos nunca defraudar. Gracias por su invaluable apoyo.

D E D I C A T O R I A

A mí querida Mami Melly
A mis Padres

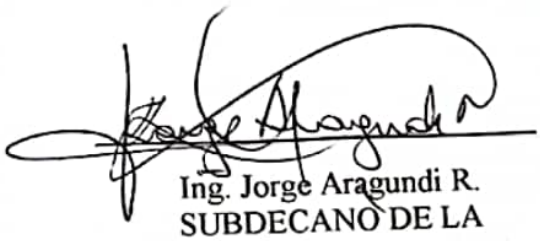
Erick Lamilla Rubio

D E D I C A T O R I A

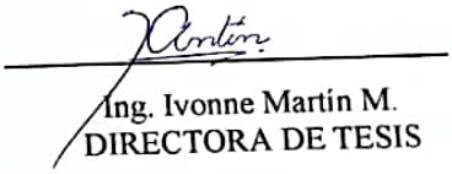
A todas las personas que me apoyaron
A mis Padres

José Patiño Sánchez

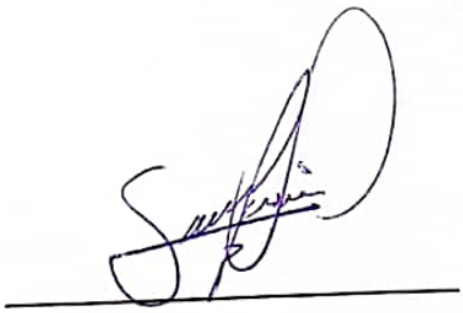
TRIBUNAL DE GRADUACIÓN



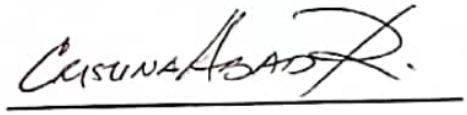
Ing. Jorge Aragundi R.
SUBDECANO DE LA FIEC
PRESIDENTE



Ing. Ivonne Martín M.
DIRECTORA DE TESIS



Ing. Gómer Rubio R.
VOCAL



Ing. Cristina Abad R.
VOCAL

D E D I C A T O R I A

A todas las personas que me apoyaron
A mis Padres

José Patiño Sánchez

TRIBUNAL DE GRADUACIÓN

Ing. Jorge Aragundi R.
SUBDECANO DE LA FIEC
PRESIDENTE

Ing. Ivonne Martín M.
DIRECTORA DE TESIS

Ing. Gomer Rubio R.
VOCAL

Ing. Cristina Abad R.
VOCAL

DECLARACIÓN EXPRESA

“La responsabilidad del contenido de esta Tesis de Grado, nos corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL”

(Reglamento de Graduación de la ESPOL).

Erick Abraham Lamilla Rubio

José Roberto Patiño Sánchez

RESUMEN

Uniplex Systems S.A. es una empresa cuya política de calidad es brindar soluciones corporativas de tecnología de información que potencien su productividad apoyándonos en personal idóneo y en la mejora continua de nuestros procesos asegurando así una relación de negocios a largo plazo y de mutuo beneficio con el cliente.

Se establecerá la importancia de implementar políticas que aseguren la integridad de la información en la empresa Uniplex Systems S.A. en Guayaquil

Se creará un sumario que involucre los pasos para aplicar la seguridad en la empresa Uniplex Systems S.A. en Guayaquil

Se realizará una auditoría para determinar las fortalezas y debilidades de la empresa Uniplex Guayaquil referente a las políticas de seguridad de Informática.

Se establecerá procesos y procedimientos de seguridad que incorporan una serie de medidas sobre los activos de información de la facultad, conociendo, asumiendo y gestionando los posibles riesgos de forma documentada, estructurada, eficiente y adaptable a futuros cambios.

Se implementará los dominios: Políticas de Seguridad, Organización de la Información, Gestión de activos y Control de Acceso de la norma 27002 para el Área de Hardware en base a los objetivos de control y controles aplicables en la empresa Uniplex Systems S.A. en Guayaquil.

En el presente proyecto de titulación se pretende dar una adecuada solución de seguridad a la empresa Uniplex Systems S.A. en Guayaquil., tomando como base estándares internacionales.

Se desea proporcionar lineamientos básicos de la seguridad de la información, gestión de riesgos y diferentes alternativas para el tratamiento de los mismos, la implementación de la norma 27002.

Se presentará un plan de tratamiento de riesgos en donde se identificarán las acciones apropiadas así como los responsables para minimizar los riesgos

identificados para posteriormente realizar la implementación del Proyecto de Gestión de Seguridad de la Información (PGSI) en base a los controles seleccionados y finalmente obtener como resultado el manual de procedimientos para la implementación del PGSI.

Para la implementación del sistema nos basaremos única y exclusivamente en la norma de seguridad de la información ISO-27002

Un Proyecto de Gestión de la seguridad de la Información (PGSI) es, como el nombre lo sugiere, un sistema de administración encargado de la información de la seguridad.

El concepto clave de un PGSI es para una organización del diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la seguridad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

En la actualidad la empresa Uniplex Systems S.A. en Guayaquil cuenta con políticas de seguridad informática de alta vulnerabilidad con respecto al resguardo de la información, por lo que es nuestra intención el mejorar y

restablecer dichas políticas siguiendo una norma estándar de seguridad como es la ISO – 27002.

La problemática se encuentra en la existencia de recursos de información compartidos por el personal administrativo de la empresa, muchos de los cuales necesitan de alta disponibilidad, confidencialidad e integridad. La posible violación de acceso indebido a estos recursos de información tanto por personas propias o extrañas a la empresa debería estar contemplada en un plan de prevención y corrección consistente que evite dichos accesos manteniendo así el flujo normal y continuo de la información.

A través del análisis de las necesidades de la empresa Uniplex Systems S.A. en este proyecto de tesis se solucionarán los siguientes problemas:

- Existencia de un manual de procedimientos para la implementación de un PGSI
- Falta de un plan de tratamiento de riesgos
- Falta de selección de controles acorde con el Manuel de procedimientos para la seguridad informática de la empresa

Justificamos este proyecto de tesis a continuación:

- En la actualidad, la información ya no se encuentra concentrada solo en libros, sino que se encuentra distribuida en diversos medios y formas: en digital, en impresos, en cintas, en casetes, en video, etc., por ello es de trascendental importancia implementar procedimientos para salvaguardar y preservar la información dentro de una empresa.

- Es un hecho que la mayoría de gente posee una pequeña noción acerca de la seguridad de la información y sus ventajas, sin embargo gran cantidad de personas no conocen cual es el primer paso a dar para tener unas políticas verdaderamente consolidadas.

- Se considera al desarrollo de las políticas de seguridad de la información como una pauta para que la empresa este acorde con las regulaciones legales y técnicas del entorno, consolidándose entre las más grandes del mercado.

- Mucha información es vulnerable; puede experimentar distorsión por gente no autorizada, perderse debido a fallas en elementos físicos, afectarle un virus informático, etc. Las políticas de seguridad de la información mantienen la integridad, confidencialidad y disponibilidad de la información previniendo así este tipo de vulnerabilidades y corrigiéndolas en caso de ser necesario.

- La experiencia que se adquiere en el proceso de implementación del sistema representa un beneficio tanto para los que componemos el grupo elaborador del proyecto como para los participantes externos del mismo.

- Algunas Políticas de Seguridad Informática solamente quedan plasmadas en un documento y no son aplicadas, por eso se implementará un plan piloto que involucre cuatro dominios de la Norma 27002, para el Área de Hardware en base a los objetivos de control y controles aplicables en la empresa Uniplex Systems S.A. en Guayaquil.

ÍNDICE GENERAL

CAPITULO 2

CAPITULO 3

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo pretende desarrollar Políticas de Seguridad Informática e implementar un Plan Piloto que involucre cuatro dominios de la Norma 27002 en el Área de Hardware para coadyuvar al crecimiento y progreso de la empresa Uniplex Systems S.A. en Guayaquil.

Tenemos bien en claro que nuestro trabajo será el definir de una manera clara y concisa los aspectos que involucran una correcta seguridad de la información así como el especificar los motivos primordiales por los cuales es necesario implementar Políticas de seguridad de la información en la empresa Uniplex Systems S.A. en Guayaquil

Determinaremos el procedimiento para corregir e instaurar políticas para la seguridad de la información en la empresa identificando las falencias y fortalezas de las políticas de seguridad de la información que están vigentes actualmente en la empresa Uniplex Systems S.A. en Guayaquil

Finalmente se implementará un Plan Piloto que involucre los cuatro dominios de la norma 27002: Políticas de seguridad, Organización de la Información, Gestión de Activos y Control de acceso para el Área de Hardware en esta empresa.

CAPITULO 1

1. INTRODUCCIÓN Y NORMAS ISO PARA LA SEGURIDAD DE LA INFORMACIÓN

Si bien es cierto, el implantar una política de seguridad en una red empresarial requiere un estudio minucioso para no olvidar la revisión de ningún tipo de gestión ya sea tecnológica como administrativa dentro de la red; pero establecer dichas políticas conlleva al desarrollo de las organizaciones de la capacidad para afrontar ataques de cualquier tipo.

1.1 Conceptos Generales de la seguridad de la Información

La principal importancia en la Seguridad de la información radica en la protección de la organización con respecto a amenazas, daños provocados por agentes internos y externos, así como también el resguardo de la información; activo de principal importancia y base fundamental para la elaboración del sistema.

A continuación se detalla los principales aspectos a proteger en un sistema de seguridad de información, los cuales serán el fundamento de protección:

a) Privacidad: Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidas o transmitidas a otros.

b) Seguridad: Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.

El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

c) Integridad: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

d) Datos: Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), video (secuencia de tramas), etc.

e) Base de Datos: Una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que además, están almacenados con criterios independientes de los programas que los utilizan.

También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System-DBMS).

Las características que presenta un DBMS son las siguientes:

- Brinda seguridad e integridad a los datos.
- Provee lenguajes de consulta (interactivo).
- Provee una manera de introducir y editar datos en forma interactiva.
- Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.

f) Acceso: Es la recuperación o grabación de datos que han sido almacenados en un sistema de computa

ción. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.

g) Ataque: Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

h) Ataque activo: Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.

i) Ataque pasivo: Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

j) Amenaza: Cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

k) Incidente: Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

l) Golpe (breach): Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

m) Confidencialidad: acceso a la información por parte únicamente de quienes están autorizados.

n) Disponibilidad: acceso a la información y sus activos asociados por parte de los usuarios autorizados cuando lo requieran.

1.2. Gestión de Riesgos

El proceso de Gestión de Riesgos es una de las piezas más importantes en un Sistema de Gestión de Información, pues conlleva a la coordinación de las actividades para dirigir y controlar una organización en torno al riesgo de seguridad de la misma[1].

En el proceso de Gestión de Riesgos se deberá tomar un método exhaustivo para lograr con éxito la seguridad de la información; requiriendo así la identificación de las vulnerabilidades y amenazas más comunes a las cuales la empresa u organización está sujeta, a la cuantificación del daño potencial que podría existir frente a dichas amenazas y el desarrollo de pasos y procedimientos de mitigación para lograr un nivel de riesgo tolerable.

Definición de Riesgo

El riesgo es todo aquello que puede ser utilizado con fines malintencionados para causar perjuicios a los usuarios en la empresa u organización, el riesgo puede ser tomado como la posibilidad de que se produzca un impacto determinado, ya sea en un Activo, en un Dominio o en toda la Organización.[2] Dicho impacto combina la probabilidad de que ocurra un evento negativo con cuánto daño podría causar este evento.

[1] Tomado del *ISO Guide 73:2002*
[2] Tomado del Wikipedia Enciclopedia Libre

Fuentes de Riesgo

Hay distintas fuentes las cuales pueden tener un impacto en la organización. Una fuente es llamada amenaza. La amenaza nace en el cambio de las condiciones del sistema, por lo que los profesionales de la seguridad realizan compensaciones para lograr un nivel aceptable de riesgo sin comprometer la disponibilidad, confidencialidad e integridad de los datos. Un programa de gestión de riesgos eficaz ofrece a los altos ejecutivos una forma de gestionar la evolución de los sistemas de seguridad de la información.

Pueden ser amenazas los diversos tipos de ataque a la organización así como fallas en los dispositivos externos de almacenamiento de información o su mal uso y administración.

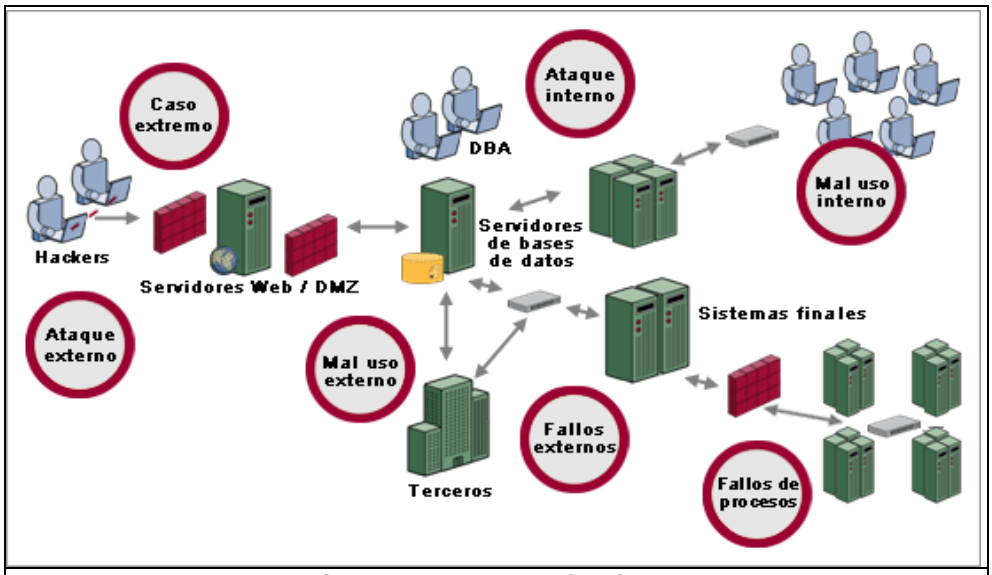


Figura 1.1: Fuentes de Riesgo

Análisis de Riesgos

La implementación de un Sistema de Gestión de Seguridad de Información de acuerdo con la norma ISO 27000 requiere determinar en nivel estándar en la empresa, y en función de dicho nivel se identifica todos los activos de información. Luego de este paso se procede a realizar un análisis de riesgo usando las herramientas de supervisión de la red para identificar los puntos o vulnerabilidades de los ataques técnicos ayudando así a identificar los problemas técnicos en los activos que se encuentran bajo riesgo. Sin embargo, las personas y los procesos pueden comprometer los controles técnicos por medio de un uso indebido accidental o intencionado, poniendo en riesgo la información y las redes.

El objetivo del análisis del riesgo es apreciar dichas magnitudes de riesgo que afecta a los activos de la información. “Se deben tomar decisiones en relación a que riesgos la organización aceptará y qué controles serán implantados para mitigar el riesgo”[3]. La norma ISO 27001:2005 como sistema dinámico obliga a la gerencia a estar constantemente revisando y definiendo controles, sus amenazas, vulnerabilidades e iniciar acciones correctivas y preventivas cuando sea necesario.

[3]Tomado del documento “Análisis del Riesgo y el Sistema de Gestión de Seguridad de la Información. El enfoque ISO 27001:2005” (Alberts. Dorofee) 2003)

Proceso de Evaluación del Riesgo

A continuación se mostrará un proceso de evaluación del riesgo cumpliendo con el estándar ISO27002:

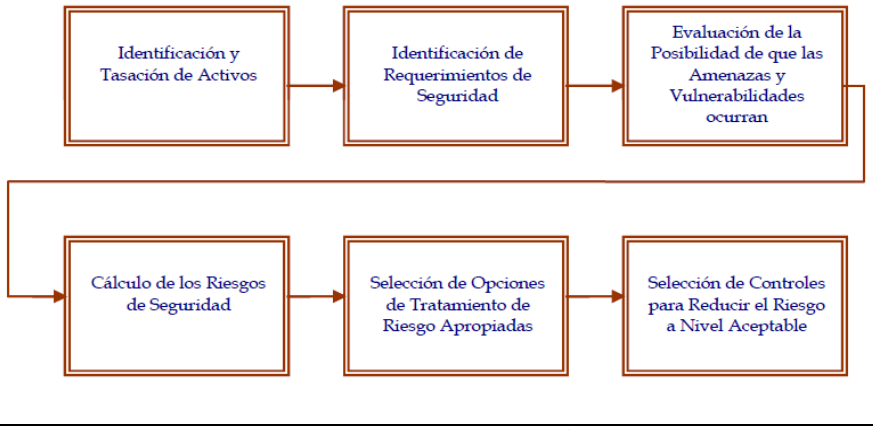
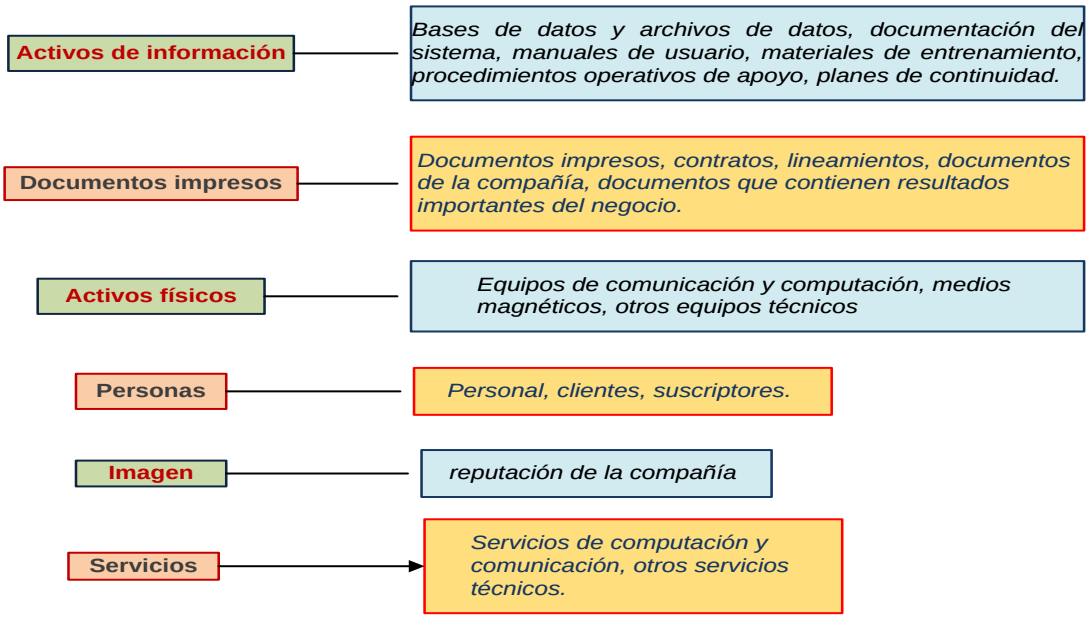


Figura 1.2: Proceso de evaluación de riesgos

En los cuales podemos definir en los siguientes procesos:

Identificación y tasación de activos: Cada activo debe estar claramente identificado y valorado apropiadamente, y su propietario y clasificación de seguridad acordada en la organización. El ISO 17799:2005 (Código de Práctica para la Gestión de la Seguridad de Información) clasifica los activos de la siguiente manera:



Identificación de requerimientos de seguridad: Con el objetivo de identificar los requisitos de seguridad de la organización, es aconsejable basarse en las tres fuentes principales, que se describen a continuación:

*a) La primera fuente es derivada de la **valoración de riesgos** de la organización. Con ella se identifica las amenazas a los activos, se evalúa las vulnerabilidades y la probabilidad de su ocurrencia.*

*b) La segunda fuente es el conjunto de **requisitos legales, estatutos, regulaciones y contratos** que debería satisfaces la organización, sus socios comerciales, los contratistas y los proveedores de servicios.*

*c) La tercera fuente está formada por los **principios, objetivos y requisitos** que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.*

Identificación de amenazas y vulnerabilidades: Las vulnerabilidades son debilidades asociadas con los activos de la empresa.

Las debilidades pueden ser explotadas por las amenazas, causando incidentes no deseados, que pudieran terminar causando pérdidas, daño o deterioro a los activos. La vulnerabilidad como tal, no causa daño, es simplemente una condición o conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.

Cálculo de los riesgos de seguridad: El propósito de la evaluación del riesgo es el de identificar y evaluar los riesgos.
La evaluación de riesgo es una consideración consecuente:

a) ***Consecuencias***.- del impacto económico que probablemente resulte de un fallo de seguridad, teniendo en cuenta las posibles consecuencias de pérdida de confidencialidad, integridad o disponibilidad de la información y otros activos;

b) ***Probabilidad***.- la probabilidad realista de que ocurra dicho fallo a la luz de las amenazas y vulnerabilidades existentes, así como de los controles implantados.

Los resultados de esta evaluación ayudarán a dirigir y determinar una adecuada acción gerencial y las prioridades para gestionar los riesgos de seguridad de la información, y la implantación de los controles adecuados para protegerse contra dichos riesgos. El proceso de evaluación de riesgos y selección de controles, pueden requerir que sea realizado varias veces para cubrir partes diferentes de la organización o sistemas de información individuales.

Es importante, efectuar revisiones periódicas de los riesgos de seguridad y de los controles implantados para:

- Tener en cuenta los cambios de los requisitos y las prioridades de negocio de la organización.
- Considerar nuevas amenazas y vulnerabilidades.
- Confirmar que las medidas de control siguen siendo eficaces y apropiadas.

Selección de Opciones para el Tratamiento del Riesgo

Si recurrimos a la ISO27002, vemos cómo, si hemos seleccionado una estrategia de reducción de riesgos para todos aquellos que en el análisis superan el umbral aceptado, tenemos que seleccionar los controles más apropiados para reducir todos esos riesgos excesivos identificados.

Una vez que disponemos del listado de controles a aplicar, tendremos que articularlos. Se deberá definir los proyectos de implementación correspondientes, especificando tareas, responsables, tiempos y recursos. Dichos parámetros constituirán el Plan de Tratamiento de Riesgo (PTR).
Para el tratamiento del riesgo existen cuatro estrategias:

Reducción del Riesgo

Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente identificados por la empresa.

Al identificar los controles a ser implantados es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como las vulnerabilidades y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- *Reduciendo la posibilidad de que la vulnerabilidad sea explotada por las amenazas.*
- *Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionando o recuperándose de ellos.*

La elección de cualquiera de estas maneras para controlar los riesgos dependerá de una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la firma requiere operar.

Un aspecto muy importante que se debe tomar en cuenta si la empresa opta por este método para el tratamiento del riesgo, es el económico.

Aceptación del Riesgo

Es probable que a la empresa se le presente situaciones donde no se pueden encontrar controles ni tampoco es viable diseñarlos o el

costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

En el caso en que la empresa no pueda manejar el riesgo debido al costo de la implantación de los controles y las consecuencias son devastadoras para la empresa, se deben visualizar las opciones de “transferencia del riesgo” o la de “evitar el riesgo”.

Transferencia del Riesgo

La transferencia del riesgo, es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente factible, transferir el riesgo a una aseguradora.

Hay que tomar en cuenta, que con las empresas aseguradoras, siempre existe un elemento de riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales se aplicarán dependiendo del tipo de ocurrencia, bajo la cual no se provee una indemnización. La transferencia del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuánto del riesgo actual está siendo transferido.

Otra posibilidad es la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. En la medida en que la empresa tercializadora esté preparada para asumir dicha responsabilidad.

Lo que debe estar claro, es que al tercerizar servicios, el riesgo residual no se delega, es responsabilidad de la empresa.

Evitar el Riesgo

La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras habituales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información si no se consigue la protección adecuada.

  La decisión por la opción de “evitar el riesgo” debe ser balanceada contra las necesidades financieras y comerciales de la empresa.

Riesgo Residual

Ya realizado el PTR sobre el proyecto u organización, se deberá de reconocer que por más eficiente que sea el PTR, existirá siempre un riesgo residual. El riesgo residual es aquel riesgo que queda en la empresa después de un arduo análisis de seguridad a través de un PTR.

El riesgo residual no tiene proporciones ni estándares; es un estimado que está en función del PTR que lleva la empresa para salvar su información.

Para el caso de un riesgo residual intolerable o peligroso, se debe tomar una decisión a nivel administrativo para resolver la situación. Uno de los procedimientos recomendados es identificar diversas opciones de tratamiento de riesgo, incrementar los controles de sistema de seguridad o establecer arreglos con aseguradoras; esto tiene como finalidad reducir al mínimo el nivel de riesgo.

Se pueden dar dos casos: discriminar los riesgos en su totalidad o aceptarlo en forma forzada. En la práctica se tiende siempre a no tolerar ningún tipo de riesgos y atenuarlos al máximo pero si las circunstancias ameritan aceptar un riesgo residual, este debe ser documentado y aprobado por la gerencia. Si el PTR no es eficaz en alcanzar los niveles de riesgos deseados, se estará obligado a cambiar de PTR o realizar las acciones correctivas correspondientes.

1.3 Controles de un Sistema de Seguridad de la Información

ISO 27001 contiene un anexo A, que considera los controles de la norma ISO 17799 para su posible aplicación en SGSI que implante cada organización.

La descripción de cada uno de los controles y dominios se verá en el capítulo II del presente proyecto de titulación.

1.4 Estructura del Sistema de Gestión

El Sistema de Gestión forma parte del conjunto de mecanismos dedicados al control y direccionamiento de cierto ámbito.

En una empresa el número de Sistemas de Gestión usadas como herramienta de seguridad no es fijo, se puede implementar un sinnúmero de sistemas de gestión siempre que estos estén dirigidos hacia la mejora de la organización sin imponer carga a la misma.

Objetivo

Los Sistemas de Gestión tienen como objetivo aplicarse en el marco de todas las actividades que se ejecutan en la organización, no solo en la parte tecnológica de la misma o a nivel informático como es el objetivo de este proyecto de titulación y son válidos solo si cada uno de estos sistemas interactúa con los demás armónicamente.

En la implementación del sistema de gestión en una empresa es necesario contar la documentación que describa y respalde el diseño y el comportamiento de las prácticas

empresariales, pues esta sirve de eje para alcanzar el nivel competitivo y eficiente que requiere la empresa en el manejo de la información.

Para obtener un sistema de gestión sólido con características maleables de acuerdo a la situación a la que se desea coordinar y controlar dentro de la organización se deben considerar como elementos apropiados para su estructuración los siguientes:

Operatividad de los Sistemas de Gestión

Para adaptarse a una organización en particular, los sistemas de gestión deben operar con los siguientes objetivos:

- ✓ *Ser escueto para la comprensión de todos los protagonistas*
- ✓ *Operar eficientemente*
- ✓ *Satisfacer mediante resultados las expectativas proyectadas*
- ✓ *Enfatizar las acciones preventivas ante cualquier clase de problema*

1.5 Normas ISO 27000

Historia

Durante más de un siglo, el Instituto Británico de Normas Técnicas (BSI) y la Organización Internacional de Normas Técnicas (ISO) han brindado parámetros

globales a 3las normas técnicas de operación, fabricación y desempeño. Solo faltaba que BSI e ISO propusieran una norma técnica para la seguridad de la información.

En 1995, el BSI publicó la primera norma técnica de seguridad; la BS 7799, la cual fue redactada con el fin de abarcar los asuntos de seguridad relacionados con el e – commerce. La Norma se consideraba inflexible y no tuvo gran acogida. No se presentó la norma técnica en un momento oportuno y los problemas de seguridad no despertaron mucho interés en ese entonces.

En Mayo de 1999, el BSI intentó de nuevo publicar su segunda versión de la Norma BS 7799, la que fue una revisión más amplia de la primera publicación.

En Diciembre del 2000, La ISO adoptó y publicó la primera parte de su norma BS 7799 bajo el nombre de ISO 17799.

En Septiembre del 2002 se publicó BS 7799 – 2; en esta revisión se adoptó el "Modelo de Proceso" con el fin de alinearla con ISO 9001 e ISO 14001.

El 15 de Octubre del 2005 se aprueba la Norma ISO 27001:2005 y en 2006 existen más de 2030 compañías certificadas a nivel mundial.

La Serie 27000

La norma ISO 27000 difiere en el resto de normas pues esta es una recopilación de estándares. Su numeración se reservó para todas aquellas normas relacionadas con los sistemas de gestión de seguridad de la información. Los rangos de numeración

reservados por ISO van de 27000 a 27019 y de 27030 a 27044. La serie de estándares 27000 pueden ser mencionados de la siguiente manera:

ISO 27000 (términos y definiciones): Contiene todo el vocabulario perfecta y concisamente definido para toda la serie 27000. Su objetivo es evitar las distintas interpretaciones entre los conceptos técnicos y de gestión.

ISO 27001 (requerimientos de un SGSI): Es la norma principal de las serie y contiene los requisitos del sistema de gestión de seguridad de la información.

ISO 27002 (objetivos de control y controles): Corresponde a una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Esta norma no es certificable. Contiene 39 objetivos de control y 133 controles agrupados en 11 dominios.

ISO 27003 (guía de implantación de un SGSI): Constituye otra guía de implementación de Seguridad de Información pero esta vez orientada al uso del PDCA y de sus requerimientos.

ISO 27004 (métricas y técnicas de medida de la efectividad de un SGSI):Se especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados.

ISO 27005 (guía para la gestión del riesgo de seguridad de la información): Establece las directrices para la gestión del riesgo en la seguridad de la información, apoyando los conceptos generales de la norma 27001. Su diseño está enfocado a la aplicación satisfactoria de la seguridad de la información en la gestión de riesgos.

ISO 27006 (proceso de acreditación de entidades de certificación y el registro de PGSI's): Esta norma tiene la finalidad de interpretar los criterios de acreditación de las diferentes normas ISO cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma.

Beneficios de las Normas ISO 27000

Las normas ISO 27000 tienen como principales beneficios:

a) Establecimiento de una metodología de gestión de la seguridad de forma clara y concisa, con una estructura sólida.
b) Reducción del riesgo de pérdida, hurto o mal uso de la información.
c) Establecimiento de medidas de seguridad en el acceso de clientes.
d) Continuidad en la revisión de riesgos y sus controles.
e) Confidencialidad comercial y garantía de calidad entre clientes y socios estratégicos.
f) Identificación de debilidades del sistema y áreas póstumas a mejorar a través de auditoría externas.
g) Posibilidad de integración con otros sistemas ISO de gestión.
h) Continuidad con las operaciones necesarias de negocio tras incidentes graves a gran escala.
i) Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
j) Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.6 Términos y Definiciones

La siguiente terminología se encuentra contenida en esta norma:

Activo (Asset).- en relación con la seguridad de información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Aceptación de Riesgos.- Decisión de aceptar un riesgo.

Análisis de Riesgo.- Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Administración del Riesgo.- Actividades coordinadas para dirigir y controlar las medidas necesarias para la observación del riesgo dentro de la organización.

Confidencialidad (Confidenciality).- Acceso a la información por parte únicamente de quienes estén autorizados.

Disponibilidad (Avalaibility).- Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Declaración de Aplicabilidad.- documento que enumera los controles aplicados por el Proyecto de Gestión de Seguridad de la Información de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos, además de la justificación tanto de su selección como de la exclusión de controles incluidos en el ANEXO A.

Evaluación de riesgos.- Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Incidente de Seguridad.- Evento único o serie de eventos de seguridad de la información inesperada o no deseada que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de información.

Integridad.- Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Riesgo Residual.- el riesgo que permanece tras el tratamiento de riesgos.

Seguridad de la Información.- Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio y fiabilidad pueden ser también consideradas.

Eventos de Seguridad de la Información.- suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardias, o una situación anterior o desconocida que podría ser relevante para la seguridad.

Tratamiento de Riesgo.- Proceso de selección e implementación de medidas para modificar el riesgo.

Valoración de Riesgos.- Proceso Completo de análisis y evaluación de riesgos.

Control.- Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica de gestión o legal.

Directriz.- Descripción que aclara lo que se debería hacer y como hacerlo, para alcanzar los objetivos establecidos en las políticas. (NTC 5411-1:2006)

Servicios de procesamiento de información.- Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

Política.- Toda intención y directriz expresada formalmente por la dirección.

Gestión del riesgo.- Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (ISO/IEC Guía 73:2002)

Tercera parte.- Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión. (ISO/IEC Guía 2:1996)

Vulnerabilidad.- Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas. (NTC 5411-1:2006)

1.7 Proyecto de Gestión de Seguridad de la Información (PGSI)

Norma ISO 27002

Contenido de la Norma ISO 27002

El contenido de la norma ISO 27002 se puede resumir como sigue a continuación:

Introducción: conceptos generales de seguridad de la información y PGSI.

Campo de aplicación: se especifica el objetivo de la norma.

Términos y definiciones: breve descripción de los términos más usados en la norma.

Estructura del estándar: descripción de la estructura de la norma.

Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

Política de seguridad: documento de política de seguridad y su gestión.

Aspectos organizativos de la seguridad de la información: organización interna; terceros.

Gestión de activos: responsabilidad sobre los activos; clasificación de la información.

Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

Seguridad física y ambiental: áreas seguras; seguridad de los equipos.

Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.

Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.

Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

Bibliografía: normas y publicaciones de referencia.

Objetivo de la Norma ISO 27002

Entre los objetivos de la norma se puede mencionar los siguientes:

a) ***Consolidación del control en la seguridad de la información:*** Aquí la implementación de un PGSI es necesaria para potenciar el servicio de seguridad.

b) ***Potenciar un servicio final:*** Aquí la implantación de un PGSI va correlacionado a los servicios o procesos de negocio. Irá enfocado a una capa de seguridad adicional.

c) ***Refuerzo de procesos internos:*** Aquí la implantación de un PGSI se enfoca al fortalecimiento servicios y procesos internos, generalmente de tipo técnico, responsables del tratamiento y conservación de la información de la empresa; áreas de diseño y recursos humanos.

d) ***Potenciar la gestión interna:*** Aquí la implementación de un PGSI se enfoca a identificar y preservar la estructuración de gestión interna. Es muy probable que este punto es el más difícil de analizar pues existen

multitud de sistemas de gestión centrados en distintos aspectos y puede ser que el de las seguridad pueda no ser el más indicado en todos los casos, pero en determinadas situaciones puede ser una importante opción.

Requisitos de la Documentación de un PGSI

Un Proyecto de Gestión de la Seguridad de la Información basado en ISO 27001 está formado por una serie de documentos que pueden clasificarse en una pirámide de cuatro niveles:

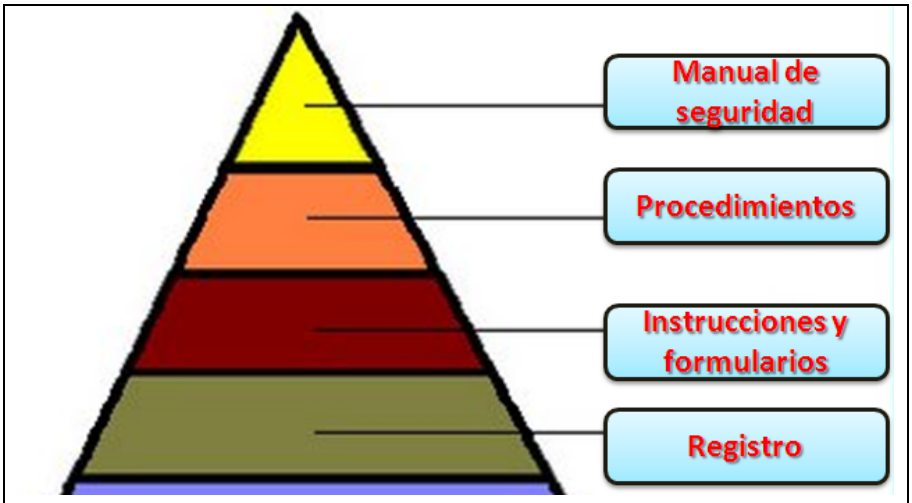


Fig. 1.3: Pirámide de cuatro niveles que diferencian la clasificación de documentos

La documentación de un PGSI deberá incluir:

Documentos de Nivel 1

Forman el manual de seguridad. Son los siguientes:

Alcance del PGSI: ámbito de la organización que queda sometido al PGSI. Se debe incluir una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas, prestando especial atención en aquellos casos en los que el ámbito de influencia del PGSI considere una parte menor de la organización como delegaciones, divisiones, áreas, procesos o tareas concretas.

Política y objetivos de seguridad: documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Metodología de evaluación de riesgos: descripción de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.

Informe de evaluación de riesgos: estudio resultante de aplicar la metodología de evaluación anteriormente mencionada.

Plan de tratamiento del riesgo: documento que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información e implantar los controles necesarios para proteger la misma.

Declaración de aplicabilidad (SOA -Statement of Applicability-, en sus siglas inglesas): documento que contiene los objetivos de

control y los controles contemplados por el PGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Procedimientos relativos al nivel 1: procedimientos que regulan cómo se realizan, gestionan y mantienen los documentos enumerados en el nivel 1.

Documentos de Nivel 2

Procedimientos: documentos que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo medir la efectividad de los controles.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4.

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del PGSI; están asociados a

documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

Control de Documentos

Todos los documentos requeridos por el PGSI serán protegidos y controlados.

Un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- ✓ Aprobar documentos y prioridades o clasificación de empleo.
- ✓ Revisiones, actualizaciones y reaprobaciones de documentos.
- ✓ Asegurar que los cambios y las revisiones de documentos sean identificados.
- ✓ Asegurar que las últimas versiones de los documentos aplicables estén disponibles y listas para ser usadas.
- ✓ Asegurar que los documentos permanezcan legibles y fácilmente identificables.
- ✓ Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- ✓ Asegurar que los documentos de origen externo sean identificados.
- ✓ Asegurar el control de la distribución de documentos.
- ✓ Prevenir el empleo no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que queden almacenados para cualquier propósito.

Responsabilidades de Administración

La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de:

- Establecimiento de la política del PGSI
- Asegurar el establecimiento de los objetivos y planes del PGSI.
- Establecer roles y responsabilidades para la seguridad de la información.
- Comunicar y concienciar a la organización sobre la importancia y apoyo necesario a los objetivos propuestos por la política de seguridad, sus responsabilidades legales y la necesidad de una continua mejora en este aspecto.
- Proveer suficientes recursos para establecer, operar, implementar, monitorizar, revisar, mantener y mejorar el SGSI.
- Decidir los criterios de aceptación de riesgos y los niveles del mismo.
- Asegurar que las auditorías internas del PGSI, sean conducidas y a su vez conduzcan a la administración para la revisión del SGSI.
- Formación, preparación y competencia:

  La organización asegurará que todo el personal a quien sean asignadas responsabilidades definidas en el SGSI sea competente y esté en capacidad de ejecutar las tareas requeridas, para ello deberá proveer las herramientas y capacitación necesaria (Documento: Planificación, guías y programas de formación y preparación).

Implementación de un PGSI

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27002, se utiliza el ciclo continuo PDCA; tradicional en los sistemas de gestión de la calidad.

A continuación se describen los pasos a seguir para la implementación del PGSI:

Plan (Establecer es PGSI)

- Definir el alcance del PGSI en términos del negocio.
- Definir una política de seguridad
- Definir una metodología de evaluación del riesgo apropiada para el PGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y unos criterios de aceptación de los riesgos.
- Identificar los riesgos
- Analizar y evaluar los riesgos
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos
- Seleccionar los objetivos de control y los controles del Anexo A de la norma ISO 27002 para el tratamiento del riesgo y que cumplan con los requerimientos identificados en el proceso de evaluación y tratamiento del riesgo
- Definir una declaración de aplicabilidad

Do (Implementar y Utilizar el PGSI)

- Definir un plan de tratamiento de riesgos
- Implantar el plan de tratamiento de riesgos
- Implementar los controles
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles seleccionados.
- Procurar programas de formación y concienciación en relación a la seguridad de la información dirigidos a todo el personal.
- Gestionar las operaciones del PGSI.
- Gestionar los recursos necesarios asignados al PGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check (Monitorear y Revisar el PGSI)

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión
- Revisar regularmente la efectividad del PGSI
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables

- Realizar periódicamente auditorías internas del PGSI en intervalos planificados.
- Revisar el PGSI por parte de la dirección
- Actualizar los planes de seguridad
- Registrar acciones y eventos

Act (Mantener y Mejora el PGSI)

La organización deberá regularmente:

- Implantar en el PGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de la norma ISO 27001.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

CAPITULO 2

2. DESCRIPCIÓN DE LOS 11 DOMINIOS DEL ESTÁNDAR ISO 27002

Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos indicados en esta norma brindan una guía general sobre las metas aceptadas comúnmente para la gestión de la seguridad de la información.

Los objetivos de control y los controles de esta norma están destinados a ser implementados para satisfacer los requisitos identificados por la evaluación de riesgos. Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

Esta norma contiene once secciones sobre controles de seguridad que en conjunto tienen un total de 39 categorías principales de seguridad y una sección de introducción a la evaluación y el tratamiento del riesgo.

Cada cláusula contiene una cantidad de categorías principales de seguridad. Estas once cláusulas (acompañadas por la cantidad de categorías principales de seguridad incluida en cada numeral) son:

a) Política de seguridad (1)

b) *Organización de la seguridad de la información (2)*

c) *Gestión de activos (2)*

d) *Seguridad de los recursos humanos (3)*

e) *Seguridad física y del entorno (2)*

f) *Gestión de operaciones y comunicaciones (10)*

g) *Control de acceso (7)*

h) *Adquisición, desarrollo y mantenimiento de sistemas de información (6)*

i) *Gestión de los incidentes de seguridad de la información (2)*

j) *Gestión de la continuidad del negocio (1)*

k) *Cumplimiento (3)*

2.1. Políticas de Seguridad

Política de Seguridad de la Información

Objetivo: brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

Las directivas deberían establecer una dirección clara de la política según los objetivos del negocio y demostrar apoyo y compromiso con la seguridad de la información a través de la emisión y el mantenimiento de la política de seguridad de la información en toda la organización.

Documentación de la Política de Seguridad de la Información

Control

La dirección debería aprobar un documento de política de seguridad de la información y lo debería publicar y comunicar a todos los empleados y partes externas pertinentes.

Guía de implementación

El documento de la política de seguridad de la información debería declarar el compromiso de la dirección y establecer el enfoque de está para la gestión de la seguridad de la información. El documento de la política debería contener declaraciones relacionadas con:

- Definición de la seguridad de la información, sus objetivos generales y el alcance e importancia de la seguridad como mecanismo que permite compartir la información (véase la introducción);

- Declaración de la intención de la dirección, que apoye las metas y los principios de seguridad de la información, de acuerdo con la estrategia y los objetivos del negocio;

- Estructura para establecer los objetivos de control y los controles, incluyendo la estructura de la evaluación de riesgos y de la gestión del riesgo;

- Explicación breve sobre las normas, las políticas y los principios de seguridad, así como de los requisitos de cumplimiento de importancia particular para la organización incluyendo los siguientes:

  Cumplimiento de los requisitos legales, reglamentarios y contractuales;

  Requisitos de educación, formación y concientización sobre seguridad;

  Gestión de la continuidad del negocio;

  Consecuencias de las violaciones de la política de seguridad;

  Definición de las responsabilidades generales y específicas para la gestión de la seguridad de la información, incluyendo el reporte de los incidentes de seguridad de la información;

  Referencias a la documentación que puede dar soporte a la política, tal como las políticas de seguridad más detalladas para sistemas específicos de información o las reglas de seguridad que deberían cumplir los usuarios.

  Esta política de seguridad de la información se debería comunicar a través de toda la organización a los usuarios de manera pertinente, accesible y comprensible para el lector.

  Información adicional

  La política de seguridad de la información podría formar parte de un documento de política general. Si la política de seguridad de la información se distribuye fuera de la organización, es necesario tener cuidado de no divulgar información sensible. Información adicional se puede encontrar en la NTC 5411-1:2006.

Revisión de la Política de Seguridad de la Información

Control

La política de seguridad de la información se debería revisar a intervalos planificados o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.

Guía de implementación

La política de seguridad de la información debería tener un dueño con responsabilidad aprobada por la dirección para el desarrollo, la revisión y la valoración de dicha política. Es conveniente que la revisión incluya las oportunidades de evaluación para mejorar la política de seguridad de la información de la organización y el enfoque para la gestión de la seguridad de la información en respuesta a los cambios en el entorno de la organización, las circunstancias del negocio, las condiciones legales o el entorno técnico.

Es conveniente que la revisión de la política de seguridad de la información tenga en cuenta los resultados de la revisión por la dirección. Deberían existir procedimientos definidos para la revisión por la dirección, incluyendo una programación o periodo de revisión.

Las entradas para la revisión por la dirección deberían incluir información sobre:

Retroalimentación de las partes interesadas;

Resultados de las revisiones independientes

Estados de las acciones preventivas y correctivas;

Resultados de las revisiones previas por parte de la dirección;

Desempeño del proceso y cumplimiento de la política de seguridad de la información;

Cambios que pudieran afectar el enfoque de la organización para la gestión de la seguridad de la información, incluyendo cambios en el entorno de la organización, las circunstancias del negocio, la disponibilidad de recursos, las condiciones contractuales, reglamentarias o legales, o el entorno técnico;

Tendencias relacionadas con las amenazas y las vulnerabilidades;

Incidentes de seguridad de la información reportados

Recomendaciones de las autoridades pertinentes

Los resultados de la revisión por la dirección deberían incluir todas las decisiones y acciones relacionadas con:

Mejora del enfoque de la organización para la gestión de la seguridad de la información y sus procesos;

Mejora de los objetivos de control y de los controles;

Mejora de la asignación de recursos y/o responsabilidades;

Es recomendable mantener un registro de la revisión por la dirección;

Se debería obtener la aprobación de la dirección para la política revisada.

2.2 Organización de la Seguridad de la Información

Organización Interna

Objetivo: gestionar la seguridad de la información dentro de la organización.

Se debería establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La dirección debería aprobar la política de seguridad de la información, asignar las funciones de seguridad, coordinar y revisar la implementación de la seguridad en toda la organización.

Si es necesario, se recomienda establecer una fuente de asesoría especializada sobre seguridad de la información y ponerla a disposición en la organización. Es conveniente desarrollar contactos con grupos o especialistas externos en seguridad, incluyendo las autoridades pertinentes, para ir al compás de las tendencias industriales, monitorear normas y métodos de evaluación, así como proveer puntos adecuados de vínculo cuando se manejan incidentes de seguridad de la información. Se debería promover un enfoque multidisciplinario para la seguridad de la información.

Compromiso de la Dirección con la Seguridad de la Información

Control

La dirección debería apoyar activamente la seguridad dentro de la organización con un rumbo claro, un compromiso demostrado, una asignación explicita y el conocimiento de las responsabilidades de la seguridad de la información.

Guía de Implementación

La dirección debería:

- asegurar que las metas de la seguridad de la información están identificadas, satisfacen los requisitos de la organización y están integradas en los procesos pertinentes;

- formular, revisar y aprobar la política de seguridad de la información;
- revisar la eficacia de la implementación de la política de seguridad de la información;
- proporcionar un rumbo claro y apoyo visible para las iniciativas de seguridad;
- Proporcionar los recursos necesarios para la seguridad de la información;
- Aprobar la asignación de funciones y responsabilidades específicas para la seguridad de la información en toda la organización;
- Iniciar planes y programas para mantener la concientización sobre la seguridad de la información;
- Asegurar la coordinación e toda la organización de la implementación de los controles de seguridad de la información.
- La dirección debería identificar las necesidades de asesoría especializada interna o externa sobre la seguridad de la información, revisar y coordinar los resultados de la asesoría en toda la organización.
- Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor o a través de un organismo de dirección ya existente, como por ejemplo el consejo directivo.
- Información adicional
- La NTC 5411-1:2006, contiene información adicional.

Coordinación de la Seguridad de la Información

Control

Las actividades de la seguridad de la información deberían ser coordinadas por los representantes de todas las partes de la organización con roles y funciones laborales pertinentes.

Guía de implementación

Comúnmente, la coordinación de la seguridad de la información involucra la cooperación y colaboración de directores, usuarios, administradores, diseñadores de aplicación, auditores y personal de seguridad, así como habilidades especializadas en áreas como seguros, temas legales, recursos humanos, tecnología de la información o gestión de riesgos.

Esta actividad debería:

a) *garantizar que las actividades de seguridades efectúan en cumplimiento de la política de seguridad de la información;*
b) *identificar la forma de manejar los incumplimientos;*
c) *aprobar metodologías y procesos para la seguridad de la información, como la evaluación de riesgos y la clasificación de información;*
d) *identificar cambios significativos en las amenazas y la exposición de la información y de los servicios de procesamiento de la información a las amenazas;*
e) *evaluar la idoneidad y coordinar la implementación de los controles de seguridad de la información;*

f) promover eficazmente la educación, la formación y la concientización de la seguridad de la información en toda la organización;

g) *valorar la información recibida del monitoreo y la revisión de los incidentes de seguridad de la información en toda la organización.*

Si la organización no emplea grupos con funciones separadas por ejemplo debido a que dichos grupos no son apropiados para el tamaño de la organización, las acciones descritas anteriormente las debería llevar a cabo otro organismo de la dirección o un solo director.

Asignación de Responsabilidad para la Seguridad de la Información

Control

Se deberían definir claramente todas las responsabilidades en cuanto a seguridad de la información.

Guía de implementación

La asignación de responsabilidades para la seguridad de la información se debería realizar de acuerdo con la política de seguridad de la información (véase el numeral 5). Se recomienda definir claramente las responsabilidades para la protección de activos individuales y para la ejecución de procesos específicos de

seguridad. Esta responsabilidad debería complementarse, cuando es necesario, con directrices más detalladas para sitios específicos y servicios específicos de procesamiento de información. Se deberían definir claramente las responsabilidades locales para la protección de activos y para realizar procesos específicos de seguridad, como por ejemplo la planificación de la continuidad del negocio.

Los individuos con responsabilidades de seguridad asignadas pueden delegar las labores de seguridad a otros. No obstante, siguen siendo responsables y deberían determinar la ejecución correcta de las labores delegadas.
Las áreas por las cuales son responsables los individuos se deberían establecer con claridad, en particular, se deberían establecer las siguientes:

a) los activos y los procesos de seguridad asociados con cada sistema particular se deberían identificar y definir claramente;

b) se debería asignar la entidad responsable de cada activo o proceso de seguridad, así como documentar esta responsabilidad (véase también el numeral 7.1.2);

c) se deberían definir y documentar claramente los niveles de autorización.

Información adicional

En muchas organizaciones se designará un director de seguridad de la información con toda la responsabilidad por el desarrollo e implementación de la seguridad y para apoyar la identificación de controles.

Sin embargo, la responsabilidad por los recursos y la implementación de controles permanecerá en los directores individuales. Una práctica comunes designar un dueño para cada activo, quien se hace responsable de su protección diaria.

Proceso de Autorización para los Servicios de Procesamiento de Información

Control

Se debería definir e implementar un proceso de autorización de la dirección para nuevos servicios de procesamiento de información.

Guía de implementación

Se recomienda tener en cuenta las siguientes directrices para el proceso de autorización:

a) *los servicios nuevos deberían tener autorización de la dirección para el usuario apropiado, autorizando su propósito y uso. La autorización también se debería obtener del director responsable de mantener el entorno de seguridad del sistema de información local para asegurar el cumplimiento de todas las políticas y los requisitos de seguridad correspondientes;*
b) *cuando es necesario, el hardware y el software se deberían verificar para asegurar que son compatibles con otros componentes del sistema;*
c) *la utilización de servicios de procesamiento de información personales o privados, por ejemplo computadores portátiles (laptops), computadores domésticos o*

dispositivos manuales para procesar información del negocio, pueden introducir nuevas vulnerabilidades y se deberían identificar e implementar los controles necesarios.

Acuerdos sobre Confidencialidad

Control

Se deberían identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.

Guía de implementación

Los acuerdos de confidencialidad o de no-divulgación deberían abordar los requisitos para proteger la información confidencial usando términos que se puedan hacer cumplir legalmente.

Para identificar los requisitos para los acuerdos de confidencialidad o de no-divulgación, se deberían considerar los siguientes elementos:

a) *definición de la información que se ha de proteger (por ejemplo la información confidencial);*
b) *duración esperada del acuerdo, incluyendo los casos en que se puede ser necesario mantener la confidencialidad indefinidamente;*
c) *acciones requeridas cuando se termina un acuerdo;*

d) *responsabilidades y acciones de los que suscriben el acuerdo de confidencialidad para evitar la divulgación no autorizada de información (tal como "necesidad de conocer");*
e) *propiedad de la información, secretos comerciales y propiedad intelectual y cómo se relaciona con la protección de información confidencial;*
f) *el uso permitido de la información confidencial y los derechos de los que suscriben el acuerdo de confidencialidad a usar la información;*
g) *derecho de auditar y monitorear las actividades que involucran a la información confidencial;*
h) *Proceso para la notificación y el reporte de divulgación no autorizada o violación de la información confidencial;*
i) *Términos para la devolución o la destrucción de la información al terminar el acuerdo;*
j) *Acciones esperadas a tomar en caso de incumplimiento de este acuerdo.*

Con base en los requisitos de seguridad de la organización, pueden ser necesarios otros elementos en un acuerdo de confidencialidad o no-divulgación.

Los acuerdos de confidencialidad o no-divulgación se deberían revisar periódicamente y cuando se produzcan cambios que influyan en estos requisitos.

Información adicional

Los acuerdos de confidencialidad y de no-divulgación protegen la información de la organización e informan a los que suscriben el acuerdo de confidencialidad, sus

responsabilidades para proteger, utilizar y divulgar información de forma responsable y autorizada.

Puede ser necesario que una organización utilice diferentes formas de acuerdos de confidencialidad y de no-divulgación en circunstancias diferentes.

Contacto con las Autoridades

Control

Se deberían mantener contactos apropiados con las autoridades pertinentes.

Guía de implementación

Las organizaciones deberían tener procedimientos establecidos que especifiquen cuándo y a través de que autoridades (policía, bomberos, autoridades de supervisión) se deberían contactar y la forma en que se deberían reportar oportunamente los incidentes identificados de la seguridad de la información, si se sospecha de incumplimiento de la ley.

Puede que las organizaciones sometidas a ataques provenientes de Internet necesiten terceras partes externas (por ejemplo un proveedor de servicios de Internet o un operador de telecomunicaciones) para tomar acción contra la fuente de los ataques.

Información adicional

El mantenimiento de dichos contactos puede ser un requisito para dar soporte a la gestión de incidentes de seguridad de la información (véase el numeral 13.2) o a la continuidad del negocio y el proceso de planes de contingencia (véase la sección 14). Los contactos con los organismos de regulación también son útiles para anticipar y preparar los cambios futuros en la ley o en los reglamentos que la organización debe cumplir. Los contactos con otras autoridades incluyen servicios públicos, servicios de emergencia, salud y seguridad, como el departamento de bomberos (en conexión con la continuidad del negocio), proveedores de telecomunicaciones (junto con enrutamiento de línea y disponibilidad) y proveedores de agua (junto con medios de refrigeración para los equipos).

Contacto con Grupos de Interés Especiales

Control

Se deberían mantener los contactos apropiados con grupos de interés especiales, otros foros especializados en seguridad de la información, y asociaciones de profesionales.

Guía de implementación

La pertenencia a foros o grupos de interés especial se debería considerar un medio para:

a) *Mejorar el conocimiento sobre las mejores prácticas y estar actualizado con la información pertinente a la seguridad;*
b) *Garantizar que la comprensión del entorno de seguridad de la información es actual y completa;*
c) *Recibir advertencia oportunas de alertas, avisos y parches relacionados con taques y vulnerabilidades;*
d) *Obtener acceso a asesoría especializada sobre seguridad de la información;*
e) *Compartir e intercambiar información acerca de nuevas tecnologías, productos amenazas o vulnerabilidades;*
f) *Suministrar puntos adecuados de enlace cuando se trata de incidentes de seguridad de la información (véase el numeral 13.2.1).*

Información adicional

Se pueden establecer acuerdos para compartir información con el objetivo de mejorar la cooperación y la coordinación de los temas de seguridad. Dichos acuerdos deberían identificar los requisitos para la protección de la información sensible.

Revisión Independiente de la Seguridad de la Información

Control

El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se deberían revisar

independientemente a intervalos planificados, o cuando cambios significativos en la implementación de la seguridad.

Guía de implementación

La dirección debería poner en marcha la revisión independiente. Esta revisión independiente es necesaria para asegurar la eficacia, idoneidad y propiedad del enfoque de la organización para la gestión de la seguridad de la información. La revisión debería incluir la evaluación de las oportunidades de mejora y la necesidad de cambios en el enfoque de la seguridad, incluyendo la política y los objetivos de control.

Dicha revisión deberá ser realizada por personas independientes del área sometida a revisión, por ejemplo por la función de auditoría interna, un director independiente o una organización de tercera parte especializada en tales revisiones. Los individuos que llevan a cabo estas revisiones deberían tener la experiencia y las habilidades adecuadas.

Se recomienda que los resultados de la revisión independiente se registren y se reporten a la dirección que ha iniciado la revisión. Estos registros se deberían conservar.

Si la revisión identifica que el enfoque y la implementación de la organización con respecto a la gestión del sistema de seguridad son inadecuados o no cumplen la orientación para la seguridad de la información establecida en el documento de la política de la seguridad de la información, la dirección debería considerar las acciones correctivas.

Información adicional

El área que los directores deberían revisar regularmente también se podría revisar independientemente. Las técnicas de revisión pueden incluir entrevistas de la dirección, verificación de registros o revisión de los documentos de la política de seguridad. La norma NTC-ISO 19011:2002, Directrices para la auditoría de los sistemas de gestión ambiental y/o de calidad también puede suministrar una guía útil para llevar a cabo la revisión independiente, incluyendo el establecimiento y la implementación de un programa de revisión.

Partes Externas

Objetivo: mantener la seguridad de la información y de los servicios de procesamiento de información de la organización a los cuales tienen acceso partes externas o que son procesados, comunicados o dirigidos por éstas.

La seguridad de la información y de los servicios de procesamiento de información no se deberían reducir introduciendo productos o servicios de partes externas.

Se debería controlar todo acceso a los servicios de procesamiento de información, así como el procesamiento y comunicación de información por partes externas.

Cuando existe una necesidad del negocio de trabajar con partes externas que pueden requerir acceso a la información de la organización y a sus servicios de procesamiento de información, o de obtener o suministrar productos y servicios de o para una parte

externa, se debería realizar una evaluación de riesgos para determinar las implicaciones para la seguridad y los requisitos de control. Los controles se deberían acordar y definir en un convenio con la parte externa.

Identificación de los Riesgos Relacionados con las Partes Externas

Se deberían identificar los riesgos a la información de la organización y a las instalaciones del procesamiento de información de los procesos de negocio que impliquen a terceros y se deberían implementar controles apropiados antes de conceder el acceso.

Guía de Implementación

Cuando existe la necesidad de permitir el acceso de una gran parte externa a los servicios de procesamiento de información o a la información de la organización, es recomendable llevar a cabo una evaluación de riesgos para identificar los requisitos para controles específicos. En la identificación de los riesgos relacionados con el acceso de partes externas se deberían considerar los siguientes aspectos:

a) *Los servicios de procesamiento de información a los cuales requiere acceso la parte externa;*
b) *El tipo de acceso que tendrá la parte externa a la información y a los servicios de procesamiento de información, por ejemplo:*

    1) *Acceso físico, por ejemplo a oficinas, recintos de computadoras y gabinetes de archivos;*

2) *Acceso lógico, por ejemplo a las bases de datos de la organización o a los sistemas de la organización;*
3) *Conexión de red entre las redes de la organización y de la parte externa por ejemplo conexión permanente, acceso remoto;*
4) *Si el acceso tendrá lugar en las instalaciones o fuera de ellas.*

c) *El valor y la sensibilidad de la información involucrada y su importancia para las operaciones del negocio;*
d) *Los controles necesarios para proteger la información que no está destinada a ser accesible por las partes externas;*
e) *El personal de la parte externa involucrado en manejar la información de la organización;*
f) *La forma en que se puede identificar a la organización o al personal autorizado a tener acceso, la manera de verificar la autorización, así como la forma en que es necesario confirmarlo;*
g) *Los diferentes medios y controles utilizados por la parte externa al almacenar, procesar, comunicar, compartir e intercambiar la información;*
h) *El impacto del acceso denegado a la parte externa cuando lo requiere y la recepción o el acceso de la parte externa a la información inexacta o engañosa;*
i) *Las prácticas y los procedimientos para tratar los incidentes de seguridad de la información y los daños potenciales, al igual que los términos y las condiciones para la continuación del acceso de la parte externa en el caso de un incidente de seguridad de la información;*
j) *Los requisitos legales y reglamentarios y otras obligaciones contractuales pertinentes a la parte externa que se deberían tener en cuenta;*
k) *La forma en que se podrían ver afectados los intereses de cualquier otro accionista debido a los acuerdos.*

El acceso de las partes externas a la información de la organización no se debería brindar hasta haber implementado los controles apropiados y cuando es viable, haber firmado un contrato que defina los términos y las condiciones para la conexión o el acceso y el acuerdo de trabajo. En general, todos los requisitos de seguridad que resultan del trabajo con partes externas, o los controles internos se deberían reflejar en el acuerdo con la parte externa

Información adicional

Las partes externas podrían poner en riesgo la información con una gestión inadecuada de la seguridad. Se deberían identificar y aplicar los controles para administrar el acceso de la parte externa a los servicios de procesamiento de información. Por ejemplo, si existe una necesidad especial de confidencialidad de la información, se podrían utilizar los acuerdos de no-divulgación.

Las organizaciones pueden enfrentar riesgos asociados con procesos, gestión y comunicación entre las organizaciones, si se aplica un alto grado de contratación externa cuando existen varias partes externas involucradas.

Los controles comprenden diferentes acuerdos con partes externas, incluyendo por ejemplo:

A) Proveedores de servicios, como los proveedores de servicios de internet, proveedores de red, servicios telefónicos, servicios de mantenimiento y soporte;

B) Servicios de seguridad dirigidos;

C) Clientes;

D) Contratación externa de servicios y/u operaciones, sistemas de tecnología de la información, servicios de recolección de datos, operaciones de centro de llamadas;

E) Asesores de negocios y gestión, y auditores;

F) Desarrolladores y proveedores, por ejemplo productos de software y sistemas de tecnología de la información;

G) Limpieza, alimentación y otros servicios de soporte contratados externamente;

H) Personal temporal, ubicación de estudiantes y otras asignaciones casuales a corto plazo;

Tales acuerdos pueden ayudar a reducir los riesgos asociados con las partes externas.

Abordaje de la Seguridad Cuando se trata con los Clientes

Control

Todos los requisitos de seguridad identificados se deberían abordar antes de dar acceso a los clientes a los activos o la información de la organización.

Guía de implementación

Los siguientes términos se deberían considerar para abordar la seguridad antes de dar acceso a los clientes a cualquiera de los activos de la organización (dependiendo del tipo y la extensión de dicho acceso, no se podrían aplicar todos ellos):

a) Protección de activos, incluyendo:

1) Procedimientos para proteger los activos de la organización, incluyendo información y software, y gestión de las vulnerabilidades conocidas;

2) *Procedimientos para determinar si alguna vez se ha puesto en peligro los activos, por ejemplo pérdida o modificación de datos;*
3) *Integridad;*
4) *Restricciones a la copia y la divulgación de la información.*

b) *Descripción del producto o servicio que se va proveer;*
c) *Las diversas razones, requisitos y beneficios del acceso del cliente;*
d) *Política de control de acceso, incluyendo:*

1) *Métodos de acceso permitido y control y uso de identificadores únicos todos como la identificación del usuario (ID) y las contraseñas;*
2) *Proceso de autorización para los privilegios y el acceso de los usuarios;*
3) *Declaración de que el acceso que no se autorice explícitamente está prohibido;*
4) *Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas;*

e) *Convenios para el reporte, la notificación y la investigación de las inexactitudes de la información (por ejemplo de detalles personales), incidentes de seguridad de la información y violaciones de la seguridad;*
f) *Descripción de cada servicio que va a estar disponible;*
g) *La meta del nivel de servicio y los niveles inaceptables de servicio;*
h) *El derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización;*
i) *Las respectivas responsabilidades civiles de la organización y del cliente;*
j) *Las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos*

sistemas legales nacionales, si el acuerdo implica cooperación con clientes en otros países

k) *Derechos de propiedad intelectual (DPI) y asignación de derechos de copia) y la protección de cualquier trabajo en colaboración.*

Información adicional

Los requisitos de seguridad relacionada con los clientes que tiene acceso a los activos de la organización pueden variar considerablemente dependiendo de la información y de los servicios de procesamiento de información a los cuales se tiene acceso. Estos requisitos de seguridad se pueden abordar empleando acuerdos con el cliente que contengan todos los riesgos y requisitos de seguridad identificados.

Los acuerdos con las partes externas también pueden involucrar a otras partes. Los acuerdos que otorgan acceso a la parte externa deberían incluir la permisividad para la designación de otras partes y las condiciones elegibles para su acceso y participación.

Abordaje de la Seguridad en los Acuerdos con Terceras Partes

Control

Los acuerdos con terceras partes que implican el acceso, proceso, comunicación o gestión de la información de la organización o de las instalaciones de procesamiento de información o la adición de productos o servicios a las instalaciones, deberían cubrir todos los requisitos de seguridad relevantes.

Guía de implementación

El acuerdo debería garantizar que no existen entendidos entre la organización y la tercera parte. Las organizaciones deberían estar satisfechas en la medida de la indemnización de la tercera parte.

Se recomienda tener en cuenta los siguientes términos para la inclusión en el acuerdo con el objeto de cumpli9r los requisitos de seguridad identificados:

a) La política de seguridad de la información;

b) Los controles para asegurar la protección del activo, incluyendo:

1) Procedimientos para proteger los activos de la organización, incluyendo información, software y hardware;

2) Todos los controles y mecanismos de protección física requeridos;

3) Controles para asegurar la protección contra software malicioso;

4) Procedimientos para determinar si alguna vez se han puesto en peligro los activos, por ejemplo pérdida o modificación de información; software y hardware;

5) Controles para asegurar la devolución o la destrucción de la información y los activos al finalizar el acuerdo o en un punto acordado en el tiempo durante la duración del acuerdo.

6) Confidencialidad, integridad, disponibilidad y cualquier otra propiedad pertinente;

7) Restricciones a la copia y a la divulgación de información, y uso de acuerdos de confidencialidad;

c) La información del usuario y del administrador en métodos, procedimientos y seguridad;

d) Asegurar la concientización del usuario sobre responsabilidades y aspectos de la seguridad de la información;

e) Las disposiciones para la transferencia de personal, cuando es apropiado;

f) Las responsabilidades relacionadas con la instalación y el mantenimiento del software y el hardware;

g) La estructura clara y los formatos acordados para la presentación de los informes;

h) El proceso claro y específico para la gestión de cambios;

i) La política de control de acceso, incluyendo:

1) Diversas razones, requisitos y beneficios de la necesidad del acceso por terceras partes;

2) Métodos de acceso permitido y control y uso de identificadores únicos, tales como las identificaciones de usuario (ID) y las contraseñas;

3) Proceso de autorización para los privilegios y el acceso del usuario;

4) Requisito para mantener una lista de las persona autorizadas a usar los servicios que se ponen a disposición, y de sus derechos y privilegios con relación a tal uso;

5) Declaración de que el acceso que no se autorice explícitamente está prohibido;

6) Proceso para revocar los derechos de acceso o interrumpir la conexión entre los sistemas,

j) *las disposiciones para el reporte, la notificación y la investigación de los incidentes de seguridad de la información y las violaciones de la seguridad, así como los incumplimientos de los requisitos establecidos en el acuerdo;*

k) *la descripción de cada servicio que va a estar disponible y una descripción de la información que va a estar disponible junto con su clasificación de seguridad;*

l) *la meta del nivel de servicio y los niveles inaceptables de servicio;*

m) *la definición de criterios verificables de desempeño, su monitoreo y reporte;*

n) *el derecho a monitorear y revocar cualquier actividad relacionada con los activos de la organización;*

o) *el derecho a auditar las responsabilidades definidas en el acuerdo, a que dichas auditorias sean realizadas por una tercer parte y a enumerar los derechos estatutarios de los auditores;*

p) *el establecimiento de un proceso de escalada para la solución de problemas;*

q) *los requisitos de la continuidad el servicio, incluyendo las medidas para la disponibilidad y confiabilidad, de acuerdo con las prioridades de negocio de la organización;*

r) *las responsabilidades civiles correspondientes de las partes del acuerdo;*

s) *las responsabilidades relacionadas con asuntos legales y la forma en que se garantiza el cumplimiento de los requisitos legales; por ejemplo la legislación sobre protección de datos, teniendo en cuenta particularmente los diversos sistemas legales nacionales, si el acuerdo implica cooperación con organizaciones en otros países;*

t) *los derechos de propiedad intelectual (DPI) y asignación de derechos de copia y la protección de cualquier trabajo en colaboración;*

u) *la participación de la tercera parte con los subcontratistas y los controles de seguridad que estos subcontratistas necesitan implementar ;*

v) *las condiciones para la renegociación / terminación del acuerdo:*

1) *se debería establecer un plan de contingencia en caso de que cualquiera de las partes desee terminar la relación antes del término de los acuerdos;*
2) *renegociación de acuerdos si cambian los requisitos de seguridad de la organización;*
3) *documentación vigente de las listas de activos, licencias, acuerdos o derechos relacionados con ellos.*

Información adicional

Los acuerdos pueden variar considerablemente para diferentes organizaciones y entre los diferentes tipos de terceras partes. Por lo tanto, se debe tener cuidado al incluir todos los riesgos y requisitos de seguridad identificados en los acuerdos. Cuando es necesario, los procedimientos y controles requeridos se pueden ampliar en el plan de gestión de la seguridad.

Si la gestión de la seguridad se contrata externamente, los acuerdos deberían abarcar la forma en que la tercera parte garantizará la seguridad adecuada, tal como lo definió la evaluación de riesgos, cómo mantendrá la seguridad, y cómo se adaptara la seguridad para identificar y tratar los cambios en los riesgos.

Algunas de las diferencias entre la contratación externa y otras formas de prestación de servicios de terceras partes incluyen el tema de la responsabilidad civil, la planificación de periodo de transición y la interrupción potencial de las operaciones durante este periodo acuerdos sobre planificación de contingencias y revisiones con la debida diligencia, así como la recolección y gestión de información sobre incidentes de seguridad. Por ello, es importante que la organización planifique y gestione la transición hacia un acuerdo contratado externamente, tenga procesos adecuados establecidos para la gestión de los cambios y la renegociación y terminación de los acuerdos.

Es necesario considerar en el acuerdo los procedimientos para el procesamiento continuo, en el caso de que la tercera parte no pueda suministrar sus servicios, para evitar cualquier retraso en la disposición de los servicios de reemplazo.

Los acuerdos con las partes externas también pueden involucrar a otras partes. Los acuerdos que otorgan acceso a la tercera parte debería incluir la permisividad para la designación da otras partes y las condiciones elegibles para su acceso y participación.

En general, los acuerdos los desarrolla en primer término la organización. Puede haber ocasiones, en algunas circunstancias, en que una tercera arte pueda desarrollar un acuerdo a imponerlo a la organización. Es necesario que la organización garantice que su propia seguridad no sufre impactos innecesarios debidos a los requisitos de la tercera parte estipulados en los acuerdos impuestos.

2.3 Gestión de Activos

Responsabilidad por los Activos

Objetivo: lograr y mantener la protección adecuada de los activos de la organización.

Todos los activos se deben incluir y deben tener un dueño designado.
Se deberían identificar los dueños para todos los activos y asignar la responsabilidad para el mantenimiento de los controles adecuados. La implementación de los

controles específicos puede ser delegada por el dueño, según el caso, pero él sigue siendo responsable de la protección adecuada de los activos.

Inventario de Activos

Control

Todos los activos deberían estar claramente identificados y se debería elaborar y mantener un inventario de todos los activos importantes.

Guía de implementación

La organización debería identificar todos los activos y documentar su importancia. El inventario de activos debería incluir toda la información necesaria para recuperarse de los desastres, incluyendo el tipo de activo, el formato, la ubicación, la información de soporte, la información sobre licencias y el valor para el negocio. Este inventario no debería duplicar innecesariamente otros inventarios, pero se debería garantizar que el contenido este acorde.

Además, se deberían acordar y documentar la propiedad y la clasificación de la información para cada uno de los activos. Con base en la importancia del activo, su valor para el negocio y su clasificación de seguridad se recomienda identificar los niveles de protección según la importancia de los activos (información adicional sobre la forma de valorar los activos para representar su importancia se puede encontrar en la norma ISO/IEC TR 13335-3).

Información adicional

Existen muchos tipos de activos, incluyendo:

a) *información bases de datos y archivos de datos, contratos y acuerdos, documentación del sistema, información sobre investigación, manuales de usuario, material de formación, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos de recuperación, registros de auditoria e información archivada;*

b) *activos de software: software de aplicación, software del sistema, herramientas de desarrollo y utilidades;*

c) *activos físicos: equipos de computación, equipos de comunicaciones, medios removibles y otros equipos;*

d) *servicios: servicios de computación y comunicaciones, servicios generales como por ejemplo iluminación, calefacción, energía y aire acondicionado;*

e) *personas y sus calificaciones, habilidades y experiencia;*

f) *intangibles tales como reputación e imagen de la organización.*

Los inventarios de activos ayudan a garantizar que se logra la protección eficaz de los activos y también se puede requerir para otros propósitos del negocio como por ejemplo por razones de salud y seguridad, financieras o de seguros (gestión de activos). El proceso para obtener un inventario de activos es un prerrequisito importante de la gestión de riesgos

Propietario de los Activos

Control

Toda la información y los activos asociados con los servicios de procesamiento de información deberían ser “propietario” de una parte designada de la organización.

Guía de implementación

El propietario del activo debería ser responsables de:

a) garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente;

b) definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

La propiedad se pueden asignar a:

1. ***un proceso del negocio;***
2. ***un conjunto definido de actividades;***
3. ***una aplicación;***
4. ***un conjunto definido de datos.***

Información adicional

Las labores rutinarias se pueden delegar, por ejemplo a un custodio que cuide el activo diariamente, pero la responsabilidad sigue siendo del [4]propietario.

---

[4]El término “propietario” identifica a un individuo o una entidad que tiene responsabilidad aprobada de la dirección por el control de la producción, el desarrollo, el mantenimiento, el uso y la seguridad de los activos. El término “propietario” no implica tenga realmente los derechos de propiedad de los activo

En los sistemas complejos de información puede ser útil asignar grupos de activos que actúan juntos para suministrar una función particular como “servicios”. En este

caso, el propietario de servicio es responsable de la entrega de éste, incluyendo el funcionamiento de los activos que lo proporcionan.

Uso Aceptable de los Activos

Control

Se deberían identificar, documentar e implementar las reglas sobre el uso aceptable de la información y de los activos asociados con los servicios de procesamiento de la información.

Guía de implementación

Todos los empleados, contratistas y usuarios por tercera parte deberían seguir las reglas para el uso aceptable de la información, incluyendo:

a) reglas para el uso del correo electrónico y de Internet.

b) *directrices para el uso de los dispositivos móviles, especialmente para su utilización fuera de las instalaciones de la organización.*

El director correspondiente debería suministrar las reglas o directrices específicas. Los empleados, contratistas y usuarios de tercera parte que utilizan o tienen acceso a los activos de la organización deberían estar conscientes de los límites que exciten para el uso de la información y de los activos de la organización asociados con los servicios de procesamiento de información, así como de los recursos. Deberías ser responsable del uso que hagan de los recursos de

procesamiento de información y de cualquier uso efectuado bajo su responsabilidad.

Clasificación de la Información

Objetivo: asegurar que la información recibe el nivel de protección adecuado.

La información se debería clasificar para indicar la necesidad, las prioridades y el grado esperado de protección al manejar la información.

La información tiene diferentes grados de sensibilidad e importancia. Algunos elementos pueden requerir un grado adicional de protección o manejo especial. Se recomienda utilizar un esquema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas especiales de manejo.

Directrices de Clasificación

Control

La información se debería clasificar en términos de su valor, de los requisitos legales, de la sensibilidad y la importancia para la organización.

Guía de implementación

Las clasificaciones y los controles de protección asociados para la información deberían considerar las necesidades del negocio respecto a compartir o restringir la información, al igual que los impactos del negocio asociados con tales necesidades.

Las directrices de clasificación deberían convenciones para la clasificación inicial y la reclasificación con el paso del tiempo, de acuerdo con alguna política predeterminada de control del acceso.

Debería ser responsabilidad del propietario del activo definir la clasificación del activo, revisarlo periódicamente y asegurarse de que se mantiene actualizado y en el nivel adecuado.

Es conveniente considerar la cantidad de categorías de clasificación y los beneficios a obtener con su utilización. Los esquemas demasiado complejos pueden volverse engorrosos y de uso costoso o no ser prácticos. Se debería tener cuidado al interpretar las etiquetas de clasificación en los documentos de otras organizaciones, las cuales pueden tener diferentes definiciones para etiquetas iguales o similares.

Información adicional

El nivel de protección se puede evaluar analizando la confidencialidad, la integridad y la disponibilidad como también otros requisitos para la información en consideración.

Con frecuencia, la información deja de ser sensible o importante después de un periodo de tiempo dado, por ejemplo, cuando la información se hace pública. Se deberían considerar estos aspectos puesto que la súper clasificación puede originar la implementación de controles innecesarios que llevan a un costo adicional.

La consideración de documentos con requisitos de seguridad similares cuando se asignan los niveles de clasificación puede ser útil para simplificar la labor de clasificación.

En términos generales, la clasificación que se da a la información es una manera corta de determinar la forma en que se debe manejar y proteger esta información.

Etiquetado y Manejo de la Información

Control

Se debería desarrollar e implementar un conjunto de procedimientos adecuados para el etiquetado y el manejo de la información de acuerdo al esquema de clasificación adoptado por organización.

Guía de implementación

Es necesario que los procedimientos para el etiquetado de la información comprendan los activos de información en formatos físicos y electrónicos.

Las salidas de los sistemas que contienen información que se clasifica como sensible o critica deberían portar una etiqueta de clasificación adecuada (en la salida). Los elementos a considerar incluyen informes impresos, presentaciones en pantalla, medios grabados (por ejemplo, cintas, discos compactos), mensajes electrónicos y transferencias de archivos.

Para cada nivel de clasificación es recomendable definir los procedimientos de manejo, incluyendo procesamiento, almacenamiento, transmisión, desclasificación y destrucción seguros. Ello debería incluir los procedimientos para la cadena de custodia y el registro de cualquier evento importante de seguridad.

Los acuerdos con otras organizaciones que incluyen compartir información deberían incluir procedimientos para identificar la clasificación de dicha información y para interpretar las etiquetas de clasificación de otras organizaciones.

Información adicional

El etiquetado y el manejo seguro de la información clasificada son un requisito clave de los acuerdos para compartir información. Las etiquetas físicas son una forma común de etiquetado. No obstante, algunos activos de información, tales como los documentos en formato electrónico, no se pueden identificar físicamente y es necesario emplear medios electrónicos de etiquetado. Por ejemplo, el etiquetado de notificación puede aparecer en la pantalla o en la presentación.

Cuando el etiquetado no es viable, se pueden aplicar otros medios para designar la clasificación de la información, por ejemplo a través de procedimientos o meta-datos.

2.4 Seguridad de los Recursos Humanos

Antes de la Contratación Laboral

Objetivo: asegurar que los empleados, contratista y usuarios de terceras partes entienden sus responsabilidades y sean aptos para las funciones para las cuales están considerados, y reducir el riesgo de robo, fraude, o uso inadecuado de las instalaciones.

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral, describiendo adecuadamente el trabajo y los términos y condiciones del mismo.

Todos los candidatos para el empleo, los contratistas y os usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para trabajos sensibles.

Los empleados, contratistas y usuarios de terceras partes de los servicios de procesamiento de información deberían firmar un acuerdo sobre sus funciones y responsabilidades de seguridad.

Roles y responsabilidades

Control

Se deberían definir y documentar los roles y responsabilidades de los empleados, contratistas y usuarios de terceras partes por la seguridad, de acuerdo con la política de seguridad de la información de la organización.

Selección

Control

Se deberían realizar revisiones para la verificación de antecedentes de los candidatos a ser empleados, contratistas o usuarios de terceras partes, de acuerdo con los reglamentos, la ética y las leyes pertinentes, y deben ser proporcionales a los requisitos del negocio, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.

Términos y Condiciones Laborales

Control

Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceras partes deberían estar de acuerdo y firmar los términos y condiciones de su contrato laboral, el cual debe establecer sus responsabilidades y las de la organización con relación a la seguridad de la información.

Durante la Vigencia del Contrato Laboral

Objetivo: asegurar que todos los empleados, contratistas y usuarios de terceras partes estén conscientes de las amenazas y preocupaciones respecto a la seguridad de la información, sus responsabilidades y sus deberes, y que estén equipados para apoyar la política de seguridad de la organización en el transcurso de su trabajo normal, al igual que reducir el riesgo de error humano.

Es conveniente definir las responsabilidades de la dirección para garantizar que se aplica la seguridad durante todo el contracto laboral de una persona dentro de la organización.

Se debería brindar un nivel adecuado de concientización, educación y formación en los procedimientos de seguridad y el uso correcto de los servicios de procesamiento de información a todos los empleados, contratistas y usuarios de terceras partes para minimizar los posibles riesgos de riesgos de seguridad. Es conveniente establecer un proceso disciplinario formal para el manejo de las violaciones de seguridad.

Responsabilidades de la Dirección

Control

La dirección debería exigir que los empleados, contratistas y usuarios de terceras partes apliquen la seguridad según las políticas y los procedimientos establecidos por la organización

Educación, Formación y Concientización Sobre la Seguridad de la Información

Control

Todos los empleados de la organización y, cuando sea pertinente, los contratistas y los usuarios de terceras partes deberían recibir formación adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones laborales.

Proceso Disciplinario

Control

Debería existir un proceso disciplinado formal para los empleados que hayan cometido alguna violación de la seguridad.

Terminación o Cambio de la Contratación Laboral

Objetivo: asegurar que los contratistas y los usuarios de terceras partes salen de la organización o cambian su contrato laboral de forma ordenada.

Se deberían establecer responsabilidades para asegurar la gestión de la salida de los empleados, contratistas o usuarios de terceras partes de la organización y que se completa la devolución de todo el equipo y la cancelación de todos los derechos de acceso.

Responsabilidades en la Terminación

Control

Se deberían definir y asignar claramente las responsabilidades para llevar a cabo la terminación o el cambio de la contratación laboral.

Devolución de Activos

Control

Todos los empleados, contratistas o usuarios de terceras partes deberían devolver todos los activos pertenecientes a la organización que estén en su poder al finalizar su contratación laboral, contrato o acuerdo.

Retiro de los Derechos de Acceso

Control

Los derechos de acceso de todos los empleados, contratistas o usuarios de terceras partes a la información y a los servicios de procesamiento de información se deberían retirar al finalizar su contratación laboral, contrato o acuerdo o se deberían ajustar después del cambio.

2.5 Seguridad Física y del Entorno

Áreas Seguras

Objetivo: evitar el acceso físico no autorizado, el daño o la interferencia a las instalaciones y a la información de la organización.

Los servicios de procesamiento de información sensible o crítica deberían estar ubicados en áreas seguras, protegidas por perímetros de seguridad definidos, con barreras de seguridad y controles de entrada adecuados. Dichas áreas deberían estar protegidas físicamente contra acceso no autorizado, daño e interferencia. La protección suministrada debería estar acorde con los riesgos identificados.

Perímetro de Seguridad Física

Control

Se deberían utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información.

Controles de Acceso Físico

Control

Las áreas seguras deberían estar protegidas con controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.

Seguridad de Oficinas, Recintos e Instalaciones

Control

Se debería diseñar y aplicar la seguridad física oficinas, recintos e instalaciones.

Protección Contra Amenazas Externas y Ambientales

Control

Se deberían diseñar y aplicar protecciones físicas contra daño por incendio, inundación, terremoto, explosión, manifestaciones sociales y otras formas de desastre natural o artificial.

Trabajo en Áreas Seguras

Control

Se deberían diseñar y aplicar la protección física y las directrices para trabajar en áreas seguras.

Áreas de Carga, Despacho y Acceso Público

Control

Los puntos de acceso tales como las áreas de carga y despacho y otros puntos por donde pueda ingresar personal no autorizado a las instalaciones se deberían controlar y, si es posible, aislar de los servicios de procesamiento de información para evitar el acceso no autorizado.

Seguridad de los Equipos

Objetivo: evitar pérdida, daño, robo o puesta en peligro de los activos, y la interrupción de las actividades de la organización.

Los equipos deberían estar protegidos contra amenazas físicas y ambientales.
La protección del equipo (incluyendo el utilizado por fuera, y el retiro de la propiedad) es necesaria para reducir el riesgo de acceso no autorizado a la información y par proteger contra pérdida o daño. También se debería considerar la ubicación y la eliminación de los equipos. Es posible que se requieran controles especiales para la ubicación contra amenazas físicas y para salvaguardar los servicios de soporte tales como energía eléctrica e infraestructura de cableado.

Ubicación y Protección de los Equipos

Control

Los equipos se deberían ubicar de modo tal que se minimice el acceso innecesario a las áreas de trabajo;

Servicios de Suministro

Control

Los equipos se deberán estar protegidos contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.

Seguridad de Cableado

Control

El cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información debería estar protegido contra interceptaciones o daños.

Mantenimiento de los Equipos

Control

Los equipos deberían recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.

Seguridad de los Equipos Fuera de las Instalaciones

Control

Se debería suministrar seguridad para los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.

Seguridad en la Reutilización o Eliminación de los Equipos

Control

Se deberían verificar todos los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación.

Retiro de Activos

Control

Ningún equipo, información ni software se deberían retirar sin autorización previa.

2.6 Gestión de Comunicaciones y Operaciones

Procedimiento Operacionales y Responsabilidades

Objetivo: asegurar la operación correcta y segura de los servicios de procesamiento de información.

Se deberían establecer todas las responsabilidades y los procedimientos para la gestión y operación de todos los servicios de procesamiento de información. Esto incluye e desarrollo de procedimientos operativos apropiados.

Cuando sea conveniente, se debería implementar la separación de funciones para reducir el riesgo de uso inadecuado deliberado o negligente del sistema.

Documentación de los Procedimientos de Operación

Control

Los procedimientos de operación se deberían documentar, mantener y estar disponibles para todos los usuarios que los necesiten.

Gestión del Cambio

Control

Se deberían controlar los cambios en los servicios y los sistemas de procesamiento de información.

Distribución (Segregación) de Funciones

Control

Las funciones y las áreas de responsabilidad se deberían distribuir para reducir las oportunidades de modificación no autorizada o no intencional, o el uso inadecuado de los activos de la organización.

Separación de las Instalaciones de Desarrollo, Ensayo y Operación

Control

Las instalaciones de desarrollo, ensayo y operación deberían estar separadas para reducir los riesgos de acceso o cambios no autorizados en el sistema operativo.

Gestión de la Prestación del Servicio por Terceras Partes

Objetivo: implementar y mantener un grado adecuado de seguridad de la información de la prestación del servicio, de conformidad con los acuerdos de prestación del servicio por terceros,

La organización debería verificar la implementación de acuerdos, monitoreo el cumplimiento de ellos y gestionar los cambios para asegurar que los servicios que se prestan cumplen los requisitos acordados con los terceros.

Prestación del Servicio

Control

Se deberían garantizar que los controles de seguridad, las definiciones del servicio y los niveles de prestación del servicio incluidos en el acuerdo, sean implementados, mantenidos y operados por el tercero.

Monitoreo y Revisión de los Servicios por Terceros

Control

Los servicios, reportes y registros suministrados por terceras partes se deberían controlar y revisar con regularidad y las auditorias se deberían llevar a cabo a intervalos regulares.

Registro de Auditorías

Control

Se deberían elaborar y mantener durante un periodo acordado las grabaciones de los registros para auditoría de las actividades de los usuarios, las excepciones y los eventos de seguridad de la información

con el fin de facilitar las investigaciones futuras y el monitoreo del control de acceso.

Monitoreo del Uso del Sistema

Control

Se debería establecer procedimientos para el monitoreo del uso de los servicios de procesamiento de información, y los resultados de las actividades de monitoreo se deberían revisar con regularidad.

Protección de la Información del Registro

Control

Los servicios y la información de la actividad de registro se deberían de proteger contra el acceso o la manipulación no autorizados.

Registros del Administrador y del Operador

Control

Se deberían registrar las actividades tanto del operador como del administrador del sistema.

Registro de Fallas

Control

Las fallas se deberían registrar y analizar, y se deberían tomar las acciones adecuadas.

Sincronización de Relojes

Control

Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de la organización o del dominio de seguridad deberían de estar sincronizados con una fuente de tiempo exacta y acordada.

2.7 Control del Acceso

Requisitos del Negocio para el Control del Acceso

Objetivo: Controlar el acceso a la información.

El acceso a la información, a los servicios de procesamiento de información y a los procesos del negocio se debería controlar con base en los requisitos de seguridad y del negocio.

Las reglas del control de acceso deberían de tener en cuenta las políticas de distribución y autorización de la información.

Política de Control de Acceso

Control

Se debería establecer, documentar y revisar la política de control de acceso con base en los requisitos del negocio y de la seguridad para el acceso.

Guía de implementación

Las reglas y los derechos para el control del acceso de cada usuario o grupo de usuario se deberían de establecer con claridad en una política del control del acceso. Los controles del acceso son tanto lógicos como físicos y se deberían de considerar en conjunto. A los usuarios y a los proveedores de servicios se les debería brindar una declaración clara de los requisitos del negocio que deben cumplir los controles del acceso.

La política debería considerar los siguientes aspectos:

a) *Requisitos de seguridad de las aplicaciones individuales del negocio;*
b) *Identificación de toda la información relacionada con las aplicaciones del negocio y los riesgos a los que se enfrenta la información;*
c) *Políticas para la distribución y autorización de la información, como por ejemplo la necesidad de conocer el principio y los niveles de seguridad y la clasificación de la información ;*
d) *Consistencia entre el control del acceso y las políticas de clasificación de la información de sistemas y redes diferentes;*
e) *Legislación pertinente y obligaciones contractuales relacionadas con la protección del acceso a los datos o los servicios;*

f) *Perfiles estándar de acceso de usuario para funciones laborales comunes en la organización.*

g) *Gestión de los derechos de acceso en un entorno distribuido y con red que reconozca todos los tipos de conexiones posibles;*

h) *Distribución de las funciones de control de acceso, por ejemplo solicitud de acceso autorización de acceso, administración del acceso.*

i) *Requisitos para la autorización formal de las solicitudes de acceso;*

j) *Requisitos para la revisión periódica de los controles de acceso;*

k) *Retiro de los derechos de acceso*

Información adicional

Se recomienda cuidado al especificar las reglas de control de acceso para considerar:

a) *diferenciación entre reglas que siempre se deben de hacer cumplir y directrices que son opcionales o condicionales;*

b) *establecimiento de reglas basadas en la premisa "En general todo está prohibido, a menos que esté expresamente permitido" y no en la regla más débil de "En general todo está permitido a menos que esté expresamente prohibido";*

c) *cambios en las etiquetas de información que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados a discreción del usuario.*

d) *Cambios en los permisos de usuario que son iniciados automáticamente por los servicios de procesamiento de información y aquellos iniciados por un administrador;*

e) *Reglas que requieren aprobación específica antes de su promulgación y aquellas que no;*

Las reglas de control de acceso deberían de tener soporte de procedimiento formales y de responsabilidades claramente definidas

Gestión del Acceso de Usuarios

Objetivo: asegurar el acceso de usuarios no autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.

Se deberían de establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas de servicio de información.

Los procedimientos deberían comprender todas las fases del ciclo de vida del acceso del usuario, desde el registro inicial de los usuarios nuevos hasta la cancelación final del registro de usuarios que ya no requieren acceso a los servicios y sistemas de información. Se debería poner atención especial según el caso a la necesidad de controlar la asignación de derechos de acceso privilegiado que permiten a los usuarios anular los controles del sistema.

Registro de Usuarios

Control

Debería de existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información.

Guía de implementación

El procedimiento de control del acceso para el registro y cancelación de usuarios debería incluir:

a) Uso de la identificación única del usuario (ID) para permitir que los usuarios queden vinculados y sean responsables de sus acciones; el uso de identificadores (ID) de grupo únicamente se debería permitir cuando son necesarios por razones operativas o del negocio, y deberían estar aprobados y documentados;

b) Verificación de que el usuario tenga autorización del dueño del sistema para el uso del sistema o servicio de información, también pueden ser conveniente que la dirección apruebe por separado los derechos de acceso;

c) Verificación de que el nivel de acceso otorgado sea adecuado para los propósitos del negocio y sea consistente con la política de seguridad de la organización, es decir, no pone en peligro la distribución de funciones;

d) Dar a los usuarios una declaración escritas de sus derechos de acceso;

e) Exigir a los usuarios firmar declaraciones que indiquen que ellos entienden las condiciones del acceso;

f) Asegurar que los proveedores del servicio no otorguen el acceso hasta que se hayan terminado los procedimiento de autorización;

g) Mantenimiento de un registro formal de todas las personas registradas para usar el servicio;

h) Retirar o bloquear inmediatamente los derechos de acceso de los usuarios que han cambiado de función, de trabajo o que han dejado la organización;

i) Verificar, retirar o bloquear periódicamente las identificaciones (ID) y cuentas redundantes de usuarios;

j) Garantizar que las identificaciones (ID) de usuarios redundantes no se otorgan a otros usuarios.

Información adicional

Se debería considerar el establecimiento de roles de acceso de usuario basadas en los requisitos del negocio que incluyan un número de derechos en perfiles típicos de acceso de usuarios. Las solicitudes y revisiones de acceso se gestionan más fácilmente en el ámbito de dichas funcionan que en el ámbito de derechos particulares.

Es conveniente considerar la inclusión de cláusulas en los contratos del personal y de los servicios que especifiquen las sanciones si el personal o los agentes del servicio intentan el acceso no autorizado.

Gestión de Privilegios

Control

Se debería restringir y controlar la asignación y el uso de privilegios.

Guía de implementación

Los sistemas de usuario múltiple que requieren protección contra el acceso no autorizado deberían controlar la asignación de privilegios a través de un proceso formal de autorización. Se recomienda tener en cuenta los siguientes elementos:

a) *se deberían identificar los usuarios y sus privilegios de acceso asociados con cada producto del sistema, como sistema operativo, sistema de gestión de base de datos y aplicaciones;*
b) *se deberían asignar los privilegios a los usuarios sobre los principios de necesidad de uso y evento por evento y de manera acorde con la política de control de acceso, es decir, el requisito mínimo para función, solo cuando sea necesario;*
c) *se debería conservar un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no se debería otorgar hasta que el proceso de autorización esté completo;*
d) *es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios;*
e) *se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios;*
f) *los privilegios se debería asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del negocio.*

Información adicional

El uso apropiado de los privilegios de administración del sistema (cualquier característica o servicio de un sistema que permita al usuario anular los controles de la

aplicación) puede ser un factor contribuyente importante a las fallas o vulnerabilidades del sistema.

Gestión de Contraseñas para Usuarios

Control

La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.

Guía de implementación

El proceso debería incluir los siguientes requisitos:

a) se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservar las contraseñas de grupo únicamente entre los miembros de éste; esta declaración firmada se podría incluir en los términos y condiciones laborales.

b) cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les es conveniente promover el desarrollo y empleo de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

c) se recomienda promover también el desarrollo y empleo de programas que eviten la necesidad de funcionar con privilegios.

d) los privilegios se deberían asignar a un identificador de usuario (ID) diferente a los utilizados para el uso normal del negocio.

Información adicional

El uso no apropiado de los privilegios de administración del sistema (cualquier característica o servicio de un sistema que permita al usuario anular los controles del sistema o de la aplicación) puede ser un factor contribuyente importante a las fallas o vulnerabilidades del sistema.

Gestión de Contraseñas para Usuarios

Control

La asignación de contraseñas se debería controlar a través de un proceso formal de gestión.

Guía de implementación

El proceso debería incluir los siguientes requisitos:

a) *Se debería exigir a los usuarios la firma de una declaración para mantener confidenciales las contraseñas personales y conservas las contraseñas de grupo únicamente entre los miembros de este; esta declaración firmada se podría incluir en los términos y condiciones laborales*

b) *Cuando se exige a los usuarios mantener sus propias contraseñas, inicialmente se les debería suministrar una contraseña temporal segura que estén forzados a cambiar inmediatamente.*

c) *Establecer procedimientos para verificar la identidad de un usuario antes de proporcionarle una contraseña temporal, de reemplazo o nueva*

d) *Las contraseñas temporales se deberían suministrar de forma segura a los usuarios; se recomienda evitar mensajes de correo electrónico de terceras partes o sin protección (texto claro);*

e) *Las contraseñas temporales deberían ser únicas para un individuo y no ser descifrables*

f) *Los usuarios deberían confirmar la entrega de las contraseñas*

g) *Las contraseñas nunca se deberían almacenar en sistemas de computador en un formato no protegido.*

h) *Las contraseñas predeterminadas por el proveedor se deberían cambiar inmediatamente después de la instalación de los sistemas o del software.*

Información adicional

Las contraseñas son un medio común de verificación de la identidad de un usuario antes de darle acceso a un sistema o servicio de información de acuerdo con la autorización del usuario. Según el caso, es recomendable considerar otras tecnologías disponibles para la identificación y autenticación del usuario tales como biométricos, (verificación de huella digital, verificación de firma) y el uso de tokens de autenticación,(tarjetas inteligentes).

Revisión de los Derechos de Acceso de los Usuarios

Control

La dirección debería establecer un procedimiento formal de revisión periódica de los derechos de acceso de los usuarios.

Guía de implementación

Se recomienda que en la revisión de los derechos de acceso se consideren las siguientes directrices:

a) *Los derechos de acceso de los usuarios se debería revisar a intervalos regulares, por ejemplo cada seis meses y después de cada cambio, como por ejemplo promoción cambio a un cargo en un nivel inferior, o terminación del contrato laboral);*
b) *Los derechos de acceso de usuarios se debería revisar y reasignar cuando hay cambios de un cargo a otro dentro de la misma organización;*
c) *Es recomendable revisar las autorizaciones para derechos de acceso privilegiado a intervalos más frecuentes, por ejemplo cada tres meses;*
d) *Se debería verificar la asignación de privilegios a intervalos regulares para garantizar que no se obtienen privilegios no autorizados;*
e) *Los cambios en las cuentas privilegiadas se deberían registrar para su revisión periódica.*

Información adicional

Es necesario revisar con regularidad los derechos de acceso de los usuarios para mantener un control eficaz del acceso a los datos y a los servicios de información.

Responsabilidades de los Usuarios

Objetivo: evitar el acceso de usuarios no autorizados, el robo o la puesta en peligro de la información y de los servicios de procesamiento de información.

La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad.

Se debería concientizar a los usuarios sobre sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular con relación al uso de contraseñas y a la seguridad del equipo del usuario.

Es recomendable implementar una política de escritorio y pantalla despejados para reducir el riesgo de acceso no autorizado o daño de reportes, medios y servicios de procesamiento de información.

Uso de Contraseñas

Control

Se debería exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas.

Guía de implementación

Todos los usuarios deberían:

a) *Mantener la confidencialidad de las contraseñas;*

b) *Evitar conservar registros (por ejemplo en papel, archivos de software o dispositivos manuales) de las contraseñas , a menos que estas se puedan almacenar de forma segura y el método de almacenamiento este aprobado;*

c) *Cambiar las contraseñas siempre que haya indicación de puesta en peligro del sistema o de la contraseña;*

d) *Seleccionar contraseñas de calidad con longitud mínima suficiente que:*

   1) *Sean fáciles de recordar;*

   2) *No se basen en algo que alguien pueda adivinar fácilmente o usando información relacionada con la persona, por ejemplo nombre, números telefónicos, fechas de cumpleaños, etc.*

   3) *No sean vulnerables al ataque de diccionarios (es decir, que no consistan en palabras incluidas en diccionarios)*

   4) *No tengan caracteres idénticos consecutivos que no sean todos numéricos ni todos alfabéticos;*

e) *Cambiar las contraseñas a intervalos regulares o con base en el numero de accesos (las contraseñas para cuentas privilegiadas se deberían cambiar con más frecuencia que las contraseñas normales) y evitar la reutilización de contraseñas antiguas;*

f) *Cambiar las contraseñas temporales en el primer registro de inicio;*

g) *No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función;*

h) *No compartir las contraseñas de usuario individuales;*

i) *No utilizar la misma contraseña para propósitos del negocio y para los que no lo son.*

Si los usuarios necesitan acceso a múltiples servicios, sistemas o plataformas y se les exige conservar múltiples contraseñas separadas, se les debería advertir que

pueden usar una sola contraseña de calidad (véase d) arriba) para todos los servicios cuando se les garantiza que se ha establecido un nivel razonable que protección para almacenar la contraseña en cada servicio, sistema o plataforma.

Información adicional

La gestión de los sistemas de ayuda del escritorio auxiliar que tratan con las contraseñas perdidas u olvidadas necesita cuidado especial puesto que también puede ser un medio de ataque al sistema de contraseña.

Equipo de Usuario Desatendido

Control

Los usuarios deberían asegurarse de que los equipos desatendidos tenga protección propia

Guía de implementación

Se debería concientizar a los usuarios sobre los requisitos y los procedimientos de seguridad para proteger los equipos desatendidos, así como sobre sus responsabilidades en la implementación de dicha protección. Se debería advertir a los usuarios sobre:

a) *Terminar las sesiones activas cuando finalice, a menos que se puedan asegurar por medio de un mecanismo de bloqueo, como un protector de pantalla protegido por contraseña;*

b) *Realizar el registro de cierre en computadoras principales, servidores y computadores, personales de oficina al terminar la sesión (es decir, no solo apagar el interruptor de la pantalla del computador o terminal);*
c) *Cuando no están en uso, asegurar los computadores personales o los terminales contra el uso no autorizado mediante una clave de bloqueo o un control equivalente como, por ejemplo, el acceso por contraseña.*

Información adicional

Los equipos instalados en las aéreas de usuario, por ejemplo las estaciones de trabajo o los servidores de archivo, pueden requerir protección específica contra el acceso no autorizado cuando se dejen desatendidos durante periodos prolongados.

Política de Escritorio Despejado y de Pantalla Despejada

Control

Se debería adoptar una política de escritorio despejado para reportes y medios de almacenamiento removibles y una política de pantalla despejada para los servicios de procesamiento de información.

Guía de implementación

En la política de escritorio despejado y pantalla despejada se deberían considerar las clasificaciones de la información, los requisitos legales y contractuales, los riesgos correspondientes y los aspectos culturales de la organización. Es recomendable tener presentes las siguientes directrices:

a) *Cuando no se requiere la información sensible o critica del negocio, como por ejemplo los medios de almacenamiento electrónicos o en papel, se debería asegurar bajo llave(idealmente una caja fuerte , un gabinete u otro mueble de seguridad) , especialmente cuando la oficina está vacía;*
b) *Las sesiones de los computadores y los terminales se deberían cerrar o proteger con un mecanismo de bloqueo de pantalla y de teclado controlado por una contraseña, un token o un mecanismo similar de autenticación de usuario cuando no están atendidos, y se deberían proteger mediante bloqueos de clave, contraseñas u otros controles cuando no se estén utilizando;*
c) *Se deberían proteger los puntos de entrada y salida de correo y las maquinas de facsímil desatendidas;*
d) *Es conveniente evitar el uso no autorizado de fotocopiadores y otra tecnología de reproducción (por ejemplo, escáneres, cámaras digitales, etc.).*
e) *Los documentos que contengan información sensible o clasificada se deberían retirar inmediatamente de las impresoras.*

Información adicional

Una política sobre escritorio despejado / pantalla despejada reduce los riesgos de acceso no autorizado, perdida y daño de la información durante y fuera de las horas

laborales normales. Las cajas fuertes u otras formas de almacenamiento seguro también podrían proteger la información almacenada allí contra desastres como incendio, terremoto, inundación o explosión.

Se deberían pensar en la utilización de impresores con función de código de pines (pin code) de forma que quien inicia la impresión sea el único que pueda obtenerla y únicamente cuando este cerca de la impresora.

Control de Acceso a las Redes

Objetivo: evitar el acceso no autorizado a los servicios en red.

Es recomendable controlar el acceso a los servicios en red tanto internos como externos.

El acceso de los usuarios a las redes y a los servicios de red no debería comprometer la seguridad de los servicios de red garantizando que:

a) *Existen interinases apropiadas entre la red de la organización y las redes que pertenecen a otras organizaciones, y las redes públicas;*
b) *Se aplican mecanismos adecuados de autenticación para los usuarios y los equipos;*
c) *Se exige control de acceso de los usuarios a los servicios de información.*

Política de Uso de los Servicios en Red

Control

Los usuarios solo deberían tener acceso a los servicios para cuyo uso están específicamente autorizados.

Guía de implementación

Se debería formular una política con respecto al uso de las redes y los servicios de red. Esta política debería abarcar:

a) *Las redes y los servicios de red a los cuales permite el acceso;*
b) *Los procedimientos de autorización para determinar a quién se le permite el acceso a que redes y que servicios en red;*
c) *Los controles y procedimientos de gestión para proteger el acceso a las conexiones de red y los servicios de red;*
d) *Los medios utilizados para el acceso a las redes y los servicios de red (por ejemplo las condiciones para permitir el acceso a la marcación a un proveedor de servicios de internet o a un sistema remoto).*
e) La política sobre el uso de los servicios de red debería ser consistente con la política de control de acceso de la organización.

Información adicional

Las conexiones inseguras y no autorizadas a servicios de red pueden afectar a toda la organización. Este control es particularmente importante para las conexiones de red de aplicaciones sensibles o críticas para el negocio o para usuarios en lugares de alto riesgo, por ejemplo en áreas públicas o externas que se hallan fuera del control y la gestión de seguridad de la organización.

Autenticación de Usuarios para Conexiones Externas

Control

Se deberían emplear métodos apropiados de autenticación para controlar el acceso de usuarios remotos.

Guía de implementación

La autenticación de usuarios remotos se puede lograr usando, por ejemplo, una técnica con base criptográfica, token de hardware o protocolos de desafío / respuesta. Las posibles implementaciones de dichas técnicas se pueden encontrar en diversas soluciones de red privada virtual (VPN). Las líneas privadas dedicadas también se pueden emplear para brindar aseguramiento de la fuente de las conexiones.

Los procedimientos y controles de devolución de marcación, por ejemplo empleando módems de retorno de marcación, pueden suministrar protección contra conexiones no deseadas o no autorizadas a los servicios de procesamiento de información de la organización. Este tipo de control autentica a los usuarios tratando de establecer una conexión con una red de la organización desde sitios remotos. Cuando se usa este control, la organización no debería utilizar servicios de red que incluyen envió de llamada o, si lo hacen, deberían desactivar el uso de dichas características para evitar las debilidades asociadas con el envió de llamada. El proceso de devolución de llamada debería garantizar que realmente se produce una desconexión en el lado de la organización. De otro modo, el usuario remoto debería mantener la línea abierta pretendiendo que ha ocurrido la verificación de la devolución de la llamada. Los procedimientos y controles de devolución de la llamada se deberían probar en su totalidad para determinar esta posibilidad.

La autenticación del nodo puede servir como un medio alterno para la autenticación de grupos de usuarios remotos cuando están conectados a un servicio seguro de computador compartido.

Para la autenticación del nodo se pueden emplear las técnicas criptográficas, por ejemplo las basadas en certificados de máquina. Esto forma parte de varias soluciones basadas en la red privada virtual (VPN).

Se deberían implementar controles de autenticación adicionales para controlar el acceso a redes inalámbricas. En particular, es necesario tener cuidado especial en la selección de los controles para redes inalámbricas debido a las grandes oportunidades para la interceptación e inserción no detectadas en el tráfico de la red.

Información adicional

Las conexiones externas suministran un potencial para el acceso no autorizado a la información del negocio, por ejemplo el acceso a los métodos de marcación. Existen diferentes métodos de autenticación, algunos de los cuales proporcionan un mayor grado de protección que otros, como por ejemplo los métodos con base en el uso de técnicas criptográficas que pueden brindar autenticación solida. Es importante determinar a partir de la evaluación de riesgos el grado necesario de protección. Ello es necesario para la selección adecuada de un método de autenticación.

Un medio para la conexión automática a un computador remoto podría suministrar una forma de obtener acceso no autorizado a una aplicación del negocio. Esto es especialmente importante si la conexión utiliza una red que esta fuera del control de la gestión de seguridad de la organización.

Identificación de los Equipos en las Redes

Control

La identificación automática de los equipos se debería considerar un medio para autenticar conexiones de equipos y ubicaciones específicas.

Guía de implementación

Se puede usar la identificación del equipo, si es importante que la comunicación únicamente se pueda iniciar desde un equipo o ligar especifico. Un identificador en el equipo o acoplado a este se puede usar para indicar si está permitido que este equipo se conecte a la red. Estos identificadores deberían indicar con claridad a que red está permitido conectar el equipo, si existe más de una red y si estas redes tienen sensibilidad diferente. Puede ser necesario considerar la protección física del equipo para mantener la seguridad del identificador de este.

Información adicional

Este control se puede complementar con otras técnicas para autenticar el usuario del equipo. La identificación del equipo se puede aplicar en adición a la autenticación del usuario.

Protección de los Puertos de Configuración y Diagnostico Remoto

Control

El acceso lógico y físico a los puertos de configuración y de diagnostico debería estar controlado.

Guía de implementación

Los controles potenciales para el acceso a los puertos de diagnostico y configuración incluyen el uso de un bloqueo de clave y procedimientos de soporte para controlar el acceso físico al puerto. Un ejemplo de un procedimiento de soporte es garantizar que los puertos de diagnostico y configuración solo sean accesibles mediante acuerdo entre el administrador del servicio de computador y el personal de soporte de hardware / software que requiere el acceso.

Los puertos, servicios y prestaciones similares instaladas en un servicio de computador o de red, que no se requieren específicamente para la funcionalidad del negocio, se deberían inhabilitar o retirar.

Información adicional

Muchos sistemas de computador, sistemas de red y sistemas de comunicación se instalan en un sitio de configuración o de diagnostico remoto para ser utilizados por los ingenieros de mantenimiento. Si no están protegidos, estos puertos de diagnostico son un medio para el acceso no autorizado.

Separación en las Redes

Control

En las redes se deberían separar los grupos de servicios de información, usuarios y sistemas de información.

Guía de implementación

Un método para el control en las redes grandes es dividirlas en dominios lógicos de red separados, por ejemplo, dominios de red internos de la organización y dominios de red externos, cada uno protegido por un perímetro de seguridad definido. Se puede aplicar un conjunto graduado de controles en diferentes dominios lógicos de red para separar aun más los entornos de seguridad de la red, por ejemplo los sistemas de acceso público, las redes internas y los activos críticos. Los dominios se deberían definir con base en una evaluación de riesgos y en los diferentes requisitos de seguridad en cada uno de los dominios.

Se puede implementar un perímetro de red instalado una puerta de enlace (Gateway) seguro entre las dos redes que se van a interconectar para controlar el acceso y el flujo de información entre los dos dominios. Esta puerta de enlace (Gateway) se debería configurar para filtrar el trafico entre estos dominios y para bloquear el acceso no autorizado, según la política de control de acceso de la organización. Un ejemplo de este tipo de puerta de enlace (Gateway) es lo que se conoce comúnmente como barrera de fuego (firewall). Otro método para apartar los dominios lógicos separados es restringir el acceso a la red usando redes privadas virtuales para grupos de usuarios dentro de la organización.

Las redes también se pueden separar utilizando la funcionalidad del dispositivo de red, por ejemplo la conmutación IP. Los dominios separados se pueden implementar entonces controlando los flujos de datos de la red usando las capacidades de enrutamiento / conmutación, como por ejemplo la listas de control de acceso.

Los criterios para separar las redes en dominios se deberían basar en la política de control de acceso y en los requisitos de acceso y deberían tener en cuenta los costos relativos y el impacto en el desempeño por la incorporación de tecnología conveniente de puerta de enlace (Gateway) o de enrutamiento de red.

Además, la separación de las redes se debería basar en el valor y la clasificación de la información almacenada o procesada en la red, los niveles de confianza o los lineamientos del negocio con el fin de reducir el impacto total de una interrupción del servicio.

También se debería pensar en la separación de las redes inalámbricas no están bien definidos, es recomendable llevar a cabo una evaluación de riesgos en tales casos para identificar los controles (por ejemplo, autenticación solida, métodos criptográficos y selección de frecuencia) para mantener la separación de la red.

Información adicional

Las redes se extienden cada vez más allá de las fronteras tradicionales de la organización, ya que se forman sociedades de negocios que pueden requerir la interconexión o compartir el procesamiento de información y las prestaciones de la red. Tal extensión puede incrementar el riesgo no autorizado a los sistemas de información existentes que utilizan la red, algunos de los cuales pueden requerir protección contra otros usuarios de la red debido a su sensibilidad o importancia.

Control de Conexión a las Redes

Control

Para redes compartidas, especialmente aquellas que se extienden mas allá de las fronteras de la organización, se debería restringir la capacidad de los usuarios para conectarse a la red, de acuerdo con la política de control de acceso y los requisitos de aplicación del negocio.

Guía de implementación

Los derechos de acceso a la red de los usuarios se deberían mantener y actualizar según se requiera a través de la política de control de acceso.

La capacidad de conexión de los usuarios se puede restringir a través de puertas de enlace (Gateway) de red que filtren el tráfico por medio de tablas o reglas predefinidas. Los siguientes son algunos ejemplos de aplicaciones a las cuales se deberían aplicar restricciones:

a) *Mensajería, por ejemplo, el correo electrónico;*
b) *Transferencia de archivos;*
c) *Acceso interactivo;*
d) *Acceso a las aplicaciones.*

Es conveniente tomar en consideración el enlace de los derechos de acceso a la red con algunas horas del día o fechas.

Información adicional

La política de control del acceso puede exigir la incorporación de controles para restringir la capacidad de conexión de los usuarios a redes compartidas, especialmente aquellas que se extienden más allá de las fronteras de la organización.

Control del Enrutamiento en la Red

Control

Se deberían implementar controles de enrutamiento en las redes con el fin de asegurar que las conexiones entre computadores y los flujos de información no incumplan la política de control de acceso de las aplicaciones del negocio.

Guía de implementación

Los controles de enrutamiento se deberían basar en mecanismos de verificación para las direcciones fuente / destino validos.

Las puertas de enlace (Gateway) de seguridad se pueden usar para validar la dirección fuente/destino en los puntos de control de las redes interna y externa, si se emplean tecnológicas proxy y / o de traducción de dirección de red. Quienes desarrollan la implementación deberían ser conscientes de las fortalezas y

deficiencias de los mecanismos desplegados. Los requisitos para el control del enrutamiento en la red se deberían basar en la política de control de acceso

Información adicional

Las redes compartidas, especialmente aquellas que van más allá de las fronteras de la organización, pueden requerir controles adicionales de enrutamiento. Esto se aplica particularmente cuando las redes son compartidas por usuarios de terceras partes (que no pertenecen a la organización).

Control de Acceso al Sistema Operativo

Objetivo: evitar el acceso no autorizado a los sistemas operativos.

Se recomienda utilizar medios de seguridad para restringir el acceso de usuarios no autorizados a los sistemas operativos. Tales medios deberían tener la capacidad para:

a) *Autenticar usuarios autorizados, de acuerdo con una política definida de control de acceso;*
b) *Registrar intentos exitosos y fallidos de autenticación del sistema;*
c) *Registrar el uso de privilegios especiales del sistema;*
d) *Emitir alarmas cuando se violan las políticas de seguridad del sistema;*
e) *Suministrar medios adecuados para la autenticación;*
f) *Cuando sea apropiado, restringir el tiempo de conexión de los usuarios.*

Procedimientos de Registro de Inicios Seguro

Control

El acceso a los sistemas operativos se debería controlar mediante un procedimiento de registro de inicio seguro.

Guía de implementación

El procedimiento de registro en un sistema operativo debería estar diseñado para minimizar la oportunidad de acceso no autorizado. Por lo tanto, el procedimiento de registro de inicio debería divulgar información mínima sobre el sistema para evitar suministrar asistencia innecesaria a un usuario no autorizado. Un buen procedimiento de registro de inicio debería cumplir los siguientes aspectos:

a) *No mostrar identificadores de aplicación ni de sistema hasta que el proceso de registro de inicio se haya completado exitosamente;*
b) *Mostrar una advertencia de notificación general indicando que solo deberían tener acceso al computador los usuarios autorizados;*
c) *No suministrar mensajes de ayuda durante el procedimiento de registro de inicio que ayuden a un usuario no autorizado;*
d) *Validar la información de registro de inicio únicamente al terminar todos los datos de entrada. Si se presenta una condición de error, el sistema no debería indicar que parte de los datos es correcta o incorrecta;*
e) *Limitar la cantidad de intentos permitidos de registro de inicio, por ejemplo tres intentos, y considerar:*

1) *Registrar intentos exitosos y fallidos.*
2) *Forzar un tiempo de dilación antes de permitir intentos adicionales del registro de inicio o de rechazar los intentos adicionales sin autorización específica;*
3) *Desconectar las conexiones de enlaces de datos.*
4) *Enviar un mensaje de alarma a la consola del sistema si se alcanza la cantidad máxima de intentos de registro de inicio;*
5) *Establecer la cantidad de reintentos de contraseña junto con la longitud mínima de ella y el valor del sistema que se protege;*

f) Limitar el tiempo máximo y mínimo permitido para el procedimiento de registro de inicio. Si se excede, el sistema debería finalizar esta operación;

g) Mostrar la siguiente información al terminar un registro de inicio exitoso:

1) *Fecha y hora del registro de inicio exitoso previo;*
2) *Detalles de los intentos fallidos de registro de inicio desde el último registro exitoso;*

h) No mostrar la contraseña que se introduce o considerar esconder los caracteres mediante símbolos;

i) No transmitir contraseñas en texto claro en la red.

Información adicional

Si las contraseñas se transmiten en texto claro durante la sesión de registro de inicio pueden ser capturadas en la red por un programa “husmeador” de red.

Identificación y Autenticación de Usuarios

Control

Todos los usuarios deberían tener u identificador único (ID del usuario) únicamente para su uso personal, y se debería elegir una técnica apropiada de autenticación para comprobar la identidad declarada de un usuario.

Guía de implementación

Este control se debería aplicar a todos los tipos de usuarios (incluyendo el personal de soporte técnico, operadores, administradores de red, programadores de sistemas y administradores de bases de datos).

Los identificadores de usuario (ID) se deberían utilizar para rastrear las actividades de la persona responsable. Las actividades de usuarios regulares no se deberían realizar desde cuentas privilegiadas.

En circunstancias excepcionales, cuando existe un beneficio claro para el negocio, se puede usar un identificador de usuario compartido para un grupo de usuarios o u n trabajo especifico. La apropiación por la dirección debería estar documentada para dichos casos. Se pueden requerir controles adicionales para mantener la responsabilidad.

Solo se deberían permitir los identificadores (ID) de usuario genéricos para uso de un individuo si existen funciones accesibles o si no es necesario rastrear las acciones ejecutadas por el identificador (por ejemplo el acceso de solo lectura), o cuando no hay

controles establecidos (por ejemplo cuando la contraseña para un identificador genérico solo se emite para un personal a la vez y el registro de tal caso).

Cuando se requiere verificación de identidad y autenticación solidas, se deberían utilizar métodos alternos a la contraseña, como los medios criptográficos, las tarjetas inteligentes, token o medios biométricos.

Información adicional

Las contraseñas son una forma muy común de identificar y autenticar con base en un secreto que solo conoce el usuario. Lo mismo se puede lograr con medios criptográficos y protocolos de autenticación. La fortaleza de la identificación y autenticación del usuario debería ser adecuada a la sensibilidad de la información a la que se tiene acceso.

Objetos tales como los tokens de memoria o las tarjetas inteligentes que poseen los usuarios también se pueden usar para la identificación y la autenticación. Las tecnologías de autenticación biométrica que utilizan características o atributos únicos de un individuo también se pueden usar para autenticar la identidad de un apersona. Una combinación de tecnológicas y mecanismos enlazados con seguridad producirá una autenticación solida.

Sistema de Gestión de Contraseñas

Control

Los sistemas para la gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.

Guía de implementación

Un sistema de gestión de contraseñas debería:

a) *Hacer cumplir el uso de identificadores de usuario (ID) individual y de contraseñas para conservar la responsabilidad;*
b) *Permitir a los usuarios la selección y el cambio de sus contraseñas e incluir un procedimiento de confirmación para tener en cuente los errores en los ingresos;*
c) *Imponer una elección de contraseñas de calidad;*
d) *Imponer cambios de contraseña;*
e) *Forzar a los usuarios a cambiar las contraseñas temporales en el primer registro de inicio;*
f) *Conservar un registro de las contraseñas de usuario previas y evitar su reutilización;*
g) *No mostrar contraseñas en la pantalla cuando se hace su ingreso;*
h) *Almacenar los archivos de contraseñas separadamente de los datos del sistema de aplicación;*
i) *Almacenar y transmitir las contraseñas en formatos protegidos (por ejemplo encriptados o codificadas);*

Información adicional

Las contraseñas son un mecanismo principal para validar una autoridad del usuario para tener acceso a un servicio de computador.

Algunas aplicaciones requieren la asignación de contraseñas de usuario por parte de una autoridad independiente, en tales casos, no se aplican los literales b), d) y e) indicados en la directriz anterior. En la mayoría de los casos, las contraseñas son seleccionadas y conservadas por los usuarios.

Uso de las Utilidades del Sistema

Control

Se debería restringir y controlar estrictamente el uso de programas utilitarios que pueden anular los controles del sistema y de la aplicación.

Guía de aplicación

Se recomienda considerar la siguiente directriz para el uso de las utilidades del sistema:

a) *Uso de procedimientos de identificación, autenticación y autorización para las utilidades del sistema;*
b) *Separación de las utilidades del sistema del software de aplicaciones,*
c) *Limitación del uso de las utilidades del sistema a la cantidad mínima viable de usuarios de confianza autorizados ;*
d) *Autorización del uso ad hoc de las utilidades del sistema;*
e) *Limitación de la disponibilidad de las utilidades del sistema, por ejemplo para la duración de u cambio autorizado;*
f) *Registro de todo uso de las utilidades del sistema;*

g) *Definición y documentación de los niveles de autorización para las utilidades del sistema;*
h) *Retiro o inhabilitación de todas las utilidades o el software del sistema basada en software innecesario;*
i) *No poner a disposición las utilidades del sistema a usuarios que tengan acceso a aplicaciones en sistemas en donde se requiere distribución de funciones.*

Información adicional

La mayoría de las instalaciones de computador tiene uno o más programas de utilidades del sistema que pueden anular los controles del sistema y de la aplicación.

Tiempo de Inactividad de la Sesión

Control

Las sesiones inactivas se deberían suspender después de un periodo definido de inactividad.

Guía de implementación

Una utilidad de tiempo de inactividad debería despejar la pantalla de sesión y también, tal vez mas tarde, cerrar tanto la sesión de la aplicación como la de red

después de un periodo definido de inactividad. La dilación del tiempo de inactividad debería reflejar los riesgos de seguridad del área, la clasificación de la información que se maneja y las aplicaciones que se utilizan, así como los riesgos relacionados con los usuarios del equipo.

Algunos sistemas pueden suministrar una forma limitada de utilidad de tiempo de inactividad la cual despeja la pantalla y evita el acceso no autorizado, pero no cierra las sesiones de aplicación ni de red.

Información adicional

Este control es importante particularmente en lugares de alto riesgo, los cuales incluyen áreas públicas o externas fuera de la gestión de seguridad de la organización. Las sesiones se deberían cerrar para evitar el acceso de personas no autorizadas y negar ataques al servicio.

Limitación del Tiempo de Conexión

Control

Se deberían utilizar restricciones en los tiempos de conexión para brindar seguridad adicional para las aplicaciones de alto riesgo.

Guía de implementación

Se deberían tener en cuenta los controles de tiempo para las aplicaciones sensible de computador, especialmente las de lugares de alto riesgo, por ejemplo áreas

públicas o externas que están fuera de la gestión de seguridad de la organización. Los siguientes son algunos ejemplos de estas restricciones:

a) *Uso de espacios de tiempo predeterminados, por ejemplo, para transmisiones de lotes de archivos o uso de sesiones interactivas de corta duración.*
b) *Restricción de los tiempos de conexión a las horas normales de oficina, si no se requiere tiempo extra u operaciones de horario prolongado;*
c) *Considerar la repetición de la autenticación a intervalos determinados.*

Información adicional

La limitación del periodo durante el cual se permite la conexión a los servicios de computador reduce la ventana de oportunidad para el acceso no autorizado. La limitación de la duración de las sesiones activas evita que los usuarios mantengan sesiones abiertas para evitar la repetición de la autenticación.

Control de Acceso a las Aplicaciones y a la Información

Objetivo: evitar el acceso no autorizado a la información contenida en los sistemas de aplicación.

Se deberían usar medios de seguridad para restringir el acceso a loa sistemas de aplicación y dentro de ellos.

El acceso lógico al software de aplicación y ala información se debería restringir a usuarios autorizados.

Los sistemas de aplicación deberían:

a) *Controlar el acceso de usuarios a la información y a las funciones del sistema de aplicación, de acuerdo con una política definida de control de acceso;*
b) *Suministrar protección contra acceso no autorizado por una utilidad, el software del sistema operativo y software malicioso que pueda anular o desviar los controles del sistema o de la aplicación;*
c) *No poner en peligro otros sistemas con los que se comparten los recursos de información.*

Restricción del Acceso a la Información

Control

Se debería restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

Guía de implementación

Las restricciones del acceso se deberían basar en los requisitos de las aplicaciones individuales del negocio. La política de control de acceso también debería ser consistente con la política de acceso de la organización.

Se debería considerar la aplicación de las siguientes directrices con el objeto de dar soporte a los requisitos de restricción del acceso:

a) *Proporcionar menús para controlar el acceso a las funciones del sistema de aplicación;*
b) *controlar los derechos de acceso de los usuarios , por ejemplo, leer, escribir, eliminar y ejecutar;*
c) *Controlar los derechos de acceso de otras aplicaciones ;*
d) *Garantizar que los datos de salida de los sistemas de aplicación que manejar información sensible solo contienen la información pertinente para el uso de la salida y que se envía únicamente a terminales o sitios autorizados; ello debería incluir revisiones periódicas de dichas salidas para garantizar el retiro de la información redundante.*

Aislamiento de Sistemas Sensibles

Control

Los sistemas sensibles deberían tener un entorno informático dedicado (aislados).

Guía de implementación

Se deberían considerar los siguientes puntos para el aislamiento de los sistemas sensibles:

a) *La sensibilidad de un sistema de aplicación se debería identificar y documentar explícitamente por parte del dueño de la aplicación;*

b) *Cuando una aplicación se ha de ejecutar en un entorno compartido, los sistemas de aplicación con los cuales compartirá recursos y los riesgos correspondientes deberían ser identificados y aceptados y aceptados por el dueño de la aplicación sensible.*

Información adicional

Algunos sistemas de aplicación son lo suficientemente sensibles a la pérdida potencial que requieren manejo especial. La sensibilidad puede indicar que el sistema de aplicación debería:

a) *Ejecutarse en un computador dedicado, o*
b) *Únicamente debería compartir recursos con sistemas de aplicación confiables.*

Computación Móvil y Trabajo Remoto

Objetivo: garantizar la seguridad de la información cuando se utilizan dispositivos de computaciones móviles y de trabajo remoto.

La protección necesaria debería estar con los riesgos que originan estas formas específicas de trabajo. Cuando se usa la computación móvil, se deberían tener en cuenta los riesgos de trabajar en un entorno sin protección y aplicar la protección adecuada. En el caso del trabajo remoto, la organización debería aplicar protección en el sitio del trabajo remoto y garantizar que se han establecido las disposiciones adecuadas para esta forma de trabajo.

Computación y Comunicaciones Móviles

Control

Se debería establecer una política formal y se deberían adoptar las medidas de seguridad apropiadas para la protección contra los riesgos debidos al uso de dispositivos de computación y comunicaciones móviles.

Guía de implementación

Cuando se usan servicios de computación y de comunicaciones móviles, por ejemplo, computadores portátiles livianos (Notebooks), microcomputadores de bolsillo (Palmtops), y computadores portátiles pesados (Laptops), tarjetas inteligentes y teléfonos móviles se debería tener cuidado especial para asegurarse de que la información no se pone en peligro. En la política de computación móvil se deberían considerar los riesgos de trabajar con equipos de computación móvil en entornos de protección.

En la política de computación móvil se deberían incluir los requisitos para la protección física, los controles de acceso, las técnicas criptográficas las copias de respaldo y la protección contra virus. Esta política también debería incluir reglas y asesoría sobre la conexión de los servicios móviles a las redes y directrices sobre el uso de estos servicios en lugares públicos.

Es conveniente tener cuidado cuando se utilizan servicios de computación móvil en lugares públicos, salas de reuniones y otras áreas sin protección fuera de las

instalaciones de la organización. Se debería establecer la protección para evitar el acceso o la divulgación no autorizados de la información almacenada y procesada por estos servicios, por ejemplo, usando técnicas criptográficas.

Los usuarios de servicios de computación móviles en lugares públicos deberían tener cuidado para evitar el riesgo de ser observados por personas no autorizadas. Es recomendable establecer procedimientos contra software malicioso y mantenerlos actualizadas.

Es conveniente hacer copias de respaldo a intervalos regulares de la información del negocio. Se debería disponer de equipo para permitir el respaldo rápido y fácil de la información. Las copias de respaldo deberían tener protección adecuada contra robo o perdida de información.

La utilización de los servicios móviles conectados a las redes debería tener una protección idónea. El acceso remoto a la información del negocio a través públicas usando servicios de computación móvil solo debería tener lugar después de la identificación y la autenticación exitosa y con el establecimiento de los mecanismos adecuadas de control del acceso. Los servicios de computación móvil también se deben proteger físicamente contra robo, especialmente cuando se deja, por ejemplo, en los automóviles y otros medios de transporte, habitaciones de hoteles, centro de conferencias y sitios de reuniones. Es conveniente establecer un procedimiento específico en el que se tengan presentes los requisitos legales, de seguros y otros de seguridad de la organización para los casos de robo o perdida de los servicios de computación móvil. El equipo que porta información sensible y / o critica importante del negocio no se debería dejar desatendido y, cuando sea posible, se debería

bloquear con algún medio físico o usar cerraduras especiales para asegurar el equipo.

Se recomienda disponer la información del personal que utiliza computación móvil para concientizarlo sobre los riesgos adicionales que se originan en este tipo de trabajo y los controles que se deberían implementar.

Información adicional

Las conexiones inalámbricas a red móvil son similares a otros tipos de conexión de red, pero tienen diferencias importantes que se debería considerar al identificar los controles. Las diferencias típicas son:

4. *Algunos protocolos de seguridad inalámbrica son inmaduros y tienen debilidades conocidas;*
4. *La información almacenada en los computadores móviles puede no tener copias de respaldo debido al ancho de banda de red limitado y / o a que el equipo móvil puede no estar conectado en las horas en las que están programadas las copias de respaldo.*

Trabajo Remoto

Control

Se deberían desarrollar e implementar políticas, planes operativos y procedimientos para las actividades de trabajo remoto.

Guía de implementación

Las organizaciones solo deberían autorizar las actividades de trabajo remoto si están satisfechas con las disposiciones de seguridad adecuadas y los controles establecidos, y si ellos cumplen la política de seguridad de la organización.

Es conveniente establecer una protección apropiada del sitio de trabajo remoto contra, por ejemplo robo del equipo y la información, divulgación no autorizada de información, acceso remoto no autorizado a los sistemas internos de la organización o el uso inadecuado de sus servicios. Las actividades de trabajo remoto deberían estar autorizadas y controladas por la dirección y se debería garantizar la instauración de disposiciones adecuadas para esta forma de trabajo.

Se recomienda considerar los siguientes aspectos:

a) *La seguridad física existente en el sitio de trabajo remoto, tomando en consideración la seguridad física de la edificación y del entorno local;*
b) *El entorno físico de trabajo remoto propuesto;*
c) *Los requisitos de seguridad de las comunicaciones, pensando en la necesidad de acceso remoto a los sistemas internos de la organización, la sensibilidad de la información a la cual se tendrá acceso y sobrepasar el enlace de comunicación y la sensibilidad del sistema interno;*
d) *La amenaza del acceso no autorizado a la información o los recursos por parte de otras personas que usan el mismo espacio, por ejemplo familiares y amigos;*

e) *El uso de redes domesticas y los requisitos o restricciones en la configuración de servicios de red inalámbrica;*

f) *Las políticas y los procedimientos para evitar disputas con respecto a los derechos de propiedad intelectual desarrollados o al equipo de propiedad privada;*

g) *El acceso a equipo de propiedad privada (para verificar la seguridad de la maquina o durante una investigación) el cual puede estar prohibido por la ley;*

h) *Los acuerdos sobre licencias de software que permitan que la organización sea responsable de la licencia para software de clientes en estaciones de trabajo de propiedad privada de los empleados contratistas o usuarios de terceras partes;*

i) *Protección antivirus y requisitos de barreras contra fuego (firewall).*

j) *Las directrices y disposiciones a considerar deberían incluir las siguientes:*

   1. *Disposición de equipo adecuado y medios de almacenamiento para las actividades de trabajo remoto, en las que no se permite el uso de equipo de propiedad privada que no este bajo el control de la organización;*
   2. *Definición del trabajo que se permite realizar las horas laborales, la confidencialidad de la información que se conserva y los sistemas y servicios internos para los cuales el trabajador tiene acceso autorizado;*
   3. *Disposición de equipo de comunicación apropiado, incluyendo los métodos para asegurar el acceso remoto;*
   4. *Seguridad física;*

5. *Reglas y directrices sobre el acceso de familiares y visitantes al equipo y a la información;*
6. *Disposición de soporte y mantenimiento de hardware y software;*
7. *Disposición de pólizas de seguros;*
8. *Procedimientos para el respaldo y la continuidad del negocio;*
9. *Auditoria y monitoreo de seguridad;*
10. *Revocación de autoridad y derechos de acceso, y la devolución del equipo al finalizar las actividades de trabajo remoto.*

Información adicional

En el trabajo remoto se emplean tecnologías de comunicaciones que le permiten al personal realizar trabajo remoto desde un lugar fijo de su organización.

2.8 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.

Requisitos de Seguridad de los Sistemas de Información

Objetivo: garantizar que la seguridad es parte integral de los sistemas de información.

Los sistemas de información incluyen sistemas operativos, infraestructura, aplicaciones del negocio, productos de vitrina, servicios y aplicaciones desarrolladas para usuarios. El diseño y la implementación del sistema de

información que da soporte a los procesos del negocio pueden ser cruciales para la seguridad. Se deberían identificar y acordar los requisitos de seguridad antes del desarrollo y / o la implementación de los sistemas de información.

Todos los requisitos de seguridad se deberían identificar en la fase de requisitos de un proyecto y se deberían justificar, acordar y documentar como parte de todo el caso del negocio para un sistema de información.

Análisis y Especificación de los Requisitos de Seguridad

Control

Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras a los sistemas existentes deberían especificar los requisitos para los controles de seguridad.

Procesamiento Correcto en las Aplicaciones

Objetivo: evitar errores, perdidas modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones.

Se deberían diseñar controles apropiados en las aplicaciones incluyendo las aplicaciones desarrolladas por el usuario para garantizar el procesamiento correcto. Estos controles deberían incluir la validación de los datos de entrada del procesamiento interno y de los datos de salida.

Se pueden necesitar controles adicionales para los sistemas que procesan o tienen impacto en la información sensible, de valor o critica. Dichos controles se deberían determinar con base en los requisitos de seguridad y en la evaluación de riesgos.

Validación de los Datos de Entrada

Control

Se deberían validar los datos de entrada a las aplicaciones para asegurar que dichos datos son correctos y apropiados.

Control de Procesamiento Interno

Control

Se deberían incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.

Integridad del Mensaje

Control

Se deberían identificar los requisitos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificar e implementar los controles adecuados.

Validación de los Datos de Salida

Control

Se deberían validar los datos de salida de una aplicación para asegurar que el procesamiento de la información almacenada es correcto y adecuado a la circunstancias.

Controles Criptográficos

Objetivo: proteger la confidencialidad, autenticidad o integridad de la información, por medios criptográficos.

Se debería desarrollar una política sobre el uso de los controles criptográficos y establecer una gestión de claves para dar soporte al empleo de técnicas criptográficas.

Política Sobre el Uso de Controles Criptográficos

Control

Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.

Gestión de Claves

Control

Se debería establecer la gestión de claves para apoyar el uso de técnicas criptográficas en la organización.

Seguridad de los Archivos del Sistema

Objetivo: garantizar la seguridad de los archivos del sistema.

Los accesos a los archivos del sistema y al código fuente del programa deberían estar protegidos, y los proyectos de tecnología de la información y las actividades de soporte se deberían efectuar de forma segura. Se debería tener cuidado para evitar la exposición de datos sensibles en los entornos de prueba.

Control del Software Operativo

Control

Se deberían establecer procedimientos para controlar la instalación de software en los sistemas operativos.

Protección de los Datos de Prueba del Sistema

Control

Los datos de prueba deberían seleccionarse cuidadosamente, así como protegerse y controlarse.

Control de Acceso al Código Fuente de los Programas.

Control

Se debería restringir el acceso al código fuente de los programas.

Seguridad en los Procesos de Desarrollo y Soporte

Objetivo: mantener la seguridad del software y de la información del sistema de aplicaciones.

Los entornos de soporte y desarrollo deberían estar estrictamente controlados.

Los directores responsables de los sistemas de aplicación también deberían ser responsables de la seguridad del entorno del proyecto del soporte. Ellos deberían garantizar que todos los cambios propuestos en el sistema se revisan para comprobar que no ponen en peligro la seguridad del sistema ni del entorno operativo.

Procedimientos de Control de Cambios

Control

Se debería controlar la implementación de cambios utilizando procedimientos formales de control de cambios.

Revisión Técnica de las Aplicaciones Después de los Cambios en el Sistema Operativo

Control

Cuando se cambian los sistemas operativos, las aplicaciones críticas para el negocio se deberían revisar y someter a prueba para asegurar que no hay impacto adverso en las operaciones ni en la seguridad de la organización.

Restricción en los Cambios a los Paquetes de Software

Control

Se debería desalentar la realización de modificaciones a los paquetes de software, limitarlas a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.

Fuga de Información

Control

Se deberían evitar las oportunidades para que se produzca fuga de información.

Desarrollo de Software Contratado Externamente

Control

La organización debería supervisar y monitorear el desarrollo de software contratado externamente.

Gestión de la Vulnerabilidad Técnica

Objetivo: reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica se debería implementar de forma eficaz, sistemática y repetible con toma de mediciones para confirmar si eficacia. Estas consideraciones deberían incluir a los sistemas operativos y otras aplicaciones en uso.

Control de las Vulnerabilidades Técnicas

Control

Se deberían obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.

2.9 Gestión de los Incidentes de la Seguridad de la Información

Reporte Sobre los Eventos y las Debilidades de la Seguridad de la Información

Objetivo: asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.

Es conveniente establecer el reporte formal del evento y los procedimientos de escalada. Todos los empleados, contratistas y usuarios de tercera parte deberían tener conciencia sobre los procedimientos para el reporte de los diferentes tipos de evento y las debilidades que puedan tener impacto en la seguridad de los archivos de la organización. Se les debería exigir que reporten todos los eventos de seguridad de la información y las debilidades tan pronto sea posible al punto de contacto designado.

Reporte Sobre los Eventos de Seguridad de la Información

Control

Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados tan pronto como sea posible.

Reporte Sobre las Debilidades de la Seguridad

Control

Se debería exigir a todos los empleados, contratistas y usuarios de tercera partes de los sistemas y servicios de información que observen y reporten todas las debilidades observadas o sospechadas en los sistemas o servicios.

Gestión de los Incidentes y las Mejoras en la Seguridad de la Información

Objetivo: considerar que se aplica un enfoque consistente y eficaz para la gestión de los incidentes de seguridad de la información.

Es conveniente establecer las responsabilidades y los procedimientos para manejar los eventos y debilidades de la seguridad de la información de manera

eficaz una vez se han reportado. Se debería aplicar un proceso de mejora continua a la respuesta para monitorear, evaluar y gestionar en su totalidad los incidentes de seguridad de la información.

Cuando se requiere evidencia, esta se debería recolectar para garantizar el cumplimiento de los requisitos legales.

Responsabilidades y Procedimientos

Control

Se deberían establecer las responsabilidades y los procedimientos de gestión para asegurar una respuesta rápida eficaz y ordenada a los incidentes de seguridad de la información.

Aprendizaje Debido a los Incidentes de Seguridad de la Información

Control

Deberían existir mecanismos que permitan cuantificar y monitorear todos los tipos, volúmenes y costos de los incidentes de seguridad de la información

Recolección de Evidencia

Control

Cuando una acción de seguimientos contra una persona u organización después de un incidente de seguridad de la información implica acciones legales (civiles o penales), la evidencia se debe recolectar, retener y presentar para cumplir con las reglas para la evidencia establecidas en la jurisdicción pertinente.

2.10 Gestión de la Continuidad del Negocio

Aspectos de Seguridad de la Información en la Gestión de la Continuidad del Negocio

Objetivo: contrarrestar las interrupciones en las actividades del negocio y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres, y asegurar su recuperación oportuna.

Se debería implementar un proceso de gestión de la continuidad del negocio para minimizar el impacto y recuperación por la pérdida de activos de organización (la cual puede ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas del equipo y acciones deliberadas) hasta un nivel

aceptable mediante la combinación de controles preventivos y de recuperación. En este proceso es convenientes identificar los procesos críticos para el negocio e integrar los requisitos de la gestión de la seguridad de la información de la continuidad del negocio con otros requisitos de continuidad relacionada con aspectos tales como operaciones, personal, material, transporte e instalaciones.

Las consecuencias de desastres, fallas de seguridad, perdida del servicio y disponibilidad de serbio se debería someter a un análisis del impacto en el negocio. Se debería desarrollar e implementas planes de continuidad del negocio para garantizar la restauración oportuna de las operaciones esenciales. La seguridad de la información debería ser una parte integral de todo el proceso de continuidad del negocio y de otros procesos de gestión en la organización.

La gestión de la continuidad del negocio debería incluir controles para identificar y reducir los riesgos, además del proceso general de evaluación de riesgos, limitar las consecuencias de los incidentes dañinos y garantizar la disponibilidad de la información requerida para todos los procesos del negocio.

Inclusión de la Seguridad de la Información en el Proceso de Gestión de la Continuidad del Negocio.

Control

Se debería desarrollar y mantener un proceso de gestión para la continuidad del negocio en todas las organizaciones el cual trate los requisitos de seguridad de la información necesarios para la continuidad del negocio de la organización.

Continuidad del Negocio y Evaluación de Riesgos

Control

Los aspectos de seguridad de la información en la continuidad del negocio se deberían basar en la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos de los negocios de la organización, por ejemplo fallas de los equipos, errores humanos, robo, desastres naturales y actos terroristas. Se debería continuar con una evaluación de riesgos para determinar la probabilidad y el impacto de tales interrupciones, en términos de tiempo, escalas de daño y periodo de recuperación.

Las evaluaciones de riesgos para la continuidad del negocio se deberían efectuar con la plena participación de los dueños de los recursos y los

procesos de los negocios. Estas evaluaciones deberían considerar todos los procesos del negocio sin limitarse a los servicios de procesamiento de información, sino incluir los resultados específicos para la seguridad de la información. Es importante vincular en conjunto todos los aspectos del riesgo para obtener un panorama completo de los requisitos en conjunto todos los aspectos de los riesgos para obtener un panorama completo de los requisitos de continuidad del negocio de la organización. La evaluación debería identificar, cuantificar y priorizar los riesgos frente a los críticos y los objetivos pertinentes para la organización, incluyendo los recursos críticos, impactos de las interrupciones, duración permitida de corte y prioridad de recuperación.

Dependiendo de los resultados de la evaluación de riesgos, se debería desarrollar una estrategia de continuidad del negocio para determinar el enfoque global para la continuidad del negocio. Una vez se ha creado esta estrategia, la dirección debería aprobarla y se debería crear y respaldar un plan para la implementación de esta estrategia.

Desarrollo e Implementación de Planes de Continuidad que Incluye la Seguridad de la Información

Control

Se debería desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la

escala de tiempo requerido después de la interrupción o la falla de los procesos críticos para el negocio.

Estructura para Planificación de las Continuidades del Negocio

Control

Se debería mantener una sola estructura del los planes de continuidad del negocio, para asegurar quien todos los planes son consistentes, y considerar los requisitos de la seguridad de la información de forma consistente, así como identificar las prioridades para pruebas y mantenimientos.

Pruebas, Mantenimientos y Reevaluación de los Planes de Continuidad del Negocio

Control

Los planes de continuidad del negocio se deberían someter a pruebas y revisiones periodísticas para asegurar su actualización y su eficacia.

2.11 Cumplimiento

Cumplimiento de los Requisitos Legales

Objetivos: evitar el incumplimiento de cualquier ley, de obligaciones estatuarias reglamentarias o contractuales y de cualquier requisito de seguridad.

El diseño, el uso, la operación y la gestión de los sistemas de información pueden estar sujetos a requisitos de seguridad estatuaria, reglamentaria y contractual.

Se debería buscar asesoría sobre los requisitos legales específicos de los asesores jurídicos de la organización o de abogados practicantes calificados. Los requisitos legales varían de un país a otro y pueden variar para la información creada en un país y que se transmiten a otro (es decir, el flujo de datos trans-fronterizo).

Identificación de la Legislación Aplicable

Control

Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deberían definir explícitamente documentar y mantener actualizados para cada sistema de información y para la organización

Derechos de Propiedad Intelectual (DPI)

Control

Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales sobre el uso del material con respecto al cual pueden existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

Protección de los Registros de la Organización

Control

Los registros importantes se deberían proteger contra perdida, destrucción, y falsificación, de acuerdo con los requisitos estatutarios, reglamentarios, contractuales y del negocio.

Protección de Datos y Privacidad de la Información Personal

Control

Se debería garantizar la protección de los datos y la privacidad de acuerdo con la legislación y los reglamentos pertinentes y, sise aplican, con las clausulas del contrato.

Prevención del Uso Inadecuado de los Servicios de Procesamiento de Información

Control

Se debería disuadir a los usuarios de utilizar los servicios de procesamiento de información para propósito no autorizados.

Reglamentos de los Controles Criptográficos

Control

Se debería utilizar controles criptográficos que cumplan todos los acuerdos, las leyes y los reglamentos pertinentes.

Cumplimiento de las Políticas y las Normas de Seguridad y Cumplimiento Técnico

Objetivo: asegurar que los sistemas cumplen con las normas y políticas de seguridad de la organización.

La seguridad de los sistemas de información se debería a intervalos regulares.

Dichas revisiones se deberían llevar acabo frente a las políticas de seguridad apropiadas y se deberían auditar las plataformas técnicas y los sistemas de información para determinar el cumplimiento de las normas aplicables sobre implementación de la seguridad y los controles de seguridad documentados.

Cumplimiento con las Políticas y las Normas de Seguridad

Control

Los directores deberían garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se llevan a cabo correctamente para lograr el cumplimiento con las políticas y las formas de seguridad.

Verificación del Cumplimiento Técnico

Control

Los sistemas de información se deberían verificar periódicamente para determinar el cumplimiento con las normas de implementación de la seguridad

Consideraciones de la Auditoria de los Sistemas de Información

Objetivo: maximizar la eficacia de los procesos de auditoría de los sistemas de información y minimizar su interferencia.

Deberían existir controles para salvaguardar los sistemas operativos y las herramientas de auditoría durante las auditorias de los sistemas de información.

También se requiere protección para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría.

Controles de Auditoría de los Sistemas de Información

Control

Los requisitos y las actividades de auditoría que implican verificaciones de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones de los procesos del negocio.

Protección de las Herramientas de Auditoría de los Sistemas de Información

Control

Se debería proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar su uso inadecuado o ponerlas en peligro.

CAPITULO 3

3. DISEÑO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA RED LAN DEL AREA DE HARDWARE EN LA EMPRESA UNIPLEX SYSTEMS S.A. EN GUAYAQUIL.

3.1. Análisis De La Situación Actual De La Intranet Corporativa

En este capítulo se describirá la infraestructura actual de la red de Uniplex Systems Guayaquil hasta finales de Febrero del 2009, los datos obtenidos son resultado de la información recogida en colaboración del administrador de la red de la Empresa, inventario realizado y revisión de las instalaciones físicas de la red.

Esta información permitirá realizar el análisis de la situación actual de la red en cuanto a seguridad para determinar el punto de partida para la implementación del Sistema de Gestión de Seguridad.

3.1.1. Antecedentes

Uniplex S.A con certificado de calidad ISO:9001 2000 es una sociedad anónima constituida mediante escritura publica otorgada ante la notaria segunda del cantón quito el 18 de noviembre de 1987 aprobada por la superintendencia de compañías el 28 de diciembre de 1987 mediante resolución 87.1.1.102007 al ser una sociedad anónima está sujeta a la ley de compañías para su funcionamiento societario y

demás leyes aplicables a empresas del sector privado, fue creada con el objeto de proveer al mercado informático herramientas y soluciones de alta tecnología para el manejo y distribución de la información. Las principales actividades de Uniplex han sido la Comunicación de Datos, Capacitación en el área informática y Provisión de Soluciones de Software.

Somos representantes de Vanguard MS (antes Motorola MND) desde el nacimiento de la organización, liderando en el mercado ecuatoriano con tecnologías como compresión de datos, módems de alta velocidad, ruteadores multimedia y los protocolos X.25, frame relay, TCP/IP, voz y vídeo sobre IP. En 1998 Uniplex incorpora la distribución de Cisco Systems, Inc. empresa líder mundial en la provisión de soluciones de seguridades de networking para el internet, y, en 2001 la distribución de 3COM, a través de cuyos productos de LAN y telefonía IP complementamos nuestra oferta de soluciones integrales en el área de telecomunicaciones. Por último en el área de telecomunicaciones se ha completado la oferta de productos con la representación de la empresa Allot, lo que nos permite ofrecer servicios y productos relacionados con calidad de servicio en Banda Ancha (QoS).

En Enero del 2000, Uniplex S.A. consolida sus operaciones con la empresa Infopower S.A.. Con esta consolidación, Uniplex S.A. duplica su tamaño, aumentando también así su capacidad de atención y servicio a nuestros clientes. La consolidación con Infopower S.A. fortalece aún más la Unidad de Negocio de Software, incorporando distribuciones importantes como Sybase Inc., Hyperion e IBM Lotus.

Uniplex, en base a los productos mencionados anteriormente, provee soluciones a las siguientes áreas: aplicaciones Internet y Portales, Business Intelligence, Misión Crítica y Alta Disponibilidad, Computación Móvil, Automatización de Procesos y Networking en todas sus líneas (WAN, LAN, multiservicios sobre IP). Proporciona además los servicios de capacitación, consultoría y diseño para las soluciones mencionadas anteriormente. En el área de capacitación técnica, Uniplex es centro de educación de software IBM (ECIS) y centro de educación autorizado de LOTUS (LAEC) y de Sybase (ASEP).

La política de calidad de la empresa es “Servir a nuestros clientes con soluciones corporativas de tecnología de información que potencien su productividad, apoyándonos en personal idóneo y en la mejora continua de nuestros procesos, asegurando así una relación de negocios a largo plazo y de mutuo beneficio.”

Infraestructura de la Red de la Empresa

Ubicación Física de Uniplex Systems

La empresa Uniplex Systems opera en la zona de nueva Kennedy, ubicado en las calles Teodoro Maldonado (antiguamente llamado E) y la Quinta Este con vigilancia las 24 horas del día.

El edificio posee 2 pisos, distribuidos en 3 áreas, las que se encuentran separadas por las escaleras de acceso. Uniplex tiene oficinas en el primer piso y la planta baja. En el primer piso se encuentra la administración, gerencia y el departamento desarrollo de software y en la planta baja se encuentra el departamento técnico de Networking y Cajeros Automáticos. Con respecto a la disposición física de los

servidores de la empresa, estos se encuentran ubicados en la planta baja del edificio, en el Área de equipos de redes que cuenta con una puerta de seguridad para su acceso.

Los pisos ocupados por la Empresa son de concreto, cuentan con cableado estructurado categoría 5e, lo que facilita la administración física de la red.
Cuentan con una red propia de energía eléctrica para los equipos, debidamente separada del cableado de datos.

Estructura de la Red Lan de Uniplex

La red LAN cuenta con 4 servidores, 21 estaciones de trabajo de las cuales 17 son desktop y 4 son portátiles que se encuentran en el edificio, distribuidas por departamentos como se muestra en la figura 3.1, las demás estaciones se encuentran en planta baja.
En el cuarto de servidores se tiene:

- 1 Switch 4226T Superstack3 3Com de 24 puertos, de los cuales actualmente se encuentran 22 puertos utilizados.
- 1 Firewall Route Finder RF600VPN Internet Security Appliance, con 3 puertos para Filtrar paquetes en LAN, WAN y DMZ.
- 1 Central Telefónica IP 3Com con 12 líneas analógicas de las cuales están 8 en uso, y 11 teléfonos IP en uso.

En el área de Hardware se tiene:

- 1 Switch D-Link DES – 1008 D de 8 puertos, de los cuales 5 se encuentran utilizados

La velocidad de transmisión por la red es de 100 Megabits por segundo.

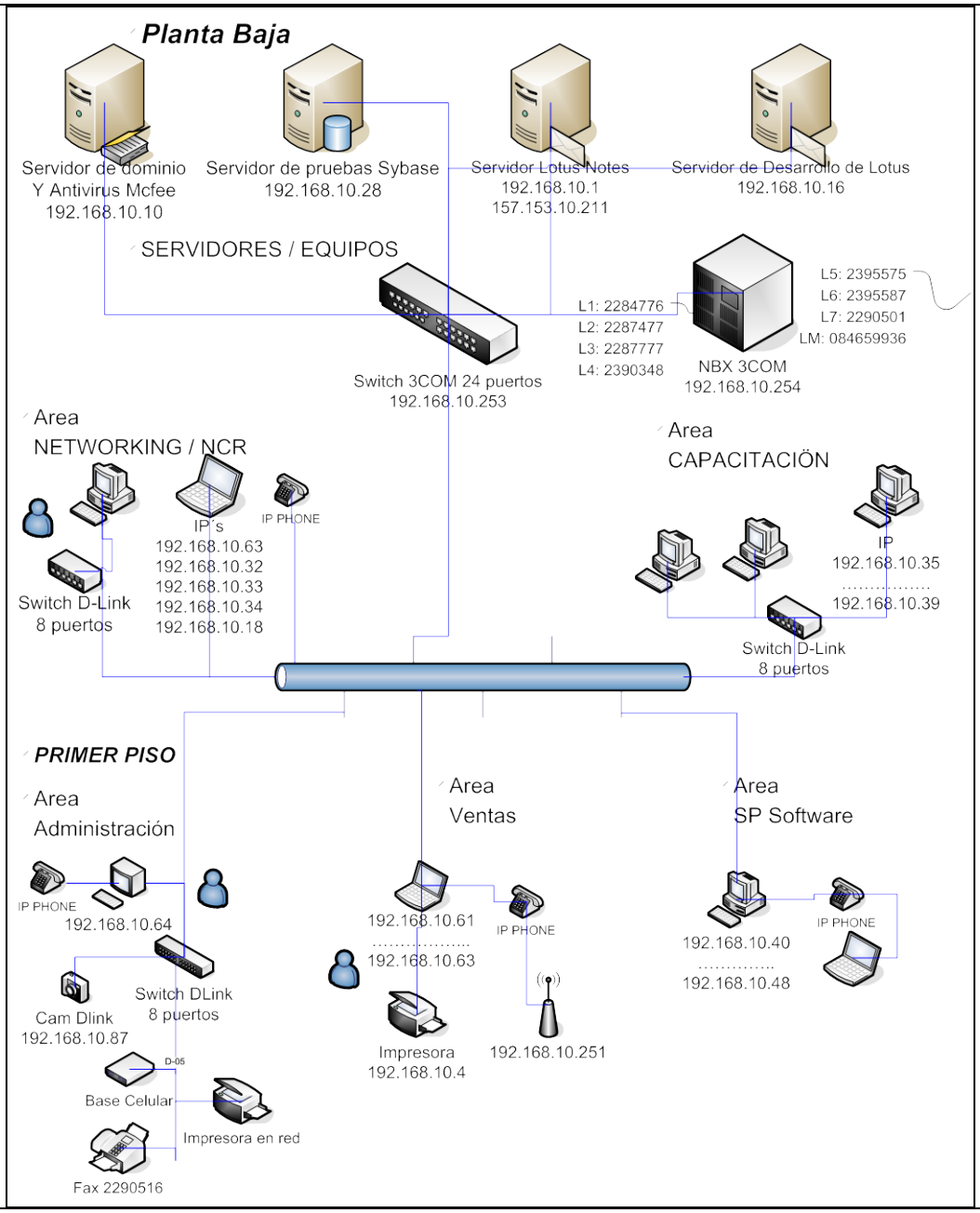


Fig. 3.1 Diagrama de la Red LAN de UNIPLEX

Datos de los Servidores

A continuación se detallan los cuatro servidores con los que cuenta Uniplex:

Base de Datos: Se utiliza como base de datos el software Sybase Adaptive Server Enterprise (ASE) versión 15, con las herramientas: Database Server, PowerBuilder, PowerDesigner, levantado sobre el sistema operativo Windows XP, para efectuar pruebas para clientes, con las siguientes características del hardware:

Aplicación	Base de Datos	
Procesador	Intel® Pentium®	2.66 Ghz
Disco Duro	40 GB	
Memoria	512 Mb de RAM	
Dirección IP	192.168.10.28	
Sistema operativo	Windows xp Service Pack 2	

Tabla 3.1: Características del servidor de Base de Datos

Correo Electrónico y Sistema de Aplicaciones: Se utiliza el sistema Lotus Domino Server 8, con el cual se procesa la mensajería empresarial y las aplicaciones tales como sistema Gestión de Caja, Facturación, Help Desk, Planificación, Biblioteca Electrónica, Enciclopedia Marketing, Sales Automation, Cursos y Calendarios, Vacaciones, Plantilla de Aplicaciones, las cuales son de uso vital y diario entre las sucursales Quito y Guayaquil, las características que tiene el equipo en hardware son:

Aplicación	Lotus Domino Server 8	
Procesador	Intel® Pentium®	2.66 Ghz
Disco Duro	160 GB	
Memoria	512 Mb de RAM	
Dirección IP	192.168.10.1	
Dirección IP WAN	157.100.153.211	
Sistema operativo	Windows xp Service Pack 3	

Tabla 3.2: Características del servidor de Correo y Aplicaciones

Desarrollo de Lotus: Se utiliza el sistema Lotus Domino Server 8, Lotus Domino Admin y Lotus Domino Designer con el cual se crean las diferentes aplicaciones para los proyectos empresariales como workflow, etc, las cuales son de uso vital y diario entre las sucursales Quito y Guayaquil, las características que tiene el equipo en hardware son:

Aplicación	Lotus Domino Admin – Designer 8	
Procesador	Intel® Xeon™	2.8 Ghz
Disco Duro	160 GB	
Memoria	2 Gb de RAM	
Dirección IP	192.168.10.16	
Sistema operativo	Windows 2003 Server Service Pack 2	

Tabla 3.3: Características del servidor de Desarrollo de Lotus

Dominio y Antivirus: Se utiliza como dominio el Active DIrectory del sistema Windows 2003 Server, al cual todas las maquinas efectúan comunicación, además en este servidor también está instalado el antivirus Mcfee centralizado con la consola EpoliceOrchestor, y el software de monitoreo del sistema de vigilancia, las características que tiene el equipo en hardware son:

Aplicación	Windows 2003 Server	
Procesador	Intel® Pentium®	1.7 Ghz
Disco Duro	160 GB	
Memoria	1 Gb de RAM	
Dirección IP	192.168.10.10	
Sistema operativo	Windows 2003 Server Service Pack 2	

Tabla 3.4: Características del servidor de Dominio y Antivirus

En cuanto a instalaciones de parches, no se tiene un procedimiento aprobado para la actualización y mantenimiento de software.

Datos de las Estaciones de Trabajo

Las 21 estaciones de trabajo tienen instalado el antivirus Mcfee client, así como otros antivirus adiciones a criterio de cada usuario, así como Microsoft Office 2003 y Microsoft Office 2007, utilizan como navegador web al Internet a Microsoft Internet Explorer 6.0 y 7.0, Mozilla 3.1, así como otras aplicaciones como Acrobat Reader dependiendo de las capacidades de la máquina. A continuación se detallan las características de los equipos:

CPU	Laptop HP Compaq nx6320
Procesador	Intel® Pentium® 4CPU 2.6 Ghz
Disco Duro	80 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.5: Características de Laptop HP

CPU	Laptop Toshiba Satellite
Procesador	Intel® Celeron® 4CPU 2 Ghz
Disco Duro	80 Gb
Memoria	256 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.6: Características de Laptop Toshiba

CPU	Desktop IBM MT-M 8191-61s
Procesador	Intel® Pentium® 4CPU 2.6 Ghz
Disco Duro	40 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.7: Características de Desktop IBM MT-M

CPU	Desktop IBM Intellistation MPRO
Procesador	Intel® Pentium® 4CPU 1.8 Ghz
Disco Duro	40 Gb
Memoria	256 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.8: Características de Desktop IBM Intellistation

CPU	Desktop IBM Netvista 6790 SB3
Procesador	Intel® Pentium® 4CPU 1.8 Ghz
Disco Duro	60 Gb
Memoria	1 Gb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.9: Características de Desktop IBM Netvista

CPU	Desktop IBM Netvista 6790 SB3
Procesador	Intel® Pentium® 4CPU 1.8 Ghz
Disco Duro	60 Gb
Memoria	1 Gb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.10: Características de Desktop IBM Netvista

CPU	Laptop Lenovo T60 2007-63S
Procesador	Intel® Core™ DUO CPU T2500 2 Ghz
Disco Duro	90 Gb
Memoria	1 Gb 987 Mhz
Sistema Operativo	Windows xp Service Pack 3

Tabla 3.11: Características de Laptop Lenovo T60

CPU	Laptop IBM Thinkpad R50e 1824 BPS
Procesador	Intel® Pentium® 2 Ghz
Disco Duro	80 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.12: Características de Laptop IBM Thinkpad R50e

CPU	Laptop HP 530
Procesador	Intel® Core™ DUO CPU T2600 @ 2.6 Ghz
Disco Duro	120 Gb
Memoria	1 Gb
Sistema Operativo	Windows Vista Service Pack 1 32 bits

Tabla 3.13: Características de Laptop HP 530

CPU	Desktop HP Vectra xE20
Procesador	Intel® Pentium® 4CPU 1.7 Ghz
Disco Duro	40 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.14: Características de Desktop HP Vectra xE20

CPU	Desktop HP Vectra xE20
Procesador	Intel® Pentium® 4CPU 1.7 Ghz
Disco Duro	30 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.15: Características de Desktop HP Vectra xE20

CPU	Desktop HP Vectra xE20
Procesador	Intel® Pentium® 4CPU 1.7 Ghz
Disco Duro	30 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 3

Tabla 3.15: Características de Desktop HP Vectra xE20

CPU	Desktop HP Vectra xE20
Procesador	Intel® Pentium® 4CPU 1.7 Ghz
Disco Duro	40 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.16: Características de Desktop HP Vectra xE20

CPU	Desktop HP Vectra xE20
Procesador	Intel® Pentium® 4CPU 1.7 Ghz
Disco Duro	40 Gb
Memoria	384 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.17: Características de Desktop HP Vectra xE20

CPU	Desktop IBM Netvista 6790 SB3
Procesador	Intel® Pentium® 4CPU 1.8 Ghz
Disco Duro	40 Gb
Memoria	512 Mb
Sistema Operativo	Windows xp Service Pack 3

Tabla 3.18: Características de Desktop IBM Netvista

CPU	Desktop Compaq Deskpro
Procesador	x86 Family 6 Model 6 Stepping AT/AT Compatible
Disco Duro	20 Gb
Memoria	197 Mb
Sistema Operativo	Windows 2000 Service Pack 4

Tabla 3.19: Características de Desktop Compaq Deskpro

CPU	Desktop Compaq Deskpro
Procesador	x86 Family 6 Model 6 Stepping AT/AT Compatible
Disco Duro	20 Gb
Memoria	197 Mb
Sistema Operativo	Windows 2000 Service Pack 4

Tabla 3.20: Características de Desktop Compaq Deskpro

CPU	Desktop Compaq Deskpro
Procesador	Pentium® III Procesor 664 Mhz
Disco Duro	10 Gb
Memoria	192 Mb
Sistema Operativo	Windows xp Service Pack 2

Tabla 3.21: Características de Desktop Compaq Deskpro

Además en la red LAN se encuentran conectadas 2 impresoras de las cuales son HP LaserJet 1200 Series, HP Color LaserJet 2600n, 1 escaner HP Scanjet 3570c, 1 Fax Sharp f0-13S.

Actualmente en la red interna no se encuentra implementado ningún sistema de gestión que permita una administración de la red. Es decir no cuenta con ninguna herramienta de Software, Hardware que permita el monitoreo de la red y el análisis de vulnerabilidades.

Estructura de la Red Wan de la Empresa

Uniplex cuenta con 1 enlace a Internet, 1 Enlace SDSL (sincrónico) de 256/256 Kbps contratado a la compañía Ecuanet y que es utilizado para acceso a las aplicaciones con la sucursal en Quito, y también es utilizado para acceso a la Internet.

Cuenta con 1 módem que es propiedad del proveedor del servicio de Internet. Lo que se encuentra conectado al router Cisco 800 para proveer tanto del servicio de Internet a la red interna como el acceso hacia los servidores en Quito.

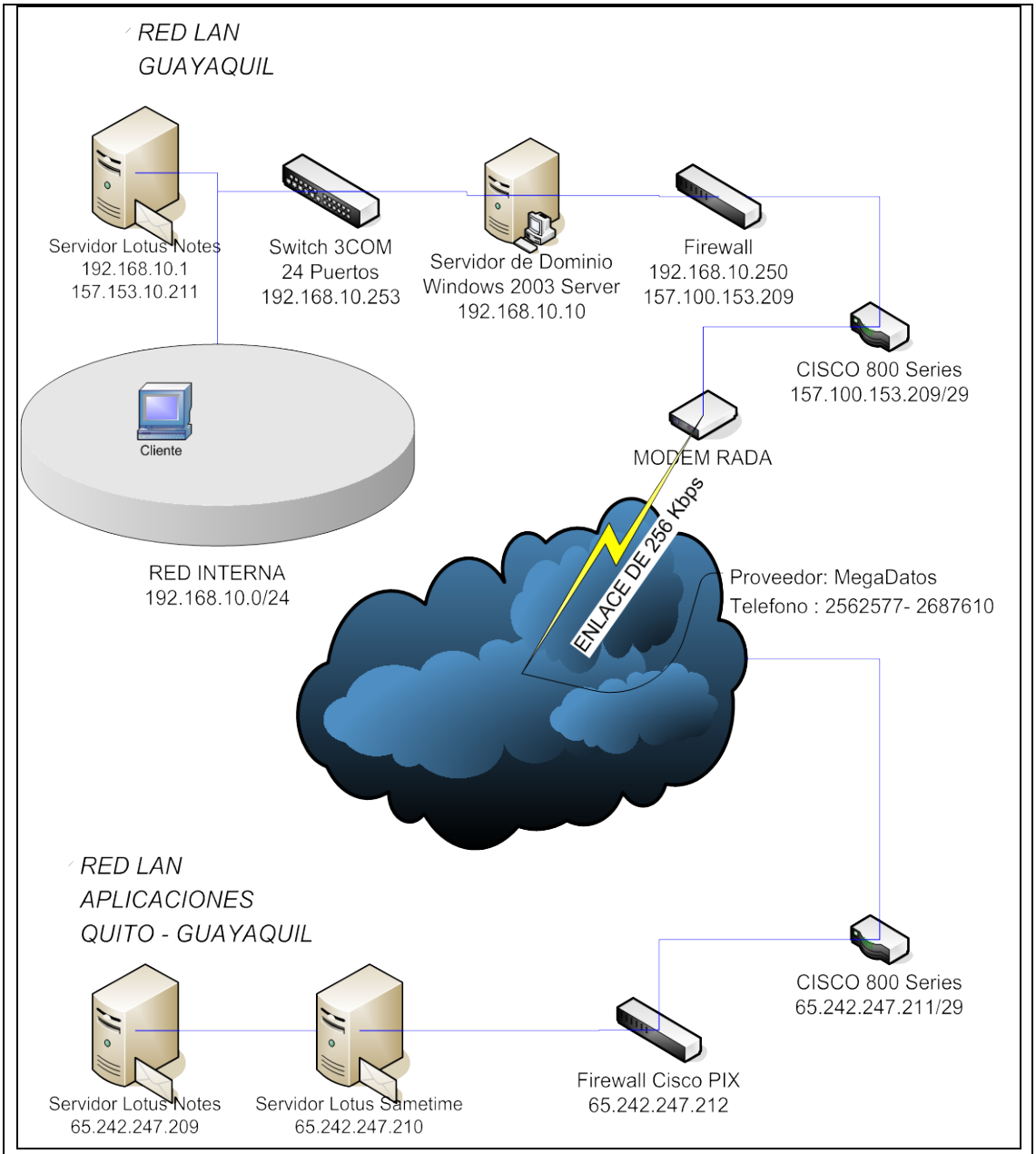


Fig. 3.2 Diagrama de la Red WAN de UNIPLEX

Enlaces de Comunicación

Uniplex cuenta para su funcionamiento con un enlace de Internet, a continuación se da una descripción de cada uno del enlace:

Proveedor:	MEGADATOS – ECUANET
Teléfono:	2562577 – 2687610
Contacto:	Daniel Parra
Ancho de Banda:	ADSL 256/256 kbps Corporativo
Contrato:	No. 6830
Direcciones IP reales:	157.153.100.208/29
Descripción del enlace:	Para uso de conexión a Internet y aplicaciones

Tabla 3.22: Característica del enlace con Ecuanet

Seguridad de la Información Implementada Actualmente en la Empresa

Para Proporcionar Una Visión De La Situación Actual De La Seguridad En El Uniplex, Se Realizó Un Análisis Para Determinar El Grado De Seguridad Y Saber Cómo La Empresa Ha Venido Salvaguardando Las Ventajas Competitivas.

Seguridad de las Comunicaciones

Correo Electrónico

Uniplex cuenta con un sistema único de correo tanto para mail interno como externo, este se encuentra alojado en el servidor interno Lotus Notes que se utiliza para la comunicación con el servidor de Quito el cual es la salida y la entrada de todo el trafico de correo, se encuentra bajo Windows y es administrado a través de Lotus Domino Admin, el mismo que fue configurado

en su momento por un ingeniero de planta y q actualmente es administrado por el Encargado del departamento de software.

Uniplex tiene adquirido en NIC un dominio (uniplex.com.ec), el mismo que es el dominio de todas las cuentas de correo que se crean.

El correo se lee a través de un cliente de correo Lotus Notes 7 u 8 dependiendo de las capacidades de la maquina el cual debe estar instalado en cada una de las maquinas clientes.
La configuración del servidor permite que todos los correos se almacenen en cada una de las maquinas clientes, y que no queden residente en el servidor.

El Lotus Notes se instala con su configuración por defecto y puede ser modificado por el usuario, el que puede modificar las siguientes características:

- Vista previa,
- Confirmación de lectura,
- Preferencias,

Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Gerente del área al que pertenece le avisa al encargado, y éste le crea la cuenta de correo respectiva.

Los empleados no usan el mail solamente para funciones laborales, sino también con fines personales. Es posible ver los mail que se envían y se

reciben a través del administrador, pero actualmente no se realizan controles, de manera que pueden usarlo para cualquier fin.

- **Antivirus**

La empresa adquirió a inicios del 2008 20 licencias corporativas del antivirus Mcfee Virus Scan enterprise Client, con lo cual se tienen protegidas a los servidores (licencia para servidor) y a el numero de maquinas indicadas (licencias Cliente), las otras computadoras (laptops) se mantienen con el avast y con el Nod32. No han existido muchos inconvenientes con virus, a excepción de algunos dispositivos extraíbles.

Desde Internet se actualizan las listas de virus del Mcfee ePoliceOrchestor, el mismo que se actualiza en el Servidor de dominio. Los usuarios no son responsables de actualizar sus propios antivirus ya que desde el servidor se distribuye automáticamente estas actualizaciones hacia los demás clientes. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

No se hacen escaneos periódicos buscando virus en los servidores ni en las PC´s. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable. En algunas máquinas (en las que han tenido problemas frecuentes con virus), cuando el equipo se inicia, entonces comienza un escaneo del antivirus antes del inicio de Windows.

- **Ataques de red**

En la empresa no disponen de herramientas destinadas exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado, hasta el momento, problemas en este sentido. No hay herramientas para detección de intrusos.

No hay controles con respecto a la ocurrencia de Denial of Service. No existen herramientas que lo detecten, ni hay líneas de base con datos sobre la actividad normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

- **Contraseñas**

El archivo de los passwords del sistema se almacena en el directorio activo del servidor de dominio Windows 2003 Server. Se usa encriptación one way (en un solo sentido), de manera que no es posible desencriptar. En el momento del logeo, se encripta la contraseña ingresada por el usuario y se compara ésta contraseña encriptada con el dato almacenado que también está cifrado, si ambos son diferentes el logeo será fallido. Para modificar las passwords, se accede con la clave de administrador a los datos del active directory, por lo que es posible la transacción, también puede cambiar su contraseña el usuario que haya ingresado a su maquina con su clave.

Seguridad de las Aplicaciones

- **Seguridad de Base de Datos y Aplicaciones Empresariales**

En la empresa se utiliza Sybase Adaptive Server Enterprise (ASE) versión 15 para el almacenamiento y la administración de los datos, los cuales están almacenados en su repositorio respectivo de Base de Datos, el cual maneja las seguridades propias, pero exclusivamente se lo utiliza para pruebas de los clientes.

Solo existe una aplicación informática de uso de la empresa, este aplicativo esta formado por algunos módulos como Planificación, Facturación, Vacaciones, Gestión de Caja. HelpDesk, Cursos y Calendarios, Sales Automation, Plantilla de Aplicaciones, Compras, Enciclopedia Marketing, Gesdoc ISO.

El nivel de acceso a cada una de las aplicaciones, se lo realiza a través del Lotus Notes, para el cual hay dos niveles de seguridad, en la primera llamada Proceso de autenticación, donde se registran el user y el password de cada usuario el cual se almacena en un ID único, cuando se dan los accesos respectivos a cada uno de los usuarios del sistema informático, viene el segundo nivel que es el control de acceso a las aplicaciones, los password tienen nivel de seguridad de 128 bits y en cada envío de información a través de la web se hace a través de encriptación y cifrado.

La única persona que puede tener acceso a los archivos de la base de las aplicaciones es el Ingeniero de soporte del área de software y todo aquel que

opere el servidor de aplicaciones (es decir las personas que tengan acceso físico al equipo y con clave).

Los aplicativos que administran la base disponen de recursos suficientes para su funcionamiento, ya que aproximadamente solo el 50% de los recursos del servidor están en uso, el resto está ocioso.

Cada una de las transacciones efectuadas se almacenan en el registro interno del servidor Lotus Domino Server, con lo que se puede determinar entre otras cosas que usuario, desde que maquina y en que fecha realizó alguna transacción.

- **Control de Aplicaciones en PC's**

Actualmente ningún usuario puede instalar aplicaciones en sus equipos, en caso de querer instalar una nueva aplicación se debe dar a conocer la necesidad de la misma y luego solicitar al departamento de networking la instalación respectiva.

No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de las PC's. Solo hay una instalación básica de alguna versión del Windows, Internet Explorer, Antivirus (Mcfee, AVAST, Nod32), solo tienen permisos de impresión a la HP 2600n la maquina de administración.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer y el Microsoft Office. No se buscan Service Packs ni nuevas versiones. No se tiene políticas de actualización de programas.

Solamente el Encargado del departamento de networking es el responsable de las instalaciones en las PC's, para los usuarios existen restricciones con respecto a la instalación de programas. Pueden bajar de la web cualquier aplicación pero no instalarla en su PC.

Cuando se hace un cambio en la configuración del servidor, no se guardan copias de las configuraciones anterior y posterior al cambio, ni se documentan los cambios que se realizan ni la fecha de las modificaciones.

Seguridad Física

- Control de Acceso Físico al Centro de Cómputo

En el momento de la instalación del centro de cómputos no se efectuó un análisis de costo-beneficio para determinar que controles de acceso físico sería necesario implementar.

La sala de equipos se encuentra ubicado en un antiguo cuarto que permanece cerrada con una única llave, de la que es custodio el administrador del sistema, pero la puerta tiene una cerradura muy vieja, por lo que es susceptible de abrir con otros objetos. La sala no dispone de un sistema de detección y extinción de incendios.

La empresa cuenta con guardias de seguridad; que están alertas las 24 horas del día pero no están presentes físicamente, en la noche se activa una alarma perimetral que esta conectada con la red de NAUTISA (empresa de seguridad) la cual brinda atención inmediata en caso de activarse, no hay tarjetas magnéticas de entrada ni llaves cifradas en ningún sector del edificio.

El personal que tiene el acceso permitido al centro de cómputos es el de Networking y Software.

En horas de oficina hay un control de entrada que identifica a los empleados y registra su hora de entrada y de salida. Los controles de acceso son propios de la unidad, no del edificio, que es de uso compartido con otras actividades. No hay ningún control sobre qué hay en el piso de arriba o en el piso de abajo.

- **Control de Acceso a los Equipos**

Dispositivos como disqueteras y lectoras de CD están habilitadas y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos.
No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno.

Una vez que se ha completado la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

Los servidores del centro de cómputos no se apagan en horarios no laborales, debido a que se debe acceder a ellos desde Quito en un horario 365x7x24, permanecen prendidos las 24 horas del día.

- **Estructura del Edificio**

Cuando se construyó el edificio de la empresa, no se tuvo en cuenta el diseño del centro de cómputos y sus condiciones de seguridad. Por este motivo actualmente está ubicado en un antiguo cuarto. Está ubicado en un piso subterráneo, ya que en los pisos superiores se encuentra otras instituciones.

Las paredes externas del centro de cómputos son del mismo tamaño de las paredes de todo el piso, existe una puerta pequeña de madera.

- **Dispositivos de Soporte**

En la empresa disponen de los siguientes dispositivos para soporte del equipamiento informático:

- Aire acondicionado para el centro de cómputo: la temperatura se mantiene entre 19ºC y 20ºC. solo para esta área, con el fin de mantener esta temperatura todos los días.

- UPS: (Uninterruptible Power Supply) en el centro de cómputos hay un ECM en serie que pueden mantener los servidores y equipos de comunicación funcionando por aproximadamente 1 hora.

- Descarga a tierra: Existe una conexión a tierra que funcionan como descarga para el edificio.

- Cableado Estructurado

La instalación del cableado fue hecha por personal propio, y se implementó un cableado estructurado. Para diagramar los canales de red se tuvieron en cuenta los posibles desastres como inundación, cortes eléctricos, problemas de desagües o campos magnéticos.

El cableado se lo realiza a través de canaletas que se ubican en el contorno de cada una de las paredes por donde tienen que pasar los cables, estas canaletas, se utilizan además perfiles de aluminio en algunas áreas. Estos paneles no son prácticos a la hora de hacer modificaciones en el cableado, debido a la cantidad de cables que pasan por ellos y al poco espacio con el que cuentan, pero resultaron económicos y son seguros en cuanto no es fácil desarmarlos.

En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además no hay distancias grandes recorridas con cables UTP.

Administración del Centro de Computo

- Responsabilidad del equipo de sistemas

No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un responsable general del área de Tecnologías de Información y Comunicaciones, que es el Encargado de TIC (Networking). Él es el que planifica y junto con el jefe de software delega las tareas a los demás empleados del área de sistemas/redes, generalmente una vez por semana haciéndolo responsable de sus propios tiempos.

El administrador es el encargado de reportar a los jefes de área sobre las actividades en el área de TIC. Estos reportes generalmente se realizan a modo de auto evaluación ya que no son un pedido de ningún directivo.

- Mantenimiento

- Solicitud de mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de tecnologías, se comunican telefónicamente con el Ing. de networkig explicando su situación. Cada requerimiento no se registra en un documento.

- Mantenimiento preventivo: Este trabajo es realizado por el personal del área de Networking previamente planificado.

- Clasificación de datos y hardware: los equipos de la empresa no han sido clasificados formalmente según su prioridad, aunque se puede identificar que las máquinas que están en el sector de administración tienen mayor

prioridad que el resto. En la escala siguen las de gerencia, y por último el resto de las PC´s, en cuanto al orden de solución de problemas.

- Rótulos: Actualmente existe un inventario detallado de las características de los equipos de computación.

- Instaladores

Los instaladores de las aplicaciones utilizadas en la empresa se encuentran en sus CD´s originales almacenados en un armario del centro de cómputos, y no disponen de instaladores en disquetes.

- Licencias

Están actualmente licenciados 21 equipos con Windows XP, 1 con Windows vista, 3 equipos con Windows 2003 Server y 25 equipos con Microsoft Office 2003. Se adquirieron las licencias de Lotus Domino Server y Lotus Domino Client, y de las herramientas de desarrollo.

- Backup

- Backups de datos en los servidores:

  Cuando se hace un cambio en la configuración del servidor, no se guardan copias de las configuraciones anterior y posterior al cambio, ni se documentan los cambios que se realizan ni la fecha de estas modificaciones.

No hay ningún procedimiento formal para la realización ni la recuperación de los backups. Además no se realizan chequeos para comprobar que el funcionamiento sea el correcto.

- Backups de datos en las PC's:

  Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de los empleados.

  Si hacen un backup deberían hacerlo en sus propias máquinas o en elementos de almacenamiento.

- Documentación

En el centro de cómputo existe documentación sobre:

- Licencias del software, y en qué máquinas está instalado.
- Números IP de las máquinas y de los equipos de comunicación.
- Gráficos de la ubicación física de los equipos de las distintas áreas.

No hay backups de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

Existe un plan de contingencia elaborado por la empresa desarrolladora del software, pero no se ha realizado la implementación del mismo.

3.2. Establecimiento de Requerimientos del PGSI

Para el establecimiento de los requerimientos del PGSI es necesario determinar la estructura organizacional de la Empresa, para de esta forma identificar los procesos críticos de la misma, así como las diferentes entidades que influyen de alguna manera, luego de entender los procesos de la organización se puede definir el alcance del PGSI dependiendo de la realidad de la empresa.

Estructura Organizacional por Procesos de Uniplex

Para tener una visión clara del alcance del establecimiento de PGSI es indispensable comprender la estructura organizacional de la empresa, para más adelante identificar los activos más importantes en base a los objetivos del negocio y su criticidad, tal como recomienda la norma ISO 27002:2008.

A continuación de detalla la estructura organizacional por procesos de la empresa y las funciones respectivas de cada proceso y subproceso, así como las organizaciones externas a UNIPLEX:

Proceso “Gestión de Recursos Humanos:

EVALUACIÓN DE LA ENTREVISTA AL ASPIRANTE
VERIFICACIÓN DE REFERENCIAS DE PERSONAL
SOLICITUD DE EMPLEO
REGISTRO DE DOCUMENTACIÓN Y PROCESO DE PERSONAL
EVALUACIÓN DE COMPETENCIAS Y DESEMPEÑO DEL PERSONAL

REGISTRÓ DE INDUCCIÓN DE PERSONAL
CARTA DE OFERTA
EFICACIA DE CAPACITACIÓN
MANUAL DE FUNCIONES
MANUAL DE EVALUACIÓN DEL PERSONAL
CATALOGO DE COMPETENCIAS
PLAN DE ENTRENAMIENTO Y COMPETENCIAS
NOMINA DE PAGO

Proceso “Gestión de Calidad”

DOCUMENTOS INTERNOS
CONTROL DE CAMBIOS
DOCUMENTOS EXTERNOS
ELIMINACIÓN DE DOCUMENTOS
RESPONSABLES

Proceso “Administración de Infraestructura Tecnologica”

ADMINISTRACIÓN DE LA RED DE DATOS Y USUARIOS
MANTENIMIENTO DE LA SEGURIDAD Y LA DISPONIBILIDAD DE LA INFORMACIÓN
MANTENIMIENTO DEL SITIO WEB DE UNIPLEX
OBTENCION Y RESTAURACION DE RESPALDOS LOTUS
OBTENCION Y RESTAURACION DE RESPALDOS SPYRAL
ADMINISTRACION DE ANTIVIRUS
CREACION DE CUENTAS Y USUARIOS
PLAN DE MANTENIMIENTO DE EQUIPOS

Proceso “Capacitación”

REALIZACIÓN DEL CURSO
PARA EL CASO DE LOTUS
PARA EL CASO DE NETWORKING
PLANIFICACION SP
CONFIGURACION DE SOLUCIONES SP
CONTRATO DE PRESTACION DE SERVICIOS PROFESIONALES
MATRIZ DE INDICADORES DE SEGUIMIENTO
POLITICA DE COMPRA DE MANUALES DE CAPACITACION

Proceso “Compras e Importaciones”

EVALUACIÓN DE PROVEEDORES
EL PROCESO DE COMPRAS
SELECCIÓN DE NUEVO PROVEEDOR
SELECCIÓN DE NUEVO PROVEEDOR DE SERVICIOS PROFESIONALES
LISTADO DE PROVEEDORES CALIFICADOS
TABLA DE AUTORIZACIONES
CONTRATO DE PRESTACION DE SERVICIOS PROFESIONALES
SEGUIMIENTO DE IMPORTACIONES
CUENTAS POR PAGAR
SELECCIÓN DE NUEVOS PROVEEDORES
REQUERIMIENTO INTERNO DE GASTOS

SOLICITUD DE CHEQUE
DIAGRAMA DE CONTROL DE DESEMPEÑO
APLICACIÓN DE COMPRAS E IMPORTACIONES

Subproceso “Compras”

RI Y NOTA DE PEDIDO
COMPRAS LOCALES
REQUISITOS GENERALES PARA UNA COMPRA *DE PRODUCTOS Y SERVICIOS PARA USO INTERNO*
CONTRATACIÓN DE SERVICIOS PROFESIONALES O DE INSTRUCTORES DE CAPACITACIÓN
IMPORTACIONES
VERIFICACIÓN DEL PRODUCTO COMPRADO

Proceso “Configuración de soluciones SP”

RESPONSABLES
DESCRIPCIÓN
BASE DE CONOCIMIENTOS (CARPETA TÉCNICA DEL CLIENTE DE SERVICIOS PROFESIONALES)
PLANIFICACIÓN DE LA CONFIGURACIÓN DE SOLUCIONES
DEFINICIÓN DE ENTRADAS
DISEÑO Y DESARROLLO
REVISIÓN DE AVANCE
VERIFICACIÓN
VALIDACIÓN – PRUEBAS DE ACEPTACIÓN
RESULTADOS DEL DISEÑO Y DESARROLLO
CONTROL DE SOLICITUD DE CAMBIOS

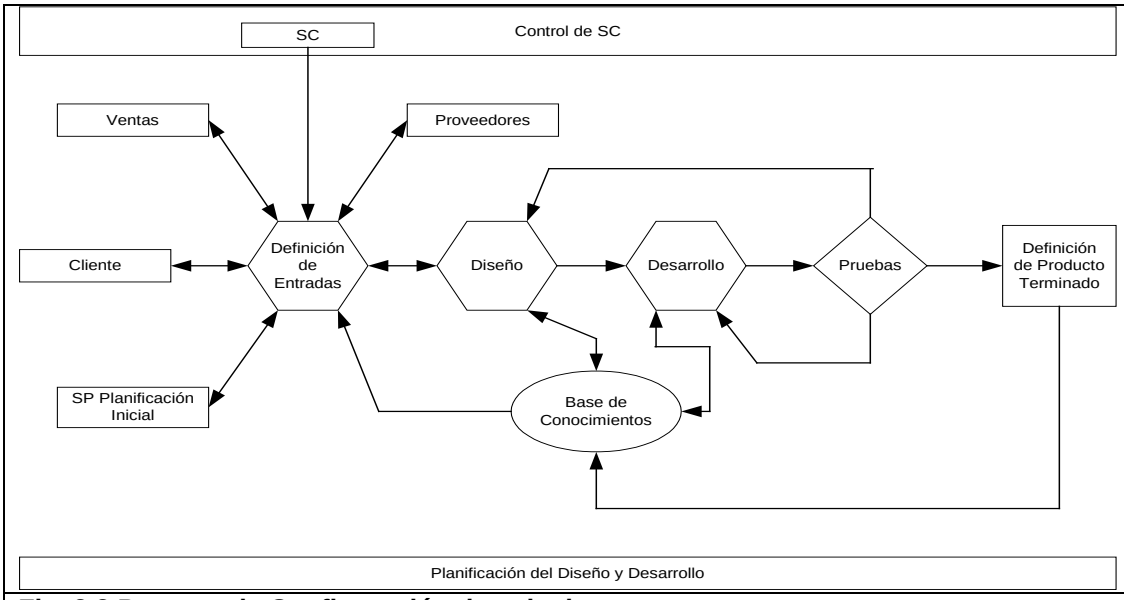


Fig. 3.3 Proceso de Configuración de soluciones

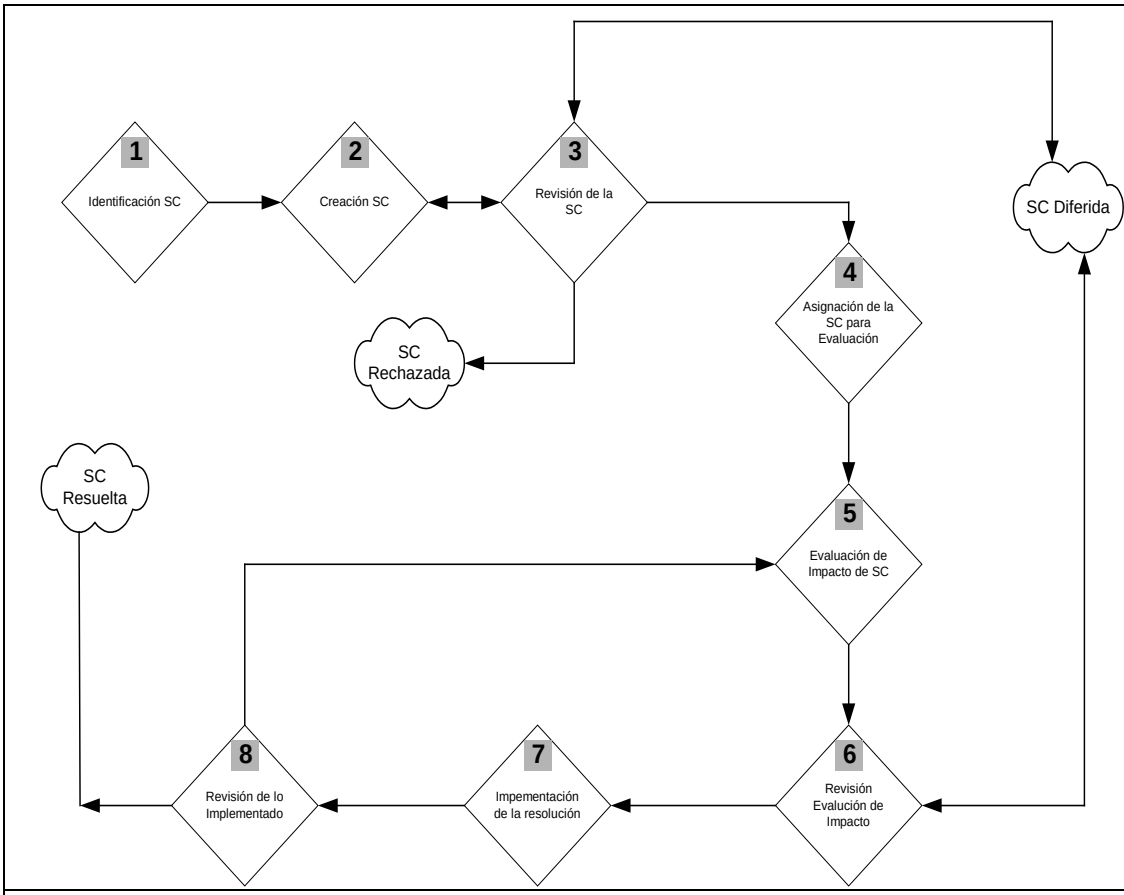


Fig 3.4: Control de solicitud de cambios

Subproceso “Gestión de bodega y facturación”

INGRESO A BODEGA
NOTA DE PEDIDO
NOTA DE ENTREGA
DISTRIBUCION FISICA DE BODEGA
NOTA DE INGRESOS DE EQUIPOS DE CLIENTES

Subproceso “Prestamos de productos HW y SW”

DISTRIBUCION FISICA DE BODEGA
NOTA DE PRESTAMO SW *Y HW*
CONTRATO DE EVALUACION DE SOFTWARE

Proceso “Gestión de cobranzas”

CONTROL Y SEGUIMIENTO DE COBRANZAS
CUANDO LA COBRANZA ES CON FACTURA
CUANDO SE RECIBE ANTICIPOS PREVIOS A LA FACTURACIÓN

Subproceso “Implantación y Soporte SP”

SOPORTE TÉCNICO
IMPLANTACION DE CONFIGURACION DE SOLUCIONES
PREPARACIÓN DEL AMBIENTE DE PRODUCCIÓN
INSTALACIÓN
INDUCCIÓN
SEGUIMIENTO
CIERRE DE LA INSTALACIÓN
MANEJO DE PRODUCTO NO CONFORME
IMPLANTACION DE SOLUCIONES LOTUS
IMPLANTACION DE SOLUCIONES NETWORKING
IMPLANTACION DE SOLUCIONES SYBASE
REPARACION DE EQUIPOS
CONTROL DE REGISTRO DE LLAMADAS DE SOPORTE
REGISTRO DE HORAS DE SOPORTE
INFORME TECNICO DE SOPORTE
INFORME DE ACTIVIDADES

Subproceso “Soporte Técnico para Autoservicio”

DEFINICIONES
RESPONSABLES
MANTENIMIENTO CORRECTIVO
MANTENIMIENTO PREVENTIVO
INSTALACIÓN DE EQUIPOS
FORMULARIO INFORME TÉCNICO
REPARACION DE PARTES DE CAJEROS AUTOMATICOS
MANTENIMIENTO PREVENTIVO DE CAJEROS AUTOMATICOS

Proceso “Planificación SP”

CAPACITACIÓN
SERVICIOS
SOPORTE PRE VENTA
SOPORTE TÉCNICO Y SOPORTE POST VENTA
CONFIGURACIÓN DE SOLUCIONES SOFTWARE Y NETWORKING
ENTRENAMIENTO A USUARIOS
PRODUCTOS A ENTREGAR
DURACIÓN DEL PROYECTO
COSTO DEL PROYECTO
USO DE HELPDESK

Subproceso “Configuración de soluciones software y networking”

ANTECEDENTES
ALCANCE
OBJETIVOS
RELEVAMIENTO DE INFORMACIÓN Y DETERMINACIÓN DE REQUERIMIENTOS
ELABORACIÓN DE DOCUMENTO DE ESPECIFICACIONES FUNCIONALES
INSTALACIÓN, PRUEBAS DE ACEPTACIÓN Y PUESTA EN MARCHA

Proceso “Ventas”

PROSPECCIÓN
ELABORACIÓN DE PROPUESTAS
CIERRE DE VENTA Y PEDIDOS
SEGUIMIENTO PARA ENTREGA DE PRODUCTOS
COMUNICACIÓN CON EL CLIENTE
PRODUCTO NO CONFORME
REPARACIÓN DE PRODUCTOS
PRÉSTAMO DE EQUIPOS
MANEJO DE VENTAS
NOTA DE PEDIDO (SISTEMA LOTUS)
ENCUESTA DE SATISFACCION DEL CLIENTE
SISTEMA SALES AUTOMATION
SISTEMA DE CLIENTES DE FILEMAKER
SISTEMA DE CONTROL DE OPORTUNIDADES DE FILEMAKER
APROBACION DE PRECIOS

Subproceso “Manejo de Ventas”

DISTRIBUCIÓN DE CUENTAS
SEGUIMIENTO DE VENTAS
PLAN DE NEGOCIOS
MEDICIÓN DE SATISFACCIÓN DEL CLIENTE

ORGANIZACIONES EXTERNAS A UNIPLEX

Clientes

Los clientes pueden ser considerados de dos maneras:

1. Con contrato de mantenimiento, aquellos que tienen una trayectoria de negocios con la empresa y que tienen en vigencia un contrato de Stand BY.
2. Soporte y Nueva adquisición, empresa que desea iniciar negocios con nosotros o aquellas que contratan para asuntos puntuales.

Prestadores de Servicios

Se refiere a las instituciones o empresas que dan servicios de mantenimiento, por ejemplo: Limpieza y reparación de aires acondicionados, etc.

Proveedores de Internet

Empresas que prestan el servicio de Internet, para este caso, es: Ecuanet.

Definición del Alcance del PGSI de Uniplex

Una vez que ya se tienen identificados los procesos que forman parte de la empresa, se determinará el alcance del PGSI en base a un método que brinde una identificación clara de las dependencias, relaciones entre las divisiones, áreas, procesos de la organización. Para nuestro caso seleccionamos un método sencillo pero preciso como es el método de las eclipses, en el cual se deben definir identificar los procesos principales de la organización, así como las

organizaciones internas y externas a los mismos, y la relación de estas con los procesos. En base a esto identificamos los procesos principales a los siguientes:

- Procesos Gerenciales
- Procesos Operativos
- Procesos de apoyo

El segundo paso de este método es identificar la eclipse intermedia las distintas interacciones que los subprocesos de la eclipse concéntrica tienen con otros procesos de la empresa. El objetivo es identificar a los dueños de esos procesos y los activos de información involucrados en el eclipse concéntrico, para determinar cuales son los recursos indispensables para que la empresa pueda cumplir con sus objetivos de negocio.

En la eclipse externa se identifican aquellas organizaciones extrínsecas a la empresa que tienen cierto tipo de interacción con los subprocesos identificados. Las flechas indican la interacción. Aquí también se deben identificar los distintos tipos de activos de información, con el objetivo de averiguar el tipo de acuerdos que se debe establecer con las terceras partes.

Esta información se obtiene del siguiente diagrama:

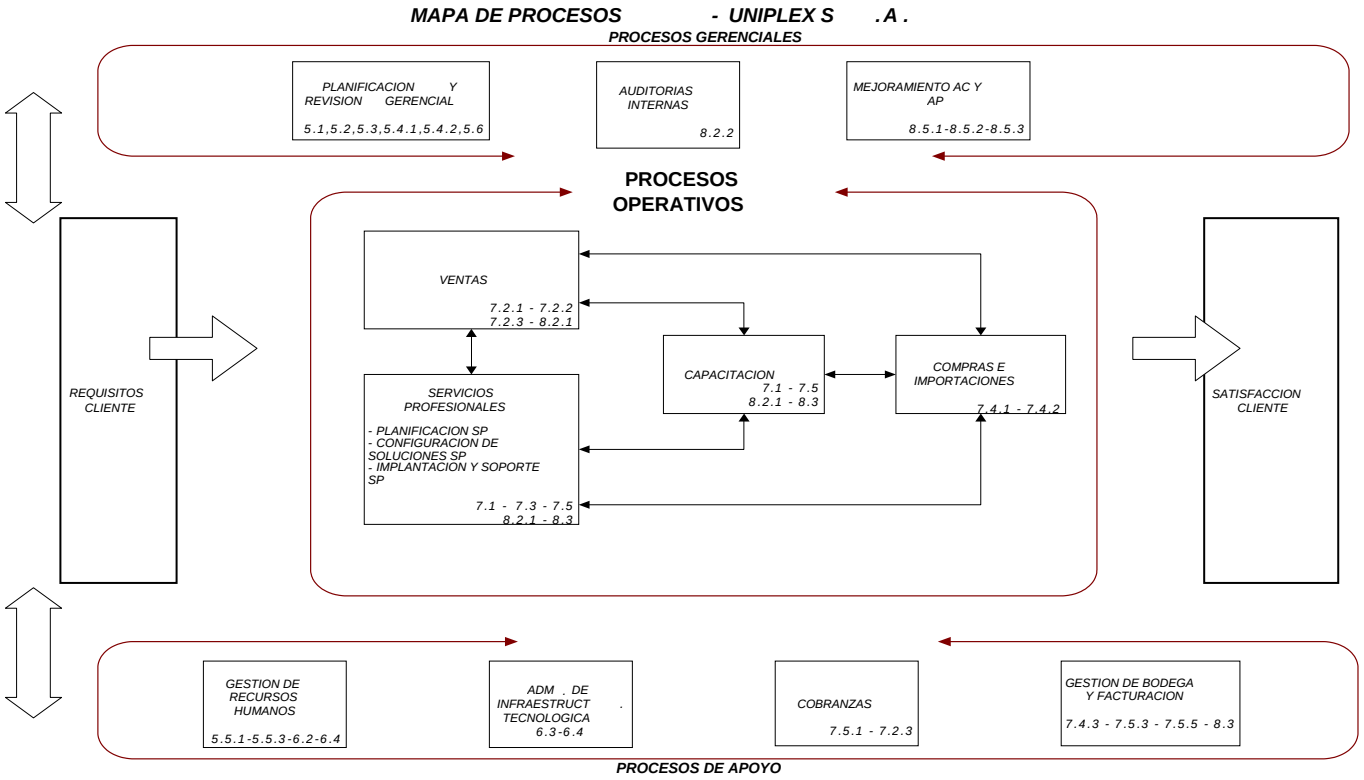


Fig 3.5: Mapa de Procesos de UNIPLEX

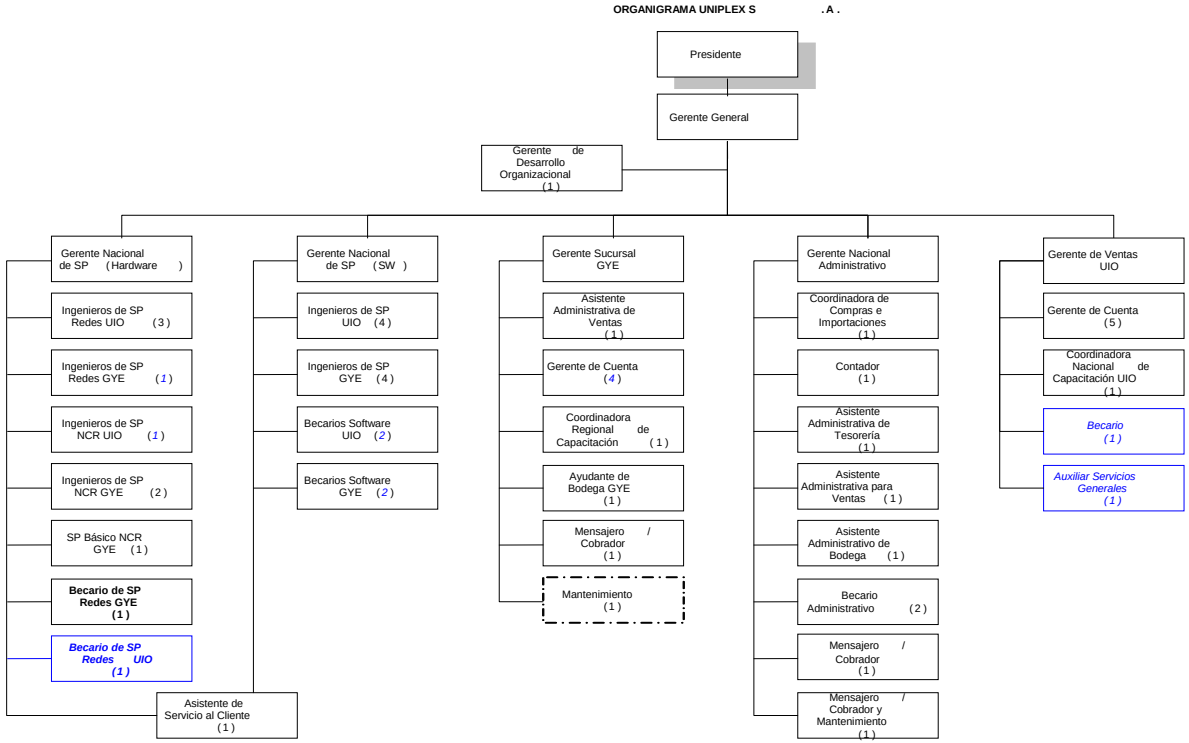


Fig 3.6: Organigrama de UNIPLEX

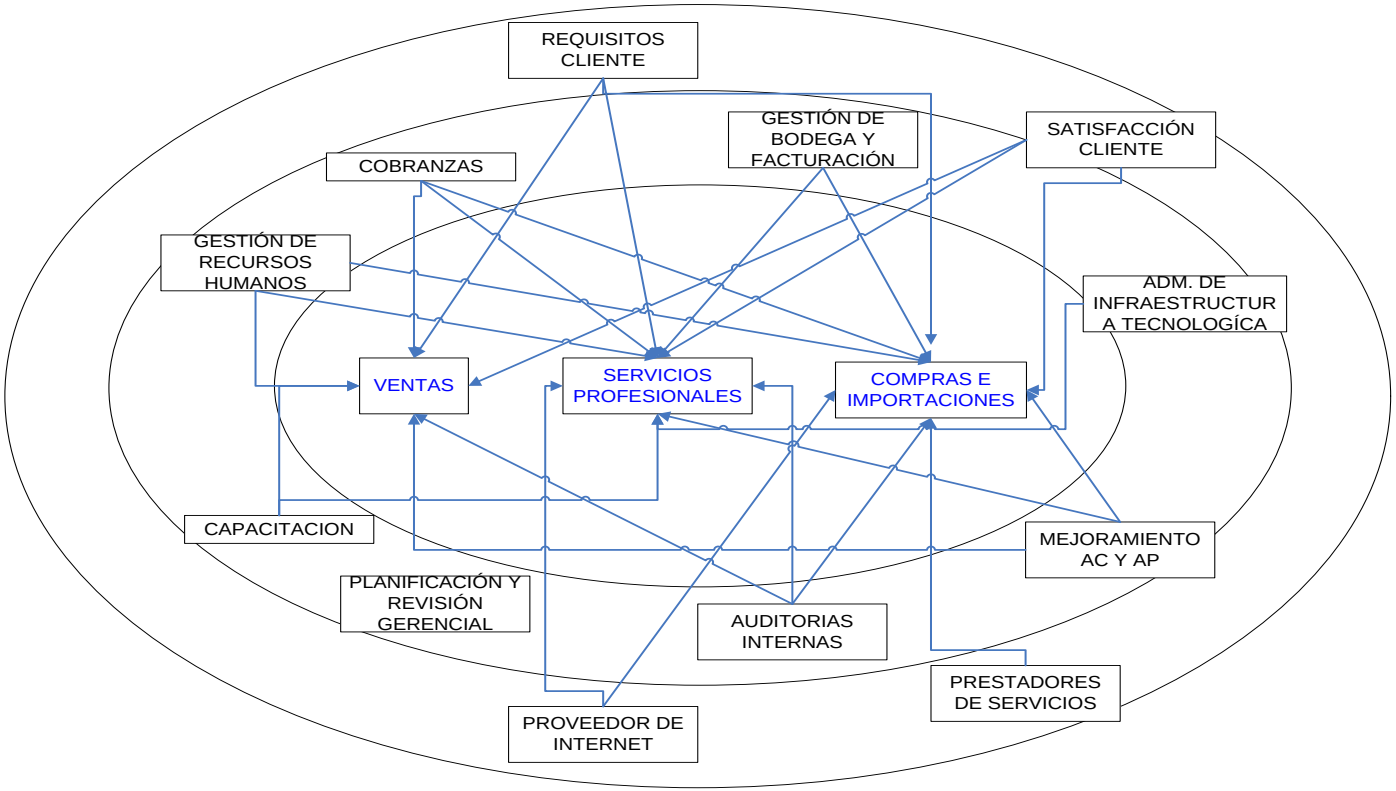


Fig. 3.7: Método de las eclipses para los procesos de UNIPLEX

3.3. Identificación, Análisis Y Evaluación de Vulnerabilidades en la Intranet Corporativa

Previa la identificación, análisis y evaluación de vulnerabilidades es necesario realizar una revisión de varias metodologías de riesgos para seleccionar la más adecuada acorde la realidad de la empresa y de esta manera analizar las vulnerabilidades actualmente presentes en la Corporación. A continuación se detallan algunas metodologías:

Metodología de Riesgos

Hay varios métodos para realizar el análisis de riesgos, cada método tiene sus propias características, así como sus ventajas y desventajas. Es necesario comprender los diferentes métodos y sus ventajas y desventajas para seleccionar un método de análisis de riesgos que se ajuste a las características de la empresa.

- ISO 13335-1:2004
- ISO73
- AS 4360 (Australia)
- NIST SO 800-30 (USA)
- MAGERIT 2.0 (España)
- EBIOS (Francia)
- OCTAVE (Cert)
- GMITS

A continuación realizamos una breve descripción de algunos de estos métodos:

- **MAGERIT**

MAGERIT es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas promovida por el Consejo Superior de Informática. MAGERIT define los procedimientos para guiar a la Administración paso a paso en el establecimiento de la protección necesaria y como respuesta a su dependencia creciente respecto de las técnicas electrónicas, informáticas y telemáticas. Los objetivos:

“Analizar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. El análisis de riesgos permite identificar las amenazas que acechan a los distintos componentes pertenecientes o relacionados con el sistema de información (conocidos como "activos"), para determinar la vulnerabilidad del sistema ante esas amenazas y para estimar el impacto o grado de perjuicio que una seguridad insuficiente puede tener para la organización. Se obtiene así una medida del riesgo que corre el sistema analizado.

Prevenir, impedir, reducir o controlar los riesgos investigados, mediante la gestión de riesgos.

- **EBIOS (Francia)**

Es una herramienta de gestión de los riesgos, el método EBIOS permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI).

Posibilita también la comunicación dentro del organismo y también con los asociados para contribuir al proceso de la gestión de los riesgos SSI.

También se considera una herramienta de negociación y de arbitraje brindando las justificaciones necesarias para la toma de decisiones (descripciones precisas, retos estratégicos, riesgos detallados con su impacto en el organismo, objetivos y requerimientos de seguridad explícitos).

Una herramienta de concienciación EBIOS permite concienciar a las partes involucradas en un proyecto (dirección general, financiera, jurídica o recursos humanos, diseñador del proyecto, director del proyecto, usuarios), implicar a los actores del sistema de información y uniformizar el vocabulario.

- **OCTAVE (Cert)**

Un equipo pequeño de personas del área operacional y el departamento de tecnologías de la información deberán trabajar juntos para dirigir las necesidades de seguridad de la organización. El equipo utiliza el conocimiento de muchos empleados para definir el estado actual de seguridad, identificación de riesgos para los activos críticos, y el conjunto de estrategias de seguridad.

OCTAVE es diferente de las valoraciones tecnológicas. Enfocada en el riesgo organizacional y estratégico, riesgos operacionales balanceados, prácticas de seguridad y tecnología.

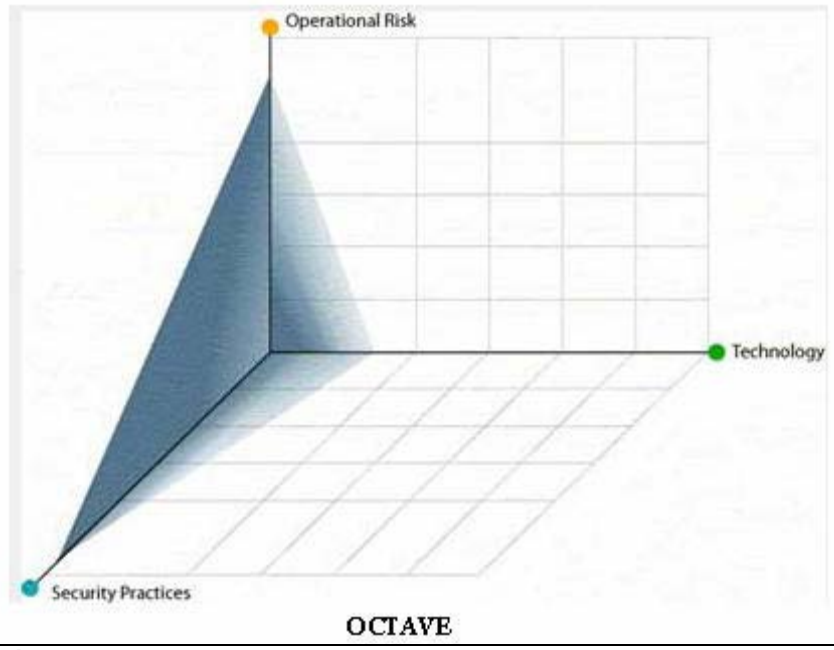


Fig 3.8: Método de Octave

Como se ilustra en la figura 3.8, OCTAVE es manejada por riesgos operacionales y prácticas de seguridad. La tecnología es examinada solo en relación con prácticas de seguridad.

El criterio de OCTAVE define un estándar para el manejo de riesgos, valoración y evaluación de seguridad de información. Actualmente hay dos métodos reconocidos:

- Método OCTAVE- para grandes organizaciones
- OCTAVE-S- para medianas organizaciones

- Guías para la Administración de Seguridad de IT

De acuerdo a las Guías para la administración de seguridad IT (GMITS), se consideran los siguientes métodos para la valoración de riesgos:

1) Acercamiento Básico

2) Análisis de riesgo detallado

3) Acercamiento combinado

4) Acercamiento informal

- **Acercamiento Básico**

La seguridad es manejada sin una valoración de riesgos, se refiere al criterio de seguridad de información general y estándares y guías usadas en una específica empresa.

Características

En vista de que este método es fácil, este puede reducir el tiempo y costo requerido para la valoración de riesgos. Sin embargo, las guías no pueden satisfacer a todas las empresas.

La seguridad es tratada de la misma manera a través de la organización. Este método emplea controles que pueden ser llevados a cabo, permitiendo a la organización reforzar su manejo de seguridad para evitar que se pase por alto los riesgos.

En este procedimiento, los dos siguientes procedimientos son llevados a cabo:

- **Análisis de riesgo detallado**

Los riesgos son evaluados en términos de posibles efectos, amenazas y vulnerabilidades causan la pérdida de confidencialidad, integridad o disponibilidad de los activos de información.

Características

Debido a que en hace en lo posible un correcto análisis de riesgos, este método puede ser usado para seleccionar apropiados controles basados en el riesgo. Sin embargo, la valoración de riesgos toma tiempo y es costoso.

- **Acercamiento combinado**

Generalmente, este método combina el acercamiento básico y el análisis de riesgo detallado.

Características

Este método compensa las ventajas y desventajas de los otros dos métodos.

Sin embargo, si los activos importantes no son propiamente identificados, este método pierde sus ventajas.

- **Acercamiento informal**

Este método involucra un análisis de riesgos basados en la experiencia o en la decisión de la persona responsable.

Características

La desventaja de este método radica en el análisis de riesgos sin aprender nuevas técnicas. Sin embargo, es posible que se cometan errores, o se pasarán por alto procedimientos, en vista de que no hay ninguna estructura.

Elección del Método de Análisis de Riesgos

Para el análisis de riesgos se optó por las: “Guías para la administración de seguridad de IT” con un análisis detallado, ya que este método nos ayuda a cumplir con nuestro objetivo que es seleccionar controles adecuados basados en los riesgos encontrados, es decir este método se ajusta a los requerimientos de la norma ISO 27002.

Escala de Valoración de Riesgos

A continuación se explicará las escalas utilizadas para la valoración del riesgo, el umbral de tolerancia del riesgo y el criterio para este umbral. Para la valoración de riesgos se identificará y evaluará a los activos basados en las necesidades de la

organización. Una organización debería determinar un criterio para la determinación de los tres elementos (confidencialidad, integridad, disponibilidad).

Activos de información (confidencialidad)	Clase	Descripción
1	Pública	Puede ser revelado y proporcionado a terceras partes. Si el contenido fuera revelado, hubiera pequeños efectos en las operaciones de la empresa.
2	Uso Interno	Puede solo ser revelada y proporcionado en Uniplex (no disponible a terceras partes). Si el contenido fuera revelado, no hubiera mucho efecto en las operaciones de la empresa
3	Secreto	Puede ser solo revelado y proporcionado a partes específicas y departamentos. Si el contenido fuera revelado, hubiera un gran efecto en las operaciones de la empresa.
4	Alta confidencialidad	Puede ser solo revelado y proporcionado a partes específicas. Si el contenido fuera revelado, hubiera un efecto irrecuperable en las operaciones de Uniplex.

Tabla 3.23: Estándares para confidencialidad

Activos de información (integridad)	Clase	Descripción
1	No necesaria	Usado solo para consulta. No tiene posibles problemas
2	Necesaria	Si el contenido fuera falsificado, hubiera problemas, pero estos no afectarían mucho las operaciones de Uniplex
3	Importante	Si la integridad se perdiera, hubiera un efecto fatal en las operaciones de la empresa

Tabla 3.24: Estándares para integridad

Activos de información (disponibilidad)	Clase	Descripción
1	Bajo	Si la información no llegara a estar disponible, no hubiera efectos en las operaciones de Uniplex
2	Mediano	Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones de la empresa. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la

		información esté disponible
3	Alto	Si la información no estuviera disponible cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones de Uniplex.

Tabla 3.25: Estándares para disponibilidad

La frecuencia de ocurrencia de las amenazas debe ser evaluada. A partir de la lista de amenazas, las amenazas deben ser revisadas basadas en la experiencia de operaciones y datos estadísticos que han sido ya coleccionados.

Las amenazas son típicamente divididas en tres categorías:

“Baja”,”Media”,”Alta”.

Amenazas		
Probabilidad de ocurrencia	**Clase**	**Descripción**
1	Bajo	Hay una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
2	Medio	Hay una moderada probabilidad. La frecuencia de ocurrencia es una vez cada medio año o menos.
3	Alto	Hay una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más

Tabla 3.26: Criterios para determinar las categorías de las amenazas

Vulnerabilidades		
Probabilidad de ocurrencia	**Clase**	**Descripción**
1	Bajo	Se tiene controles de seguridad muy débiles o no se tiene ningún control de seguridad, de tal manera que esta vulnerabilidad es susceptible de ser explotada fácilmente
2	Medio	Hay un moderado control de seguridad
3	Alto	Si en el activo se tiene los controles de seguridad adecuados, de tal manera que sea muy difícil explotar esta vulnerabilidad

Tabla 3.27: Criterios para determinar las categorías de las vulnerabilidades

Identificación de Activos

Para la identificación de los activos se utilizaron los datos proporcionados por el administrador de la red, y para facilitar el análisis y gestión de riesgos se han

dividido los activos en cinco categorías de información, a continuación se detalla cada una de las cinco categorías:

- **Activos de Información**

Documentos y Registros	
Descripción	Soporte estático no electrónico que contiene datos.
Activos	Actas Documentación de procesos (POA: Plan Operativo Anual) Contratos con los clientes Contratos con los proveedores de servicio médico Facturas Memos Oficios Reglamento del SRI Papel Tarjetas de Afiliación

Activos Auxiliares	
Descripción	Otros dispositivos que ayudan al funcionamiento de la organización
Activos	Suministros de oficina

Activos Intangibles	
Descripción	Activos que representan el buen nombre de la empresa y la imagen que los clientes tienen de ella.
Activos	Imagen y Reputación de la empresa

- **Software**

Sistemas Operativos	
Descripción	Esta denominación comprende todos los programas de una computadora que constituyen la base operativa sobre la cual se ejecutarán todos los otros programas (servicios o aplicaciones). Incluye un núcleo y funciones o servicios básicos. Dependiendo de su arquitectura, un sistema operativo puede ser monolítico o puede estar formado por un micronúcleo y un conjunto de módulos del sistema. El sistema operativo abarca principalmente todos los servicios de gestión del hardware (CPU, memoria, discos, periféricos e interfaces redes), los servicios de gestión de tareas o procesos y los servicios de gestión de usuarios y de sus derechos.
Activos	Windows Server 2003 Enterprise Edition Linux CentOs 4.2 Linux Red Hat 8.0 NBX Resource Pack 5.0 Aptra 3.3.1 Windows XP Profesional SP 2

Paquete de programas o software estándar	
Descripción	El software estándar o paquete de programas es un producto comercializado como tal (y no como desarrollo único o específico) con soporte, versión y mantenimiento. Presta un servicio « genérico» a los usuarios y a las aplicaciones pero no es personalizado o específico como la aplicación profesional.
Activos	Antivirus Mcfee Cliente. Antivirus Mcfee ePolice Orchestor Lotus Notes Lotus Domino Server Microsoft Visio Nero Suite Microsoft Visual Studio Microsoft Project Adobe Illustrator Belarc

Software de aplicación de oficina	
Descripción	Datos y servicios informáticos compartidos y privados, que utilizan los protocolos y tecnologías de comunicación (por ejemplo, tecnología de Internet).
Activos	Aplicación Lotus Notes para acceso a la información de usuarios

- **Activos Físicos**

Hardware Portatil	
Descripción	Hardware informático diseñado para poder ser transportado manualmente con el fin de utilizarlo en lugares diferentes.
Activos	Portátil

PC´s de oficina	
Descripción	Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo.
Activos	Estaciones de trabajo.

Equipos de Oficina	
Descripción	Hardware informático que pertenece al organismo o que es utilizado en los locales del organismo.
Activos	Estaciones de trabajo.

Servidores	
Descripción	Hardware informático que pertenece al organismo y maneja información importante de la empresa y clientes.
Activos	Servidor de Base de datos Servidor de Correo electrónico y aplicaciones Servidor de Dominio y Antivirus Servidor Desarrollo de Lotus

Soporte Electrónico	
Descripción	Soporte informático conectado a una computadora o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos sin modificar su pequeño tamaño. Se utiliza a partir de equipo informático estándar.
Activos	Disquete, CD-ROM, disco duro extraíble, memoria extraíble

Medios de comunicación	
Descripción	Los medios o soportes de comunicación y telecomunicación pueden caracterizarse principalmente por las características físicas y técnicas del soporte (punto a punto, difusión) y por los protocolos de comunicación (enlace o red – capas 2 y 3 del modelo OSI de 7 capas).
Activos	Cableado Estructurado, tecnología Ethernet, cables, Switch, router, MODEM.

Establecimiento	
Descripción	El tipo establecimiento está formado por el conjunto de lugares que contienen todo o parte del sistema y los medios físicos necesarios para su funcionamiento.
Activos	Edificio, oficinas, zona de acceso reservado, zona protegida

- **Servicios**

Comunicación	
Descripción	Servicios y equipo de telecomunicaciones propiedad de la empresa.
Activos	Línea telefónica, central telefónica, redes telefónicas internas.

Energía	
Descripción	Servicios y medios (fuentes de energía y cableado) necesarios para a alimentación eléctrica del hardware y los periféricos.
Activos	Entrada de la red eléctrica.

Correo Electrónico	
Descripción	Dispositivo que permite, a los usuarios habilitados, el ingreso, la consulta diferida y la transmisión de documentos informáticos o de mensajes electrónicos, a partir de computadoras conectadas en red.
Activos	Correo electrónico interno, correo electrónico vía web.

Portal Externo	
Descripción	Un portal externo es un punto de acceso que encontrará o utilizará un usuario cuando busque información o un servicio del organismo. Los portales brindan un gran abanico de recursos y de servicios.
Activos	Portal de información (Página Web de la empresa)

- **Personas**

Personas	
Descripción	Es el personal que manipula elementos delicados en el marco de su actividad y que tiene una responsabilidad particular en ese tema. Puede disponer de privilegios particulares de acceso al sistema de información para cumplir con sus tareas cotidianas.
Activos	Dirección de Recursos Humanos, Dirección Financiera, Administrador del Sistema, Dirección General

Identificación de Requerimientos

Se identificará los requerimientos de los activos de Uniplex en base a los objetivos del negocio, aspectos legales para de esta manera identificar las obligaciones del PGSI. Los requerimientos están determinados con respecto a:

Confidencialidad (C), Disponibilidad (D) e Integridad (I)

- ***ACTIVOS DE INFORMACIÓN***

Los requerimientos de seguridad de la información deberían están enfocados en base a la Confidencialidad, Disponibilidad e Integridad.

- La información no debería ser vista por personal no autorizado (C)
- La información puede ser modificada únicamente por personal autorizado (I)
- La información debería estar disponible en cualquier momento (D)

- ***SOFTWARE***

Si el Software es comercial la confidencialidad no aplica, para software propietario de la organización existe el requerimiento de confidencialidad.

- Las aplicaciones no deberían ser utilizadas por personal no autorizado.(C)
- El software puede ser modificado únicamente por personal autorizado (I)
- El software, en especial aplicaciones deberían estar disponibles al menos durante la jornada laboral (D)

- ***ACTIVOS FÍSICOS***

Para los activos físicos se debe enfocar los requerimientos de hardware, no en la información que procesen, que transmitan o almacenen.

- Los cambios en el Hardware deben ser realizados únicamente por personal autorizado (I)
- El Hardware debe ser accesible por el personal autorizado al menos durante la jornada laboral (D)

- ***SERVICIOS***

Los servicios agrupan información, software y activos físicos, se deben especificar los requerimientos en base a los aspectos más importantes.

- Los servicios deberían ser consistentes y completos (I)
- Los servicios deberían estar disponibles cuando ser requiera (D)

Típicamente la confidencialidad no aplica a servicios, sin embargo depende de la naturaleza del servicio.

- ***PERSONAS***

Para las personas los requerimientos únicamente se enfocan en la disponibilidad de las personas. Por ejemplo:

- El administrador del sistema debe proveer el funcionamiento correcto de los servicios de la red y sistemas (Disponibilidad del personal)

Valoración de los Activos

El objetivo es identificar la valoración de todos los activos dentro del alcance del PGSI, indicando que impacto puede sufrir el negocio con la pérdida de Confidencialidad, Integridad, Disponibilidad.

Para obtener esta valoración, se realizaron conversaciones con el personal encargado de cada proceso; que conocen la importancia de cada activo dentro de la empresa, para así determinar los niveles de Confidencialidad, Integridad y Disponibilidad requeridos para cada proceso, que permitan cumplir con las operaciones del negocio.

ACTIVOS	ELEMENTOS DE INFORMACIÓN	VALOR	RAZÓN

Hardware Portátil	Confidencialidad	3	La información almacenada debe ser vista únicamente por el personal autorizado.
	Integridad	3	Es necesaria la integridad de la información almacenada, en especial cuando es la de clientes
	Disponibilidad	2	Para que los empleados puedan trabajar adecuadamente necesitan acceder a la información, sin embargo pueden recurrir a documentos o servidores donde contengan información
PC´s de oficina	Confidencialidad	3	La información almacenada debe ser vista únicamente por el personal autorizado.
	Integridad	3	Es necesaria la integridad de la información almacenada, en especial cuando es la de clientes
	Disponibilidad	2	Para que los empleados puedan trabajar adecuadamente necesitan acceder a la información, sin embargo pueden recurrir a documentos o servidores donde contengan información
Servidores	Confidencialidad	4	Solo personal específico debe acceder a la información de los servidores debido a que manejan información clientes, proveedores, empleados de la compañía. Para que no la puedan modificar.
	Integridad	3	Es necesario asegurar que la información de los servidores no sea alterada ni modificada sin autorización, para que no se perjudique el negocio
	Disponibilidad	3	Es indispensable que los servidores estén accesibles al menos el 100% en las horas laborables, para no afectar a los clientes, proveedores, inclusive empleados.
Equipos de Oficina	Confidencialidad	2	Información de negocio que se imprima o se fotocopie necesita confidencialidad.
	Integridad	2	Se necesita los equipos de oficina(impresora), pero si eventualmente falla se puede seguir trabajando
	Disponibilidad	2	Si bien son necesarios los equipos, se puede trabajar aunque no estén disponibles
Soporte Electrónico	Confidencialidad	2	Cuando se tenga información de negocio almacenada en estos equipos es necesario su protección
	Integridad	1	Es un medio temporal para almacenar información
	Disponibilidad	1	No es requerido, cuando la información es redundante
			Debido a que la documentación maneja

Documentación y Registros	Confidencialidad	3	información de clientes, proveedores y empleados es necesaria que pueda ser vista por personal autorizado para que no sea modificada.
	Integridad	3	Es necesario que la documentación no sea alterada, ni se produzca pérdidas de la misma debido a que son el único respaldo físico de contratos, procedimientos, etc.
	Disponibilidad	2	Se debe acceder a la información en cualquier momento que sea requerido
Empleados	Confidencialidad	2	Cierta información debe ser manejada al interior de la empresa por lo cual no debe ser divulgada
	Integridad	1	No hay aspectos de integridad relacionados con los empleados
	Disponibilidad	2	Los empleados deben estar disponibles para resolver posibles problemas que se presenten
Establecimiento	Confidencialidad	1	Es un edificio público
	Integridad	3	Se debe proteger la integridad física del edificio Matriz donde se encuentran los servidores
	Disponibilidad	1	Si no pueden acceder al edificio, se puede acceder remotamente a la aplicación del sistema
Servicio de Comunicaciones	Confidencialidad	2	Se debe proteger que las líneas no sean interceptadas para que no se escuchen conversaciones de negocio.
	Integridad	2	Se necesita que los servicios de comunicaciones funcionen adecuadamente
	Disponibilidad	3	Se requiere que estén disponibles, debido a que son necesarias para la comunicación con los proveedores, clientes, reclamos, etc.
Servicio de energía eléctrica	Confidencialidad	1	La entrada de la red eléctrica no requiere confidencialidad
	Integridad	2	La entrada de la red eléctrica no debe sufrir de manipulaciones
	Disponibilidad	3	Para que las operaciones de la empresa sean desarrolladas es importante que esté en funcionamiento la mayor parte del tiempo la entrada de la red eléctrica
Servicio de correo	Confidencialidad	4	Debe tener confidencialidad porque probablemente esté viajando información de Uniplex que debe manejar solo ciertos departamentos y especialmente si la información viaja por una red pública
			Los datos no deben ser modificados, pero en el caso que se pierda la integridad al

electrónico	Integridad	2	utilizar el servicio de correo electrónico, los datos originales podrán ser recuperados
	Disponibilidad	2	El correo electrónico debe estar disponible en horas de trabajo, pero en el caso de que no esté disponible, existen otros métodos que ayudan a solucionar este problema , como servicio de fax, hyperterminal, teléfono, etc.
Aplicación Lotus para acceso a la información del servicio	Confidencialidad	4	Alta confidencialidad porque maneja información personal de los usuarios
	Integridad	3	La aplicación debe mantener la integridad para evitar modificaciones en la información de los clientes.
	Disponibilidad	2	Es importante tener siempre disponible la información de los usuarios, pero si no estuviera disponible en este momento y se la obtuviera después, no afecta críticamente las operaciones de la empresa
Portal de información (Página Web de la empresa)	Confidencialidad	1	El sitio Web debe ser accesible por cualquier persona, en cualquier momento
	Integridad	3	La información presentada en el sitio Web debe ser correcta
	Disponibilidad	3	El sitio Web debe estar disponible a los clientes
Suministros de Oficina	Confidencialidad	1	Es el equipamiento de oficina estándar, no se requiere confidencialidad
	Integridad	2	El equipo de oficina debe trabajar confiablemente, es usado para procesar los registros de los clientes. Cualquier error puede ser reconocido cuando se observa la salida.
	Disponibilidad	1	Los suministro s de oficina durante las horas normal de trabajo, no causa mayor problema si alguna pieza falla, ya que hay impresoras, teléfonos, etc
Imagen de la empresa Reputación	Confidencialidad	1	La confidencialidad no es aplicada en la imagen y reputación de la empresa
	Integridad	1	La integridad no es aplicada en la imagen y reputación de la empresa
	Disponibilidad	1	La disponibilidad no es aplicada en la imagen y reputación de la empresa
Paquetes o software estándar	Confidencialidad	1	Este es un software estándar el cual no es confidencial para todos
	Integridad	2	El software debe funcionar correctamente
	Disponibilidad	2	El software debe estar disponible durante horas de trabajo, pero si hay un problema con un PC, otro PC puede ser usado
	Confidencialidad	4	Los datos de los clientes, que es información personal es procesada en el

Sistemas Operativos			servidor, razón por la cual estos datos deber ser adecuadamente protegidos
	Integridad	3	Los datos de los clientes, que es información personal es procesada en el servidor, estos datos deben ser correctos
	Disponibilidad	3	La continua disponibilidad del servidor es necesaria para un exitoso desempeño de la organización
Medios y Soporte	Confidencialidad	1	El cableado estructurado no requiere confidencialidad
	Integridad	3	El cableado estructurado debe funcionar bien, ya que es parte de la red de la empresa
	Disponibilidad	3	Siempre debe estar disponible ya que probablemente cause la interrupción de actividades propias de la Organización

Tabla 3.28: Valoración de Activos

Identificación de Amenazas y Vulnerabilidades

El objetivo es identificar las amenazas a las que se exponen los activos dentro del alcance del PGSI y las vulnerabilidades que pueden ser explotadas por las amenazas. A continuación detallamos las amenazas principales clasificadas acorde al origen de la misma.

1.- Desastres Naturales.- Sucesos que pueden ocurrir sin intervención humana	
Amenaza: Fuego Daños por agua Desastres Naturales	**Activos:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros
Afecta: Disponibilidad del Servicio, Integridad, Trazabilidad del servicio, Trazabilidad de los datos	

2.- De origen industrial.- Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
Amenaza: Corte de suministro eléctrico Degradación en el HW Condiciones inadecuadas de temperatura y /o Humedad	**Activo:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros
Afecta: Disponibilidad, Confidencialidad, Integridad, Trazabilidad del servicio, Trazabilidad	

de los datos, Funcionamiento y Procesamiento correcto de datos.

3.- Errores y Fallos no intencionados.- Fallos no intencionales causados por las personas.	
Amenaza: Errores de los usuarios Errores de Administración Errores de Configuración Escapes de Información Alteración de información Degradación de información Introducción de Información incorrecta Divulgación de información Errores de actualización Indisponibilidad del personal Incumplimiento con la legislación Corrupción de archivos de registros Brechas de seguridad no detectadas Virus de Computación, Fuerza Bruta y ataques de diccionario	**Activo:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros. Software
Afecta: Disponibilidad del Servicio, Confidencialidad, Integridad, Autenticidad de los usuarios del servicio, Autenticidad del origen de datos, Cumplimiento con regulaciones de seguridad, Trazabilidad del servicio, Trazabilidad de los datos	

4.- Ataques intencionados.- Fallos deliberados causados por las personas.	
Amenaza: Instalación no autorizada o cambios de SW Manipulación de la configuración Brechas de seguridad no detectadas Suplantación de la identidad del usuario. Uso no previsto Abuso de privilegios de acceso Acceso no autorizado Análisis de Tráfico Negación de Servicio Robo Ataque Destructivo Ingeniería Social Inautorizada copia de SW o información Virus de Computación, Fuerza Bruta y ataques de diccionario	**Activo:** Activos Físicos Servicios de Comunicación, Energía Documentación y Registros. Software
Afecta: Disponibilidad del Servicio, Confidencialidad, Integridad, Autenticidad de los usuarios del servicio, Autenticidad del origen de datos, Cumplimiento con regulaciones de seguridad, Trazabilidad del servicio, Trazabilidad de los datos, Plan de Contingencia	

En la siguiente tabla se detallan las vulnerabilidades que se presentan en cada uno de los activos, y las amenazas que pueden explotar dichas vulnerabilidades.

Activos	Amenazas	Vulnerabilidad
Hardware Portátil	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Instalación no autorizada o cambios de Software	Falta de control de acceso
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados
	Uso no previsto	Falta de políticas
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
	Degradación del HW	Falta de mantenimiento adecuado
	Inautorizada copia de SW o información propietaria	Falta de políticas
	Ataque destructivo	Falta de protección física
	Robo	Falta de protección física adecuada
PC´s de oficina	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Instalación no autorizada o cambios de Software	Falta de control de acceso
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados
	Uso no previsto	Falta de políticas
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
	Degradación del HW	Falta de mantenimiento adecuado
	Inautorizada copia de SW o información propietaria	Falta de políticas
	Ataque destructivo	Falta de protección física
	Robo	Falta de protección física adecuada
	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres

Servidores	Corrupción de archivos de registros	Falta de Protección de los archivos de registro
	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Acceso no autorizado a través de la red	Código malicioso desconocido
	Degradación o Falla del HW	Falta de mantenimiento adecuado
	Manipulación de la configuración	Falta de control de acceso
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal
	Incapacidad de restauración	Falta de planes de continuidad del negocio
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores
	Ataque destructivo	Falta de protección física
Equipos de Oficina	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Degradación o Falla de HW	Falta de Mantenimiento
	Ataque destructivo	Falta de protección física
	Uso no previsto	Falta de políticas Falta de control de acceso
Soporte Electrónico	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección Soporte física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad
	Ataque destructivo	Falta de protección física
	Robo	Falta de atención del personal
Documentación y Registros.	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección Soporte física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Pérdida de información	Errores de los empleados Almacenamiento no protegido
	Divulgación de información de clientes	Almacenamiento no protegido
	Incumplimiento de leyes en cuanto a la información de clientes o empleados	Falta de conocimiento de los empleados

	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema
	Contratos incompletos	Falta de control para el establecimiento de contratos
	Ataque destructivo	Falta de protección física
	Incapacidad de restauración	Falta de planes de continuidad del negocio
	Modificación no autorizada de información	Insuficiente entrenamiento de empleados
Empleados	Errores de los empleados y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
Establecimientos	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Acceso no autorizado	Falta de políticas Falta de protección física
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
Servicio de Comunicaciones	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Degradación del servicio y equipos	Falta de mantenimiento adecuado
	Errores de configuración	Falta de conocimiento del administrador
	Manipulación de la configuración	Falta de control de acceso
	Uso no previsto	Falta de políticas
	Ataque destructivo	Falta de protección física
	Fallas de servicios de telefonía	Falta de acuerdos bien definidos con terceras partes
Servicio de energía eléctrica	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Ataques destructivos	Falta de protección física
Servicio de correo electrónico	Errores de los usuarios	Falta de conocimiento del uso del servicio
	Suplantación de la identidad del usuario	Falta de control de acceso
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Uso no previsto	Falta de políticas
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes
	Errores de los usuarios	Falta de conocimiento del uso de la

Aplicación Lotus para acceso a la información de usuarios		aplicación
	Errores de configuración	Falta de capacitación del administrador del sistema
	Escapes de información	Falta de control de acceso
	Errores de actualización del programa	Falta de procedimientos aprobados
	Manipulación de la configuración	Falta de control de acceso
	Suplantación de identidad del usuario	Falta de control de acceso
	Abuso de privilegios de acceso	Falta de políticas de seguridad
	Negación de servicio	Incapacidad para distinguir una petición real de una petición falsificada
Portal de información (Página Web de la empresa)	Modificación no autorizada del sitio Web	Falta de procedimientos para cambios
	Negación de servicio	Falta de recursos necesarios
	Sitio Web no disponible	Fallas en los acuerdos de niveles de servicio
	Publicación de información incorrecta de la Uniplex	Falta de procedimiento aprobados
Suministros de Oficina	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres
	Robo	Falta de atención Falta de protección física
Imagen de la empresa Reputación	Divulgación de datos de los clientes	Insuficiente seguridad de información de los clientes
Paquetes o software estándar	Negación de Servicio	Capacidad insuficiente de los recursos
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección(AV) actualizada
	Spoofing, Escape de información	Falta de control de acceso
	Falta de capacidad de restauración	Falta de copias backup continuas
	Uso no previsto	Falta de políticas de seguridad
Sistemas Operativos	Negación de Servicio	Capacidad insuficiente de los recursos
	Negación de Servicio	Falta de capacitación del administrador Incompleto o incorrecto documentación del sistema
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección (AV) actualizada
	Falta de capacidad de restauración	Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas Instalación de SW no autorizado
	Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad

	Alteración no autorizado de la configuración	Falta de control de acceso
Medios y Soporte	Acceso no autorizado a la información	Falta de protección física
	Robo	Falta de protección física
	Daños de cables	Falta de protección física
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Brechas de seguridad no detectadas	Falta de monitoreo de la red

Tabla 3.29: Amenazas y Vulnerabilidades

Exposición del Riesgo

Se analizará la probabilidad de que cada amenaza y el nivel de vulnerabilidad, teniendo como resultado el nivel de exposición de riesgo de cada activo de Uniplex.

Valoración:

A= probabilidad de ocurrencia de la amenaza, en base a los registros de los últimos 2 años.

V= Nivel de vulnerabilidad.

Activos	Amenazas	Valor	Descripción
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra Uniplex
	V1: Falta de protección contra fuego	Media	Actualmente en Uniplex no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran los usuarios, con los equipos portátiles no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres

Hardware Portátil	desastres		naturales
	A4: Acceso no autorizado a la portátil	Media	Existen diferentes motivos para acceso al equipo sin autorización, ya sea código malicioso,
	V4: Falta de Protección por desatención de equipos	Alta	Se puede acceder fácilmente a la máquina, si no se la deja con la respectiva seguridad
	A5: Corte de suministro eléctrico o Falla en el aire acondicionado	Media	Los cortes de suministros eléctricos se presentan todos los años en el país
	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Media	Los portátiles no se conectan a un UPS general, únicamente cuentan con la batería
	A6: Instalación no autorizada o cambios de Software	Baja	Este problema no ha ocurrido en el último año
	V6: Falta de control de acceso	Media	Los usuarios no tienen permisos para instalar programas, pero existe la opción de que violen las seguridades de la información del administrador
	A7: Incumplimiento con la legislación	Baja	No se presentan registros
	V7: Falta de conocimiento de protección de derechos de SW por parte de los empleados	Alta	En la empresa no se tiene conocimiento de las leyes de protección de derechos de autor
	A8: Uso no previsto	Media	Es considerable el porcentaje de personas que utiliza los recursos para otras actividades diferentes del negocio
	V8: Falta de las políticas	Alta	No se encuentran definidas políticas de seguridad
	A9: Incumplimiento con controles de seguridad	Alta	El porcentaje de fallas en la seguridad es alto
	V9: Falta de conocimiento de seguridad por parte del personal	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A10: Degradación del HW	Medio	Los equipos ya han presentado varias fallas de HW
	V10: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento continuo de los equipos
	A11: Copia no autorizada de SW o información propietaria	Medio	Se han encontrado Cd piratas de SW con licencia.
	V11: Falta de políticas	Alta	No se encuentran definidas

			políticas de seguridad para conocimiento de los usuarios
	A12: Ataque destructivo	Baja	No se presentan registros de este problema
	V12: Falta de protección física	Alta	Los usuarios se llevan las portátiles, y las utilizan en medios no seguros
	A13: Robo	Media	Se tiene registrado un caso de robo de equipos
	V 13: Falta de protección física	Alta	No se tiene una adecuada protección física dentro de Uniplex
PCs de oficina	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra Uniplex
	V1: Falta de protección contra fuego	Media	Actualmente en Uniplex no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran los usuarios, con los equipos portátiles no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Acceso no autorizado a la portátil	Media	Existen diferentes motivos para acceso al equipo sin autorización, ya sea código malicioso,
	V4: Falta de Protección por desatención de equipos	Alta	Se puede acceder fácilmente a la máquina, si no se la deja con la respectiva seguridad
	A5: Corte de suministro eléctrico o Falla en el aire acondicionado	Media	Los cortes de suministros eléctricos se presentan todos los años en el país
	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Media	Los portátiles no se conectan a un UPS general, únicamente cuentan con la batería
	A6: Instalación no autorizada o cambios de Software	Baja	Este problema no ha ocurrido en el último año
	V6: Falta de control de acceso	Baja	Los usuarios no tienen permisos para instalar programas, pero existe la opción de que violen las seguridades de la

			información del administrador
	A7: Incumplimiento con la legislación	Baja	No se presentan registros
	V7: Falta de conocimiento de protección de derechos de SW por parte de los empleados	Alta	En la empresa no se tiene conocimiento de las leyes de protección de derechos de autor
	A8: Uso no previsto	Media	Es considerable el porcentaje de personas que utiliza los recursos para otras actividades diferentes del negocio
	V8: Falta de las políticas	Alta	No se encuentran definidas políticas de seguridad
	A9: Incumplimiento con controles de seguridad	Alta	El porcentaje de fallas en la seguridad es alto
	V9: Falta de conocimiento de seguridad por parte del personal	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A10: Degradación del HW	Media	Los equipos ya han presentado varias fallas de HW
	V10: Falta de mantenimiento adecuado	Media	No se realiza un mantenimiento continuo de los equipos
	A11: Copia no autorizada de SW o información propietaria	Media	Se han encontrado Cd piratas de SW con licencia.
	V11: Falta de políticas	Alta	No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A12: Ataque destructivo	Baja	No se presentan registros de este problema
	V12: Falta de protección física	Alta	Los usuarios se llevan las portátiles, y las utilizan en medios no seguros
	A13: Robo	Media	Se tiene registrado un caso de robo de equipos
	V 13: Falta de protección física	Alta	No se tiene una adecuada protección física dentro de Uniplex
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra Uniplex
	V1: Falta de protección contra fuego	Media	Actualmente en Uniplex no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Media	Las instalaciones donde se encuentran los servidores eran un antiguo cuarto, del cual no

Servidores			se han retirado las instalaciones de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4:Corrupción de archivos de registros	Baja	No se han presentado problemas de este nivel
	V4: Falta de Protección de los archivos de registro	Media	La única persona que tiene acceso a los servidores es el administrador, pero puede ser interceptada la información que viaja en la red
	A5: Negación de Servicio	Media	Este ataque no se ha presentado todavía, pero puede ocurrir
	V5: Incapacidad de distinguir una petición real de una falsa	Alta	No existe una protección efectiva ante este ataque
	A6: Corte de suministro eléctrico o Falla en el aire acondicionado	Media	Los cortes de energía eléctrica son frecuentes en el país
	V6: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Media	Los servidores se encuentran conectados al UPS que tiene una duración de 3 horas, luego del cual se apagarían.
	A7: Acceso no autorizado a través de la red	Media	Existe siempre la posibilidad que alguien no autorizado logré ingresar a través de la red
	V7: Código malicioso desconocido	Media	Esto puede pasar, pues siempre sale nuevo código dañino que no es reconocido por los antivirus.
	A8: Degradación o Falla del HW	Media	Son equipos que no han sido actualizados de HW hace mucho tiempo
	V8: Falta de mantenimiento adecuado	Media	No se realiza un mantenimiento preventivo y correctivo adecuado
	A9: Manipulación de la configuración	Baja	No se tiene registros de este tipo de problemas
	V9: Falta de control de acceso	Alta	El ingreso al cuarto de servidores no está muy protegido, únicamente cuenta con una puerta de una llave de fácil apertura
	A10: Incumplimiento con controles de seguridad	Media	Se han presentado registros de intentos de ingreso a los servidores sin autorización

	V10: Falta de conocimiento de seguridad por parte del personal	Alta	Los empleados de la empresa tienen muy poco conocimiento de las políticas de seguridad
	A11: Incapacidad de restauración	Alta	No se encuentra definido un plan de contingencia
	V11: Falta de planes de continuidad del negocio	Alta	No se realizan respaldos, ni se encuentran definidos procedimientos para enfrentar fallas
	A12: Análisis de tráfico	Media	Se han encontrado sniffers en la red
	V12: Falta de establecimiento de una conexión segura	Media	Se utilizan protocolos de encripción SSL en http
	A13: Brechas de seguridad no detectadas	Baja	No se han registrado eventos de este problema
	V13: Falta de monitoreo de los servidores	Alta	No se realiza continuo monitoreo de los servidores
	A14: Ataque destructivo	Baja	En la empresa no se ha presentado este problema
	V 14: Falta de protección física	Alta	La seguridad del edificio es muy escasa
Equipos de Oficina	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la empresa
	V1: Falta de protección contra fuego	Media	Actualmente en Uniplex no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran los usuarios, con los equipos no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Degradación o Falla de HW	Media	Se han presentado problemas en algunas impresoras y teléfonos
	V4: Falta de Mantenimiento	Alta	No se realiza un mantenimiento de los equipos, los mismos que utilizados por todos los usuarios.
	A5: Ataque destructivo	Baja	En la empresa no se ha presentado este problema
	V5: Falta de protección física	Alta	La seguridad del edificio es muy escasa

	A6: Uso no previsto	Alta	Se han encontrado a varios usuarios con uso no adecuado del teléfono y las impresoras
	V6.1: Falta de Políticas	Alta	No se encuentran definidos procedimientos para un uso adecuado de los equipos
	V6.2: Falta de Control de Acceso	Alta	No se tiene control para el uso de los equipos
Soporte electrónico	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra Uniplex
	V1: Falta de protección contra fuego	Media	Actualmente en la empresa no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	El soporte electrónico se guarda adecuadamente en estanterías adecuadas
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Condiciones inadecuadas de temperatura y/o humedad	Baja	Esto no se ha registrado debido al funcionamiento adecuado del aire acondicionado
	V4: Susceptibidad al calor y humedad	Alta	Los CD, disquetes son susceptibles a la humedad
	A5:Ataque destructivo	Baja	En la empresa no se ha presentado este problema
	V5: Falta de protección física	Alta	La seguridad de estos elementos es muy escasa
	A6:Escape de información	Alta	Se han presentado pérdidas en la oficina
	V6: Manipulación inadecuada de información	Alta	No se tiene un procedimiento aprobado de manipulación de la información
	A7: Robo	Alta	Se han presentado pérdidas en la oficina
	V7:Falta de atención del personal	Alta	El personal deja descuidadas sus cosas
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la empresa
	V1: Falta de protección contra fuego	Media	Actualmente en la empresa no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente

Documentación y Registros.	V2: Falta de protección física adecuada	Baja	Los documentos se encuentran en gavetas protegidas contra ingreso de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Pérdida de información	Media	Se han presentado problemas debido a fallas de los empleados
	V4.1: Errores de los empleados	Alta	No se realizan respaldos de la información, esto combinado con los errores de los usuarios
	V4.2 : Almacenamiento no protegido	Media	Los documentos se encuentran en gavetas bajo llave. Pero susceptible a daños por fuerza bruta
	A5: Divulgación de información de clientes	Media	No se encuentran definidos políticas de confidencialidad
	V5: Almacenamiento no protegido	Media	Los documentos se encuentran en gavetas bajo llave. Pero susceptible a daños por fuerza bruta
	A6: Incumplimiento de leyes en cuanto a la información de clientes o empleados	Baja	No se han presentado problemas de este tipo con clientes
	V6: Falta de conocimiento de los empleados	Media	Los empleados nuevos no son capacitados apropiadamente, lo que ocasiona desconocimiento de los reglamentos
	A7: Incorrecta o incompleta documentación del sistema	Baja	La compañía tiene documentado los procesos del Sistema
	V7: Falta de documentación actualizada del sistema	Media	No se encuentran documentación actualizada de los cambios realizados en el sistema.
	A8: Contratos incompletos	Media	Se han presentado problemas con el contrato con los proveedores de Internet
	V8: Falta de control para el establecimiento de contratos	Baja	Los contratos los revisan todos los niveles de la empresa, desde el solicitante hasta el director ejecutivo
	A9: Ataque destructivo	Baja	En la empresa no se ha presentado este problema
	V9: Falta de protección física	Alta	La seguridad de estos elementos es muy escasa

	A10: Incapacidad de restauración	Alta	No se encuentra definido un plan de contingencia
	V10: Falta de planes de continuidad del negocio	Alta	No se realizan respaldos, ni se encuentran definidos procedimientos para enfrentar fallas
	A11: Modificación no autorizada de la información	Media	Se han registrado problemas debidos a cambios en la información no previstos
	V11: Insuficiente entrenamiento de empleados	Baja	Los empleados conocen sus responsabilidades, y autorizaciones permitidas a la información
Empleados	A1: Errores de los empleados y acciones equivocadas	Alta	Nuevos empleados encuentran frecuentemente fallas debido a errores de empleados anteriores
	V1: Falta de conocimiento y oportuno entrenamiento	Media	Los empleados nuevos no son capacitados apropiadamente, lo que ocasiona desconocimiento de los reglamentos
	A2: Insuficiente personal	Media	Se presenta sobre todo en fechas de vacaciones de empleados, o cuando se enferman
	V2: Falta de acuerdos definidos para reemplazo de empleados	Media	No se encuentra definido un procedimiento claro para el reemplazo temporal
	A3: Divulgación de información confidencial	Media	Se puede presentar con empleados que han salido en malos términos de la empresa
	V3: Falta de acuerdos de confidencialidad	Baja	Se encuentra definido en el contrato los acuerdos de confidencialidad a los que se compromete el empleado
Establecimientos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la empresa
	V1: Falta de protección contra fuego	Media	Actualmente en la empresa no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones no presentan daños mayores debido a lluvias
	A3: Acceso no autorizado	Media	Se han registrado varios problemas debido a ingreso de personas no autorizadas
	V3.1: Falta de protección física	Alta	Uniplex cuenta con un único guardia que controla todo el edificio

	V3.2: Falta de políticas	Alta	No se encuentran definidas políticas para restringir el acceso a determinados lugares de la empresa
	A4: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V4: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
Servicio de Comunicaciones	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la empresa
	V1: Falta de protección contra fuego	Media	Actualmente en Uniplex no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de accidente
	V2: Falta de protección física adecuada	Baja	Las instalaciones donde se encuentran la PBX, no presentan penetrabilidad de agua.
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son fácilmente afectados por desastres	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A4: Degradación del servicio y equipos	Media	Se han presentado problemas debido a congestión de las líneas, y pérdidas del servicio de telefonía
	V4: Falta de mantenimiento Adecuado	Alta	No se realiza un mantenimiento adecuado de la central telefónica.
	A5: Errores de configuración	Baja	No se tienen registros de problemas debido a errores de configuración de la central
	V5: Falta de conocimiento del administrador	Media	El administrador tiene conocimiento muy básico de la central
	A6: Manipulación de la configuración	Baja	No se han registrado problemas debido a cambios en la configuración
	V6: Falta de control de acceso	Media	No se tiene control para el uso de los servicios
	A7: Uso no previsto	Media	En el año se han presentado varios incidentes donde se han encontrado a los empleados utilizando los equipos para fines personales, más que para fines de negocio

	V7: Falta de políticas	Media	No se encuentran políticas de seguridad definidas y de conocimiento de los usuarios
	A8: Daños de cables, ataques destructivos	Baja	En la empresa no se ha presentado este problema
	V8: Falta de protección adecuada	Alta	Los cables de líneas telefónicas se encuentran en lugares públicos.
	A9: Fallas de servicios de telefonía	Alta	Se encuentra registrado varias fallas al año de las líneas telefónicas
	V9: Falta de acuerdos bien definidos con terceras partes	Alta	No se negocian contratos que cubran los cambios continuos del negocio de terceras partes.
Servicio de energía eléctrica	A 1: Fuego	Baja	La oportunidad que de se produzca fuego no es muy alta
	V1: Falta de protección contra fuego	Alta	Actualmente en la empresa no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Media	Al año se presentan algunos registros de daños causados por lluvias.
	V2: Falta de protección física adecuada	Media	La entrada de la red eléctrica no se encuentra en un lugar seguro
	A3: Desastres naturales	Baja	En los últimos años no se ha presentado ningún desastre natural y es poco probable que ocurra
	V3: Falta de protección frente a desastres naturales	Media	No existen protecciones requeridas para enfrentar daños causados ante desastres naturales
	A 4: Ataque destructivo	Baja	Este tipo de ataque es muy poco probable que ocurra
	V 4: Falta de protección física	Baja	La entrada de la red eléctrica se encuentra en un lugar seguro
Servicio de correo electrónico	A1: Errores de los usuarios	Baja	Sólo se ha registrado una sola vez al año este incidente
	V1: Falta de conocimiento del uso del servicio	Media	Los usuario deben recibir entrenamiento en cómo usar los servicios
	A2: Suplantación de la identidad del usuario	Baja	No se ha registrado ningún incidente todavía
	V2: Falta de control de acceso	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A3: Análisis de tráfico	Baja	No se ha registrado ningún incidente
	V3: Falta de establecimiento de una conexión segura (VPN)	Alta	Ya que la información viaja en texto plano por la red pública sin encripción, se tiene un alto nivel de vulnerabilidad

	A4: Uso no previsto	Alta	En varias ocasiones se ha utilizado este servicio con fines personales
	V4: Falta de políticas	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	Media	En el año se registró este incidente dos veces
	V5: Falta de acuerdos bien definidos con terceras partes	Alta	No se tienen bien definidos los acuerdos de servicios con los proveedores de Internet
Aplicación Lotus para acceso a la información de usuarios	A1: Errores de los usuarios	Media	Se han presentado varios registros de problemas debido a fallas de los usuarios de la aplicación
	V1: Falta de conocimiento del uso de la aplicación	Baja	Al ingresar un nuevo usuario del servicio se le capacita para el correcto uso del sistema
	A2: Errores de configuración	Baja	Todavía no se ha registrado errores de configuración
	V2: Falta de capacitación del administrador del sistema	Baja	El administrador es una persona preparada con experiencia
	A3: Escapes de información	Baja	Todavía no se ha registrado errores en el mantenimiento o actualización del programa, pero puede suceder
	V3: Falta de control de acceso	Media	Se controla el acceso a este aplicativo mediante ID y claves, las cuales pueden ser fácilmente vulnerables debido a que no se cuenta con una política definida de generación de claves.
	A4: Errores de actualización del programa	Baja	No se ha registrado este incidente
	V4: Falta de procedimientos aprobados	Alta	No se cuenta con procedimiento de actualización de este SW
	A5: Manipulación de la configuración	Baja	Todavía no se ha registrado ninguna manipulación en la configuración
	V5: Falta de control de acceso	Media	Es posible que los usuarios utilicen passwords no apropiados ya que no se cuentan con política.
	A6: Suplantación de la identidad del usuario	Baja	No se ha registrado ningún incidente
	V6: Falta de Control de		En vista de que no se lleva

	acceso	Alta	actualizaciones del aplicativo, es más fácil explotar esta vulnerabilidad
	A7: Abuso de privilegios de acceso	Baja	No se ha registrado ningún incidente
	V7: Falta de políticas de seguridad	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A8: Negación de servicio	Media	Esta forma de ataque no ha tenido lugar todavía, pero podría pasar en cualquier momento
	V8: Incapacidad para distinguir una petición real de una petición falsificada	Alta	Hay ciertas formas de ataque de deniego de servicio, donde no existe ninguna protección contra estos tipos de ataque
Portal de información (Página Web de la empresa)	A1: Modificación no autorizada del sitio Web	Baja	La probabilidad global de modificación desautorizada es baja; el sitio de Web es bien protegido contra eso.
	V1: Falta de procedimientos para cambios	Alta	Actualmente no se cuenta con procedimientos para cambios del Sitio Web
	A2: Negación de servicio	Baja	No se ha registrado ningún incidente
	V2: Falta de recursos necesarios	Media	Los usuario deben recibir entrenamiento en cómo usar los servicios
	A3: Sitio Web no disponible	Media	Dos veces en el año se registro este evento
	V3: Fallas en los acuerdos de niveles de servicio	Media	No se tienen bien definidos los nivel es de servicio en los contratos
	A4: Publicación de información incorrecta de la empresa	Baja	Hasta el momento no se ha tenido ningún tipo de problema con esta amenaza
	V 4: Falta de procedimiento Aprobados	Baja	Antes de la publicación de información, se tienen una aprobación de la gerencia
Suministros de Oficina	A1: Fuego	Baja	La oportunidad que de se produzca fuego no es muy alta
	V1: Falta de protección contra fuego	Alta	Actualmente en la empresa no se tienen ninguna protección contra fuego, como extintores
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente
	V2: Falta de protección física adecuada	Baja	No se tiene cercanía con instalaciones de agua
	A3: Desastres naturales	Baja	No se ha registrado este tipo de incidente
	V3: Condiciones locales donde los recursos son	Media	No existen protecciones requeridas para enfrentar daños

	fácilmente afectados por desastres naturales		causados ante desastres naturales
	A4: Robo	Alta	Se ha presentado en algunas ocasiones este incidente
	V4.1: Falta de atención	Baja	El personal está en las instalaciones en horas de trabajo, y además cuenta con un guardia las 24 horas
	V4.2: Falta de protección física	Baja	Los suministros de oficina están debidamente asegurados
Imagen de la empresa Reputación	A1: Divulgación de datos de los clientes	Baja	No se ha registrado este tipo de incidente
	V1: Insuficiente seguridad de información de los clientes	Alta	Es vulnerable a eventos donde puede conducir a la mala imagen en público
Paquetes o software estándar	A1: Negación de Servicio	Baja	No se ha registrado este tipo de incidente
	V1: Capacidad insuficiente de los recursos	Baja	Se cuenta con los recursos suficientes
	A2: Virus de Computación, Fuerza Bruta y ataques de diccionario	Alta	Se ha registrado varias veces virus
	V2: Falta de Protección(AV) actualizada	Alta	No se lleva ningún tipo de actualización para el software
	A3: Spoofing, Escape de información	Baja	No se ha registrado este tipo de incidente
	V3: Falta de control de acceso	Baja	En el Sw estándar no se necesita ningún tipo de control de acceso
	A4: Falta de capacidad de restauración	Baja	No se ha registrado este tipo de incidente
	V4: Falta de copias de backup continuas	Alta	No se tiene copias de respalda para restauración
	A5: Uso no previsto	Alta	El personal en algunas ocasiones hacen uso de estas herramientas con fines personales
	V5: Falta de políticas de seguridad	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A 1: Negación de Servicio	Baja	Esta forma de ataque no ha tomado lugar todavía, pero podría pasar en cualquier momento
	V 1: Capacidad insuficiente de los recursos	Media	La recursos de los SOs, es suficiente para la cantidad de información que maneja la empresa.

Sistemas operativos	A2: Errores de Configuración del servicio	Baja	No se han presentado registros de este problema
	V2.1: Falta de capacitación del administrador	Media	El administrador no cuenta con gran conocimiento de los Sistemas operativos de los servidores.
	V2.2: Incompleto o incorrecto documentación del sistema	Media	Se tiene la documentación del sistema, pero sin seguir ningún procedimiento aprobado
	A 3: Virus de Computación, Fuerza Bruta y ataques de diccionario	Media	El servidor ha sido afectado una vez por un Virus de computación
	V 3: Falta de Protección (AV) actualizada	Alta	No se sigue procedimientos aprobados para la actualización y mantenimiento del software
	A 4: Falta de capacidad de restauración	Media	Todavía no ha pasado este incidente pero puede pasar en cualquier tiempo si no se tiene copias de backups
	V 4: Falta de copias de backup continuas	Alta	Esta vulnerabilidad puede ser fácilmente afectada porque no se tiene copias de backups
	A 5: Pérdida de Servicio	Baja	No se ha registrado ningún incidente
	V 5.1: Actualizaciones Incorrectas	Alta	No se cuenta con un procedimiento para las actualizaciones
	V 5.2: Instalación de SW no autorizado	Alta	Esta vulnerabilidad puede ser fácilmente debido a que no se sigue ninguna política de seguridad
	A 6: Controles de Seguridad no cumplidos	Alta	En la empresa no se ha definido controles de seguridad, razón por la cual ciertos controles no han sido cumplidos
	V 6: Falta de Políticas de Seguridad	Alta	Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía
	A7: Alteración no autorizado de la configuración	Baja	No se ha registrado ningún incidente
	V 7: Falta de control de acceso	Alta	El control de acceso puede ser fácilmente vulnerado debido a la débil seguridad física de los equipos de cómputo
	A1: Acceso no autorizado a la información	Media	Se han encontrado máquinas personales conectadas a la red
	V1: Falta de protección	Media	No se tiene una adecuada

Medios y Soporte	física		protección física dentro de Uniplex
	A 2: Robo	Baja	No se ha registrado ningún incidente
	V 2: Falta de protección física	Alta	No se tiene una adecuada protección física dentro de la empresa
	A3: Daños de cables	Baja	No se ha registrado este tipo de incidente
	V3: Falta de protección adecuada	Baja	El sistema de cableado esta debidamente instalado y protegido
	A4: Análisis de tráfico	Baja	No se ha registrado este tipo de incidente
	V4: Falta de establecimiento de una conexión segura (VPN)	Alta	La información viaja en texto plano en la red interna
	A5: Brechas de seguridad no detectadas	Baja	No se ha registrado este tipo de incidente
	V5: Falta de monitoreo de la red	Alta	No cuenta con ningún tipo de monitoreo de la red

Tabla 3.30: Exposición del Riesgo

3.4. Plan de Tratamiento de Riesgos para Identificar Acciones, Responsabilidades y Prioridades en la Gestión de los Riesgos de la Seguridad de la Intranet.

A continuación describimos las principales responsabilidades de los miembros implicados en la seguridad de la información para la gestión de los riesgos basados en los dominios:

- El **Área de Networking y Software** son responsables de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad a lo largo de toda la organización, todo esto en coordinación con la Dirección Ejecutiva y Jefatura Administrativa Financiera y con el área de Auditoría Interna.

También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

- El **Encargado de Networking** es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

- El **Jefe del área de software** es responsable de establecer los controles de acceso apropiados para cada usuario de Base de Datos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra, El personal de Sistemas también es responsable de informar al Encargado de Networking sobre toda actividad sospechosa o evento insólito.

- El **Departamento de Networking y el de Software** de Uniplex filial Guayaquil, procederá a revisar y proponer a la máxima autoridad de la empresa para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información; monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes; tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad; aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información;

garantizar que la seguridad sea parte del proceso de planificación de la información; evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios; promover la difusión y apoyo a la seguridad de la información dentro de la empresa y coordinar el proceso de administración de la continuidad de las actividades de la empresa

- Los usuarios son responsables de cumplir con todas las políticas de Uniplex relativas a la seguridad informática y en particular:
- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de Uniplex a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de Uniplex a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo en Uniplex.
- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- Reportar inmediatamente a su jefe inmediato o a un funcionario de Sistemas cualquier evento que pueda comprometer la seguridad de Uniplex y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

- El **Departamento de Networking y Software** tendrá a cargo el mantenimiento y la presentación para la aprobación de la Política, ante la máxima autoridad de Uniplex, el seguimiento de acuerdo a las incumbencias propias de cada área de las actividades relativas a la seguridad de la información (análisis de riesgos, monitoreo de incidentes, supervisión de la investigación, implementación de controles, administración de la continuidad, impulsión de procesos de concientización, etc.) y la proposición de asignación de funciones.

- Los **Responsables de las Unidades Organizativas** cumplirán la función de autorizar la incorporación de nuevos recursos de procesamiento de información a las áreas de su incumbencia.

- El **Responsable del Área Legal** participará notificará a los proveedores sobre las modificaciones que se efectúen a la Política de Seguridad, además de participar en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento y en el tratamiento de incidentes de seguridad que requieran de su intervención.

- El **Responsable del Área de Recursos Humanos** incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios.

El Responsable de Seguridad Informática tendrá a su cargo, entre otros:

- Definir procedimientos para el control de cambios a los procesos operativos documentados.

- □Definir y documentar una norma clara con respecto al uso del correo electrónico (políticas del correo electrónico).

- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo.

- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad.

- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

- □Implementar los controles de seguridad definidos (software malicioso y accesos no autorizados).
- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como cintas, discos, casetes e informes impresos y para la eliminación segura de los mismos.

Una vez que hemos definido los responsables para el manejo de las vulnerabilidades, tenemos que identificar las acciones que vamos a tomar sobre cada riesgo, por lo cual realizamos una valoración de los mismos en base a la información obtenida en el capítulo anterior. Además de obtener la valoración vamos a tomar la decisión de aceptar o tratar el riesgo.

Valoración del Riesgo del PGSI

La valoración de riesgos es ejecutada una vez que ya se ha creado un inventario de activos de información y determinando las categorías de importancia de los activos de información y el criterio para la evaluación de amenazas y vulnerabilidades.

El valor de un riesgo puede ser calculado usando la siguiente fórmula y los valores para el •valor de los activos de información", •escala de las amenazas" y •nivel de vulnerabilidad".

C: Valor del riesgo por la confidencialidad

I: Valor del riesgo por la integridad

D: Valor del riesgo por la disponibilidad

Valor del riesgo = •Valor del activo" x •Amenazas" x •Vulnerabilidades"

(Ejemplo)

Elementos de activos de información	Valor de los activos
C: confidencialidad	4
I: integridad	2
D: disponibilidad	1

Amenaza 3

Vulnerabilidad 3

El valor del riesgo para este caso es calculado de la siguiente forma:

Valor del riesgo por la confidencialidad: 4 x 3 x 3 = 36

Valor del riesgo por la integridad: 2 x 3 x 3 = 18

Valor del riesgo por la disponibilidad: 1 x 3 x 3 = 9

Fig 3.9: Ejemplo de cálculo para la valoración del riesgo

En base a la información obtenida en la anterior parte se puede realizar este cálculo y determinar el valor de riesgo de cada activo.

Una vez que tenemos la valoración de los riesgos debemos tomar la decisión de aceptar el riesgo o reducirlo, debemos determinar un valor mínimo como límite para aceptar el riesgo, sobre ese valor deben tomarse medidas sobre los riesgos. En nuestro caso seleccionamos como nivel límite de riesgo es el 4, es decir valores menores a 4 se tomará la decisión de aceptar el riesgo.

Luego de analizar el cuadro anterior determinamos que con este nivel los riesgos que aceptamos son aquellos que tienen una mínima probabilidad de ocurrencia con un poco impacto en caso de que lleguen a presentarse. A continuación presentamos una tabla con los niveles de riesgos:

	AMENAZA		
	1	2	3
	VULNERABILIDAD		

ACTIVOS DE INFORMACIÓN	1	2	3	1	2	3	1	2	3
1	1	2	3	2	4	6	3	6	9
2	2	4	6	4	8	12	6	12	18
3	3	6	9	6	12	18	9	18	27
4	4	8	12	8	16	24	12	24	36

Tabla 3.31: Niveles de Riesgos

Aquellos riesgos con niveles menores a 4 como se muestra en la tabla anterior, son aquellos que se van a aceptar. Como se puede observar son aquellos con una valoración mínima para no afectar la funcionalidad de la organización.

A continuación presentamos las opciones para el tratamiento de los riesgos:

3.5. Estudio de Factibilidad de Aplicación de los Controles de la Norma (Anexo A) para la Intranet.

En base a las vulnerabilidades identificadas en la empresa se detallarán los controles que ayudarán a cubrir estas vulnerabilidades, los demás controles no se consideraron debido a que no dan una mayor solución a los riesgos.

- **Factibilidad de los Controles del Dominio Política de Seguridad**

Política de Seguridad de la Información.

Documento de Política de Seguridad de la Información

Mediante las políticas de seguridad se busca que los empleados tengan conocimiento de la seguridad de información, de tal manera que se reduzca los errores de los empleados y también limitará los problemas que podría ocurrir y sus

impactos. El entrenamiento y otros controles asegurarán que los empleados comprendan el problema del mal uso y también se les informará que cualquier uso no autorizado será demandado y todas las evidencias necesarias serán recopiladas. Las personas que trabajan en Uniplex deben seguir políticas de acuerdo a las leyes relevantes, las cuales prohíben la copia de SW o información propietaria.

El documento de políticas de seguridad, específica la dirección de seguridad que va a seguir la empresa, se reducirá este problema si en la empresa se emite políticas de seguridad y se da conocer a todo el personal.

- **Factibilidad de los Controles del Dominio Aspectos Organizativos para la Seguridad**

Organización interna.

Asignación de responsabilidades sobre seguridad de la información

Asegurar un entrenamiento adecuado de los empleados, mejorando la cultura de la seguridad de información en la empresa, lo cual reducirá los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos.

Proceso de autorización de recursos para el tratamiento de la información

Con estos controles se trata de reducir el riesgo de acceso a los recursos de la información de forma no autorizada, para lo cual se asigna responsabilidades para la seguridad de la información a través de la empresa, para evitar el mal uso de los activos.

- **Factibilidad de los Controles del Dominio Gestión de Activos de la Red de Información**

Responsabilidad sobre los activos.

Inventario de activos

Se trata de controlar que los activos no sean robados mediante la asignación de propietarios, y con el inventario se busca tener identificados todos los activos de Uniplex.

Propiedad de los recursos

Se trata de controlar que los activos no sean robados mediante la asignación de propietarios, y con el inventario se busca tener identificados todos los activos de la empresa.

Uso aceptable del uso de los recursos

Para minimizar este riesgo se emplean guías de utilización de los activos fuera de las premisas de la empresa.

- **Factibilidad de los Controles del Dominio Seguridad de los Recursos Humanos**

Seguridad en la definición del trabajo y los recursos.

Roles y Responsabilidades

Introduciendo estos controles y haciendo que los empleados estén conscientes de su propia responsabilidad, lo cual ayudará a reducir el riesgo de probabilidad de este problema. Si algo sale mal, el impacto seguirá siendo alto, este riesgo no puede reducirse más allá.

Se busca reducir este riesgo, si se escoge de manera oportuna a los empleados, para lo cual se tendrá una política de selección del personal donde se detallará sus roles y responsabilidades, de esta manera evitar que los empleados realicen tareas que estén fuera de sus responsabilidades.

Selección y política del personal

Se busca reducir este riesgo, si se escoge de manera oportuna a los empleados, para lo cual se tendrá una política de selección del personal.

Términos y condiciones de la relación laboral

Se reducirá el riesgo del mal uso de los activos si los empleados comprenden sus responsabilidades, y sus roles con respecto a la seguridad de información.

Durante el empleo.

Responsabilidades de administración

Si se asegura que los empleados tengan un apropiado conocimiento de las amenazas de la seguridad, se reducirá este riesgo y sus posibles impactos. También con la ayuda del conocimiento de los roles y responsabilidades de cada empleado, se reducirá el mal uso de los activos

Conocimiento, educación y entrenamiento de la seguridad de información

Si se asegura que los empleados tengan un apropiado conocimiento de las amenazas de la seguridad, se reducirá este riesgo y sus posibles impactos.
Asegurar un entrenamiento adecuado de los empleados, mejorando la cultura de la seguridad de información en la empresa, lo cual reducirá los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos.

Proceso disciplinario

Si se asegura que los empleados tengan un apropiado conocimiento de las amenazas de la seguridad, se reducirá este riesgo y sus posibles impactos.

Los empleados de la empresa deben tener conocimiento de los riesgos que se toma al ejecutar código malicioso desconocido y qué consecuencias puede traer esta acción, este debe ser un proceso disciplinario continuo.

- **Factibilidad de los Controles del Dominio Seguridad Física y del Entorno**

Áreas seguras

Perímetro de seguridad física

Con la aplicación de este control, se dará una protección adecuada para evitar un ataque destructivo. Con la provisión de una protección física adecuada a los activos de Uniplex:

Con la aplicación de estos controles se brinda a los empleados los recursos necesarios para llevar un correcto manejo de la documentación o registro, como por ejemplo. Escritorios con llaves, para proteger la información más sensible.

Controles físicos de entradas

Mediante este control se evita el acceso no autorizado a los activos de la empresa, mediante una protección física adecuada.

Seguridad de oficinas, despachos y recursos

Con este control se da una protección física adecuada a los activos de la empresa, además de brindar a los empleados los recursos necesarios para llevar un correcto manejo de la documentación o registro, como por ejemplo. Escritorios con llaves, para proteger la información más sensible.

Seguridad de los equipos.

Utilidades de apoyo

Se evita la interrupción de los servicios que ofrecen los activos con la aplicación de estos controles

Mantenimiento de equipos

Se minimiza este riesgo con un apropiado mantenimiento de los equipos de la empresa.

Seguridad de equipos fuera de los locales de la organización

Con estos controles se asegura que los equipos sean protegidos de amenazas físicas y del ambiente, y por ende se evita el acceso no autorizado a estos activos.

- **Factibilidad de los Controles del Dominio Gestión de Comunicaciones y Operaciones**

Procedimientos y responsabilidades de operación

Documentación de procedimientos operativos

Se debe tener documentados los procedimientos de actualización para evitar una errónea actualización y por consiguiente pérdida del servicio

La utilización de este control reducirá este riesgo, ya que se documentará solo los procedimientos de operación permitidos y necesarios para la ejecución del Sistema Operativo.

Control de cambios operacionales

Se debe tener documentados los procedimientos de actualización para evitar una errónea actualización y por consiguiente pérdida del servicio.

Gestión de servicios externos.

Entrega del servicio

Con este control se busca reducir las fallas en los acuerdos de niveles de servicio con partes externas, para lo cual la empresa debe mantener un nivel apropiado de seguridad y chequear la implementación de los acuerdos.

Monitorización y revisión de los servicios de las terceras partes

Se reducirá el riesgo de fallos de servicios entregados por terceras partes si se tiene bien definidos los acuerdos y se toma en cuenta aspectos relacionados con la seguridad.

Planificación y aceptación del sistema.

Planificación de la capacidad

Con una adecuada planificación del sistema se evitará la degradación del servicio.

Aceptación del sistema

Con una adecuada planificación del sistema se evitará la degradación del servicio.

Protección contra software malicioso.

Controles contra software malicioso

Los controles seleccionados reducirán la probabilidad de que este problema ocurra, pero un nuevo código malicioso siempre puede causar un problema, por lo tanto el riesgo no puede reducirse más allá.

Estos controles reducirán la probabilidad de que este problema ocurra mediante la implementación de procedimientos apropiados para la protección contra software malicioso.

Gestión interna de respaldo.

Recuperación de la información

Este control reducirá este riesgo al máximo mediante una política de respaldo y una restauración oportuna.

Gestión de la seguridad de red.

Controles de red

Con la aplicación de estos controles se reducirá el riesgo de la negación del servicio mediante una adecuada gestión de la red.

Es establecimiento de estos controles busca mantener la confidencialidad de los datos y así evitar el acceso no autorizado a la red, información y servicio.

Seguridad de los servicios de red

Es establecimiento de estos controles buscar mantener la confidencialidad de los datos y así evitar el acceso no autorizado a la red, información y servicio.

Utilización de los medios de información.

Gestión de medios removibles

Con el establecimiento de estos controles se busca tener un procedimiento de manipulación de información para protegerla del mal uso o divulgación no autorizada.

Procedimientos de manipulación de la información

Con el establecimiento de estos controles se busca tener un procedimiento de manipulación de información para protegerla del mal uso o divulgación no autorizada.

Intercambio de información.

Mensajería electrónica

Se trata de minimizar la transmisión de software malicioso a través del uso de comunicaciones electrónicas. Con estos controles se trata de asegurar un intercambio de información segura.

Sistemas de información comerciales

Se trata de minimizar la transmisión de software malicioso a través del uso de comunicaciones electrónicas.

Monitorización.

Registro de auditoria

Una monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad, con este objetivo se ha implementado en la empresa herramientas de administración de redes para realizar una adecuada monitorización y detectar a tiempo huecos de seguridad.

Monitorización del uso del sistema

Monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad.

Registros del administrador y operador

Una monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad.

Registro de fallas

Monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad.

- **Factibilidad de los Controles del Dominio Control de Acceso**

Requerimiento de negocios para control de acceso

Política de control de acceso

Es necesario implementar en las políticas de seguridad el control de acceso necesario que se deben tener para permitir el ingreso a las oficinas así como el procedimiento para eliminar los permisos de personas que han salido de la empresa, si bien el riesgo no va a desaparecer el objetivo es disminuirlo.

Se requieren políticas de control de acceso donde se justifiquen las responsabilidades y obligaciones de las personas que tienen acceso a modificar información de la empresa, y los controles necesarios para proteger información crítica; si bien el riesgo no va a desaparecer el objetivo es disminuirlo.

Gestión de acceso de usuarios

Registro de usuarios

Se requiere un procedimiento de registro de ingreso y salida de usuarios para garantizar el acceso a los sistemas y servicios de información.

Gestión de privilegios

Se requiere un procedimiento de revisión continua de privilegios para garantizar y revocar el acceso a los sistemas y servicios de información. Y de esta manera disminuir cambios no autorizados en información crítica

Revisión de derechos de acceso de los usuarios

Es necesario mantener un control del acceso a los datos y servicios de información, por lo cual se requiere realizar una revisión periódica de los derechos de acceso de los usuarios.

Responsabilidades de los usuarios

Uso de contraseñas

Es necesario que los usuarios estén informados del uso de la contraseña, así como las responsabilidades, y la forma de mantenerla en reserva para evitar acceso a información confidencial por parte de personas ajenas.

Equipo informático de usuarios desatendido

Es necesario que los usuarios tengan conocimiento de la protección que requieren sus equipos, para evitar acceso de terceras personas o pérdida de información de los mismos.

Políticas de limpieza de pantalla y escritorio

Es necesario establecer políticas de limpieza de escritorio para evitar papeles y unidades extraíbles que contengan información que requiera protección.

Control de acceso a la red

Política de uso de los servicios de la red

Es necesario asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios.

Autenticación de usuarios para conexiones externas

Es necesario asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por lo cual se requiere mantener un control sobre los sistemas críticos que almacenan información importante de la empresa.

Autenticación de nodos de la red

Es necesario asegurar que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, una alternativa para evitar conexiones falsas es la autenticación de los nodos permitidos para la red.

Protección a puertos de diagnóstico remoto

Es necesario mantener un control sobre puertos que pueden ser una puerta de ingreso no autorizado a la información de la empresa, por lo cual se deben definir los puertos necesarios y bloquear los demás.

Control de conexión a las redes

Los requisitos de la política de control de accesos para redes compartidas, necesitan incorporar controles que restrinjan las capacidades de conexión de los usuarios. Para evitar congestión en los servicios, debido a peticiones falsas.
Por lo cual es indispensable mantener un monitoreo sobre la red para detectar brechas de seguridad y disminuirlas.

Control de enrutamientos en la redes

La conversión de direcciones de la red también es un mecanismo muy útil para aislar redes y evitar rutas de propagación de problemas de seguridad en las redes.

Control de acceso al sistema operativo

Identificación y autenticación del usuario

Se requiere que todos los usuarios deberían disponer de un identificador único para su uso personal y exclusivo, a fin de que pueda posteriormente seguirse la pista de las actividades de cada responsable particular.

Control de acceso a las aplicaciones

Restricción de acceso a la información

Se debería dar acceso a la información y a las funciones del sistema de aplicaciones sólo a los usuarios de éste, incluido el personal de apoyo. De esta

manera se tendría un mejor control de las personas que tienen acceso para una auditoria.

- **Factibilidad de los Controles del Dominio Adquisición, Desarrollo y Mantenimiento de Sistemas de Información**

Controles criptográficos

Política de uso de los controles criptográficos

La organización debería desarrollar una política de uso de las medidas criptográficas para proteger la información.

Seguridad en los procesos de desarrollo y soporte

Procedimientos de control de cambios

Se deberían exigir procedimientos formales de control de cambios que garanticen que la seguridad y los procedimientos de control no se alteran y no ocasionan problemas de funcionamiento en la aplicación.

Revisión técnica de los cambios en el sistema operativo

Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.

Restricciones en los cambios a los paquetes de software

Es necesario usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea posible y practicable para evitar cambios que afecten el funcionamiento correcto de los servicios.

Canales encubiertos y código troyano

Es necesario usar los paquetes de software suministrados por los proveedores sin modificación en la medida que sea posible y practicable para evitar cambios que afecten el funcionamiento correcto de los servicios. Y puertas que puedan ser aprovechadas por jackers o intrusos.

Gestión de vulnerabilidad técnica

Control de vulnerabilidades técnicas

Se requiere de información oportuna sobre vulnerabilidades técnicas de los sistemas de información que son utilizados en la organización, y la evaluación de la exposición de la organización a tales vulnerabilidades. A fin de evitar brechas de seguridad que pueden ser fácilmente explotadas. Permitiendo el acceso a la red de intrusos.

- **Factibilidad de Los Controles del Dominio Gestión de Incidentes de Seguridad de la Información**

Divulgación de eventos y de debilidades de la seguridad de la información

Divulgación de eventos de la seguridad de la información

Es necesario implementar procedimientos de divulgación formal del acontecimiento de la seguridad de la información, junto con una respuesta del incidente y un procedimiento de escalada, para que los empleados puedan implementar las medidas correctivas necesarias.

Administración de incidentes y mejoras de la seguridad de la información

Responsabilidades y procedimientos

Es necesario implementar responsabilidades y los procedimientos se deben establecer para asegurar una respuesta rápida, eficaz, y ordenada a los incidentes de la seguridad de la información.

- **Factibilidad de los Controles del Dominio Gestión de Continuidad del Negocio**

Aspectos de la gestión de continuidad del negocio

Proceso de gestión de la continuidad del negocio

Es indispensable considerar en la gestión de la continuidad del negocio controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales. Debido a fallas en algún equipo o sistema.

Desarrollo e implantación de planes de contingencia

Este control es indispensable para asegurar la disponibilidad de la información en niveles aceptables y de acuerdo al nivel crítico en el negocio cuando se presente alguna falla que pueda afectar los servicios.

- **Factibilidad de los Controles del Dominio Cumplimiento**

Cumplimiento con los requisitos legales

Derechos de propiedad intelectual

Se deben implantar procedimientos apropiados para asegurar el cumplimiento de las restricciones legales sobre el uso del material protegido como derechos de autor y los productos de software propietario

Salvaguarda de los registros de la organización

Se requiere proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación. Es necesario guardar de forma segura ciertos registros, tanto para cumplir ciertos requisitos legales o regulatorios, como para soportar actividades esenciales del negocio.

Protección de los datos y de la privacidad de la información personal

Es necesario basarse en las leyes que protegen datos personales, para evitar problemas legales en los que puede verse involucrada la organización.

Evitar el mal uso de los recursos de tratamiento de la información

Es necesario que los usuarios estén conscientes que el uso de un computador con fines no autorizados puede llegar a ser un delito penal.

Revisiones de la política de seguridad y de la conformidad técnica

Conformidad con la política de seguridad

Es necesario que los gerentes, jefes de departamentos se aseguren que se estén cumpliendo correctamente todos los procedimientos de seguridad dentro de su área de responsabilidad, para evitar problemas legales.

3.6. Selección de los Controles de Acuerdo a la Factibilidad de Aplicación.

Una vez indicadas las razones por las cuales se debería escoger los controles, se procederá a la selección de los controles específicos para cubrir cada uno de las amenazas y vulnerabilidades identificadas.

Planteamiento del Problema

Es importante comprender varios factores que conllevaron a aplicar los diferentes controles que sugiere la Norma ISO 27002, actualmente la empresa presenta varios puntos de fallas de seguridad tanto en la red como en la infraestructura. A continuación se indica varios problemas de seguridad presentes en la red de datos de Uniplex.

- En la empresa no se cuenta con algún tipo de protección contra ataques provenientes del Internet, por esta razón es importante contar con un sistema de seguridad para que minimice esta amenaza.
- Actualmente no se cuenta con una política de seguridad establecida para definir los lineamientos de seguridad, esto conjuntamente con la falta de un

sistema de seguridad hace a la red muy vulnerable a tener huecos de seguridad, especialmente por el hecho de que los empleados navegan libremente por el Internet sin ningún tipo de cuidado y descargan programas provenientes de sitios no confiables. Además no se tiene restricciones en el uso de los recursos de la Corporación con fines personales como por ejemplo: chatear, revisar su correo electrónico personal.

- Para el acceso físico al cuarto de servidores no se cuenta con alguna restricción formal, lo cual puede ocasionar problemas debido a accesos no autorizados.
- No se cuenta con alguna herramienta de administración de red para monitorear continuamente la red de tal forma que se pueda detectar un ataque a tiempo, por ejemplo por algún comportamiento anormal de alguna máquina, o evitar alguna pérdida de servicio mediante la generación de avisos.

Controles Seleccionados de la Norma Iso 27002

Los controles seleccionados son los que se adjunta en la siguiente lista:

ACTIVO	Amenazas	Vulnerabilidades	Uso de la norma 27002
HARDWARE PORTÁTIL	**Acceso no autorizado a la portátil**	**Falta de Protección por desatención de equipos**	2.5.1. Áreas seguras
			2.5.2.5. Seguridad de equipos fuera de los locales de la organización
			2.7.1. Requisitos del negocio para control del acceso
			2.7.1.1. Política de control de acceso
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.11.2. Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
			2.11.2.1. Cumplimiento con las políticas y las normas de seguridad
HARDWARE PORTÁTIL	**Corte de suministro eléctrico o Falla en el aire acondicionado**	**Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado**	2.5.2. Seguridad de los equipos
			2.5.2.2. Servicios de Suministro
			2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
			2.10.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información
			2.10.1.5. Pruebas, Mantenimiento y reevaluación de los planes de continuidad del negocio

HARDWARE PORTÁTIL	**Incumplimiento con la legislación**	**Falta de conocimiento de protección de derechos de SW por parte de los empleados**	2.4.2. Durante la vigencia del contrato laboral
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.11.2. Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
			2.11.2.1. Cumplimiento con las políticas y las normas de seguridad
HARDWARE PORTÁTIL	**Uso no previsto**	**Falta de las políticas**	2.1.1. Política de seguridad de la información
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.4. Proceso de autorización para los servicios de procesamiento de información
			2.4.1. Antes de la contratación laboral
			2.4.1.1. Roles y responsabilidades
			2.4.1.3. Términos y condiciones laborales
			2.4.2. Durante la vigencia del contrato laboral
			2.4.2.1. Responsabilidades de la dirección

			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de registro de inicio seguro

HARDWARE PORTÁTIL	**Incumplimiento con controles de seguridad**	**Falta de conocimiento de seguridad por parte del personal**	2.4.2. Durante el vigencia del contrato laboral
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.9.1. Reporte sobre los eventos y las debilidades de la seguridad de la información
			2.9.1.1. Reporte sobre los eventos de seguridad de la información
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
HARDWARE PORTÁTIL	**Degradación del HW**	**Falta de mantenimiento adecuado**	2.5.2. Seguridad de los equipos
			2.5.2.4. Mantenimiento de los equipos
HARDWARE	**Inautorizada copia de**	**Falta de políticas**	2.1.1. Política de seguridad de la información

PORTÁTIL	**SW o información propietaria**		2.1.1.1. Documento de política de seguridad de la información
			2.11.1. Cumplimiento con los requisitos legales
			2.11.1.2. Derechos de propiedad intelectual (DPI)
			2.11.1.4. Protección de los datos y de la privacidad de la información personal
HARDWARE PORTÁTIL	**Ataque destructivo**	**Falta de protección física**	2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.5.1.4. Protección contra amenazas externas y ambientales
HARDWARE PORTÁTIL	**Robo**	**Falta de protección física**	2.3.1. Responsabilidad por los activos
			2.3.1.1. Inventario de activos
			2.3.1.2. Propietario de los activos
			2.3.1.3. Uso aceptable de los activos
			2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.7.3. Responsabilidades de los usuarios
			2.7.3.2. Equipo de usuario desatendido

ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***

PC's DE OFICINA	**Acceso no autorizado al equipo**	**Falta de Protección por desatención de equipos**	2.5.1. Áreas seguras
			2.5.2.5. Seguridad de equipos fuera de los locales de la organización
			2.7.1. Requisitos del negocio para control del acceso
			2.7.1.1. Política de control de acceso
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.11.2. Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
			2.11.2.1. Cumplimiento con las políticas y las normas de seguridad
PC's DE OFICINA	**Corte de suministro eléctrico o Falla en el aire acondicionado**	**Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado**	2.5.2. Seguridad de los equipos
			2.5.2.2. Servicios de Suministro
			2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
			2.10.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información
			2.10.1.5. Pruebas, Mantenimiento y reevaluación de los planes de continuidad del negocio
PC's DE OFICINA	**Incumplimiento con la legislación**	**Falta de conocimiento de protección de derechos de SW por**	2.4.2. Durante la vigencia del contrato laboral
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información

		parte de los empleados	2.11.2. Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
			2.11.2.1. Cumplimiento con las políticas y las normas de seguridad

PC's DE OFICINA	**Uso no previsto**	**Falta de las políticas**	2.1.1. Política de seguridad de la información
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.4. Proceso de autorización para los servicios de procesamiento de información
			2.4.1. Antes de la contratación laboral
			2.4.1.1. Roles y responsabilidades
			2.4.1.3. Términos y condiciones laborales
			2.4.2. Durante la vigencia del contrato laboral
			2.4.2.1. Responsabilidades de la dirección
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de registro de inicio seguro

PC's DE OFICINA	**Incumplimiento con controles de seguridad**	**Falta de conocimiento de seguridad por parte del personal**	2.4.2. Durante el vigencia del contrato laboral
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.9.1. Reporte sobre los eventos y las debilidades de la seguridad de la información
			2.9.1.1. Reporte sobre los eventos de seguridad de la información
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de registro de inicio seguro
PC's DE OFICINA	**Degradación del HW**	**Falta de mantenimiento adecuado**	2.5.2. Seguridad de los equipos
			2.5.2.4. Mantenimiento de los equipos

PC's DE OFICINA	**Inautorizada copia de SW o información propietaria**	**Falta de políticas**	2.1.1. Política de seguridad de la información
			2.1.1.1. Documento de política de seguridad de la información
			2.11.1. Cumplimiento con los requisitos legales
			2.11.1.2. Derechos de propiedad intelectual (DPI)
			2.11.1.4. Protección de los datos y de la privacidad de la información personal

PC's DE OFICINA	**Ataque destructivo**	**Falta de protección física**	2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.5.1.4. Protección contra amenazas externas y ambientales
PC's DE OFICINA	**Robo**	**Falta de protección física**	2.3.1. Responsabilidad por los activos
			2.3.1.1. Inventario de activos
			2.3.1.2. Propietario de los activos
			2.3.1.3. Uso aceptable de los activos
			2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.7.3. Responsabilidades de los usuarios
			2.7.3.2. Equipo de usuario desatendido

ACTIVO	Amenazas	Vulnerabilidades	Uso de la norma 27002
SERVIDORES	**Negación de Servicio**	**Incapacidad de distinguir una petición real de una falsa**	2.6.6. Gestión de la seguridad de las redes, 2.6.6.1. Controles de las redes 2.6.6.2. Seguridad de los servicios de la red 2.6.4. Control de acceso a las redes 2.6.4.1. Política de uso de los servicios en red 2.6.4.2. Autenticación de usuarios para conexiones externas 2.6.4.3. Autenticación de los equipos en la red 2.6.4.4. Protección de los puertos de configuración y diagnóstico remoto 2.6.4.6. Control de conexión a las redes 2.8.6. Gestión de la Vulnerabilidad Técnica 2.8.6.1. Control de las Vulnerabilidades Técnicas
SERVIDORES	**Corte de suministro eléctrico o Falla en el aire acondicionado**	**Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado**	2.5.2. Seguridad de los equipos 2.5.2.2. Servicios de suministro 2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio 2.10.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información 2.10.1.5. Pruebas, Mantenimiento y reevaluación de los planes de continuidad del negocio
SERVIDORES	**Acceso no autorizado**	**Código malicioso**	2.6.6. Gestión de la seguridad de las redes

	a través de la red	**desconocido**	2.6.6.1. Controles de las redes
			2.6.6.2. Seguridad de los servicios de la red
			2.6.4. Control de acceso a las redes
			2.6.4.1. Política de uso de los servicios en red
			2.6.4.2. Autenticación de usuarios para conexiones externas
			2.6.4.3. Autenticación de los equipos en las redes
			2.6.4.4. Protección de los puertos de configuración y diagnóstico remoto
			2.6.4.6. Control de conexión a las redes
			2.8.6. Gestión de la Vulnerabilidad Técnica
			2.8.6.1. Control de las Vulnerabilidades Técnicas

SERVIDORES	**Degradación o Falla del HW**	**Falta de mantenimiento adecuado**	2.2.1. Organización interna
			2.5.2. Seguridad de los equipos
			2.5.2.4. Mantenimiento de los equipos
SERVIDORES	**Manipulación de la configuración**	**Falta de control de acceso**	2.5.1.1. Perímetro de seguridad física
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.7.2. Gestión del acceso de usuarios
			2.7.2.2. Gestión de privilegios
			2.7.2.4. Revisión de los derechos de acceso de los usuarios
			2.7.5. Control de acceso al sistema operativo
			2.7.5.2. Identificación y autenticación de usuarios
SERVIDORES	**Incumplimiento con controles de seguridad**	**Falta de conocimiento de seguridad por parte del personal**	2.4.2. Durante la vigencia del contrato laboral
			2.4.2.2. Educación formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.9.1. Reporte sobre los eventos y las debilidades de la seguridad de la información
			2.9.1.1. Reporte sobre los eventos de seguridad de la información
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
SERVIDORES	**Incapacidad de restauración**	**Falta de planes de continuidad del**	2.6.5 Respaldo
			2.6.5.1 Respaldo de la información

		negocio	2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
			2.10.1.1. Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio
			2.10.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

	Análisis de tráfico	**Falta de establecimiento de una conexión segura (VPN)**	2.6.6 Gestión de la seguridad de las redes.
			2.6.6.1 Controles de las redes
			2.6.6.2 Seguridad de los servicios de la red
			2.7.4. Control de acceso a las redes
			2.7.4.2. Autenticación de usuarios para conexiones externas
			2.7.4.4. Protección de los puertos de configuración y diagnóstico remoto
			2.7.5. Control de acceso al sistema operativo
			2.7.5.2. Identificación y autenticación de usuarios
			2.7.6. Gestión de la Vulnerabilidad Técnica
SERVIDORES			2.8.6.1. Control de las Vulnerabilidades Técnicas
	Brechas de seguridad no detectadas	**Falta de monitoreo de los servidores**	2.6.2 Monitoreo. Objetivo: Detectar actividades no autorizadas.
			2.6.2.4 Monitoreo del uso del sistema
			2.6.2.6 Registros del administrador y del operador
SERVIDORES			2.6.2.6 Registro de fallas

			2.7.4. Control de acceso a las redes
			2.7.4.2. Autenticación de usuarios para conexiones externas
			2.7.4.4. Protección de los puertos de configuración y diagnóstico remoto
SERVIDORES	**Ataque destructivo**	**Falta de protección física**	2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.5.1.4. Protección contra amenazas externas y ambientales

ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
EQUIPOS DE OFICINA	**Degradación o Falla de HW**	**Falta de Mantenimiento**	2.7.2. Seguridad de los equipos
			2.7.2.4. Mantenimiento de equipos
EQUIPOS DE OFICINA	**Uso no previsto**	**Falta de Políticas Falta de Control de Acceso**	2.1.1. Política de seguridad de la información
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.4. Proceso de autorización para los servicios reprocesamiento de información
			2.4.1. Antes de la contratación laboral
			2.4.1.1. Roles y responsabilidades

			2.4.1.3. Términos y condiciones laborales
			2.4.2. Durante la vigencia del contrato laboral
			2.4.2.1. Responsabilidades de la dirección
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de inicio seguro

ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
SOPORTE ELECTRÓNICO	**Robo**	**Falta de atención del personal**	2.3.1. Responsabilidad por los activos
			2.3.1.1. Inventario de activos
			2.3.1.2. Propiedad de los activos
			2.3.1.3. Uso aceptable de los activos
			2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.7.3. Responsabilidades de los usuarios
			2.7.3.2. Equipo de usuario desatendido

SOPORTE ELECTRÓNICO	**Escape de información**	**Manipulación inadecuada de información**	2.6.7. Manejo de los medios
			2.6.7.1. Gestión de los medios removibles
			2.6.7.3. Procedimientos de manipulación de la información
			2.7.3. Responsabilidades de los usuarios
			2.7.3.3. Políticas de escritorio despejado y de pantalla despejada
ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
DOCUMENTACIÓN Y REGISTROS	**Pérdida de información**	**Errores de los empleados**	2.1.1. Política de seguridad de la información.
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.3. Asignación de responsabilidades para la seguridad de la información
			2.4.1. Antes de la contratación laboral.
			2.4.1.1. Roles y responsabilidades
			2.4.2. Durante la vigencia del contrato laboral.
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos

DOCUMENTACIÓN Y REGISTROS	**Pérdida de información**	**Almacenamiento no protegido**	2.5.1 Áreas seguras.
			2.5.1.1 Perímetro de seguridad física

			2.5.1.3 Seguridad de oficinas, recintos e instalaciones
			2.7.1. Requisitos del negocio para el control del acceso
			2.7.1.1. Política de control de acceso
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
DOCUMENTACIÓN Y REGISTROS	**Divulgación de información de clientes**	**Almacenamiento no protegido**	2.5.1 Áreas seguras.
			2.5.1.1 Perímetro de seguridad física
			2.5.1.3 Seguridad de oficinas, recintos e instalaciones
			2.7.1. Requisitos del negocio para el control del acceso
			2.7.1.1. Política de control de acceso
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
			2.11.1. Cumplimiento de los requisitos legales
			2.11.1.3. Procedimiento de los registros de la organización
			2.11.1.4. Protección de los datos y privacidad de la información personal

DOCUMENTACIÓN Y REGISTROS	**Ataque destructivo**	**Falta de protección física**	2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones

			2.5.1.4. Protección contra amenazas externas y ambientales
DOCUMENTACIÓN Y REGISTROS	**Incapacidad de restauración**	**Falta de planes de continuidad del negocio**	2.6.5. Respaldo
			2.6.5.1. Respaldo de la información
			2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
			2.10.1.3. Desarrollo e implementación de planes de contingencia que incluyan la seguridad de la información
ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
EMPLEADOS	**Errores de los empleados y acciones equivocadas**	**Falta de conocimiento y oportuno entrenamiento**	2.4.1. Antes de la contratación laboral.
			2.4.1.1. Roles y responsabilidades
			2.4.1.2. Selección
			2.4.2. Durante la vigencia del contrato laboral.
			2.4.2.1. Responsabilidades de la dirección
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos

ACTIVO	Amenazas	Vulnerabilidades	Uso de la norma 27002
ESTABLECIMIENTO	Acceso no autorizado	Falta de políticas Falta de protección física	2.1.1. Política de seguridad de la información.
			5.1.1. Documento de la política de seguridad de la información
			2.1.1 Áreas seguras.
			2.5.1.2 Controles de acceso físico
			2.7.1. Requerimiento de negocios para el control del acceso
			2.7.1.1. Política de control de acceso
			2.9.1. Reporte sobre los eventos y las debilidades de la seguridad de la información
			2.9.1.2. Reporte sobre las debilidades en la seguridad
ACTIVO	**Amenazas**	**Vulnerabilidades**	**Uso de la norma 27002**
SERVICIO DE COMUNICACIONES	Degradación del servicio y equipos	Falta de mantenimiento adecuado	2.5.2. Seguridad de los equipos
			2.5.2.4. Mantenimiento de los equipos
SERVICIO DE COMUNICACIONES	Uso no previsto	Falta de políticas	2.1.1. Política de seguridad de la información.
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.4. Proceso de autorización para los servicios de procesamiento de la información
			2.4.1. Antes de la contratación laboral
			2.4.1.1. Roles y responsabilidades
			2.4.1.3. Términos y condiciones laborales
			2.4.2. Durante la vigencia del contrato laboral

			2.4.2.1. Responsabilidades de la dirección
			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de registro de inicio seguro

SERVICIO DE COMUNICACIONES	**Ataque destructivo**	**Falta de protección física**	2.5.1. Áreas seguras
			2.5.1.1. Perímetro de seguridad física
			2.5.1.2. Controles de acceso físico
			2.5.1.3. Seguridad de oficinas, recintos e instalaciones
			2.5.1.4. Protección contra amenazas externas y ambientales
SERVICIO DE COMUNICACIONES	**Fallas de servicios telefonía**	**Falta de acuerdos bien definidos con terceras partes**	2.6.2 Gestión de la prestación del servicio por terceras partes
			2.6.2.1 Prestación del servicio
			2.6.2.2 Monitoreo y revisión de los servicios por terceros

ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
SERVICIO DE CORREO	**Suplantación de la identidad del usuario**	**Falta de control de acceso**	2.6.6 Gestión de la seguridad de las redes
			2.6.6.1 Controles de las redes

ELECTRÓNICO			2.6.6.2 Seguridad de los servicios de la red
			2.7.2. Gestión del acceso de usuarios
			2.7.2.1. Registro de Usuarios
			2.7.2.4. Revisión de los derechos de acceso de los usuarios
SERVICIO DE CORREO ELECTRÓNICO	**Análisis de tráfico**	**Falta de establecimiento de una conexión segura (VPN)**	2.6.6 Gestión de la seguridad de las redes
			2.6.6.1 Controles de las redes
			2.6.6.2 Seguridad de los servicios de la red
			2.8.3. Controles criptográficos
			2.8.3.1.Política sobre el uso de controles criptográficos

SERVICIO DE CORREO ELECTRÓNICO	**Uso no previsto**	**Falta de políticas**	2.1.1. Política de seguridad de la información
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.4. Proceso de autorización para los servicios de procesamiento de información
			2.4.1. Antes de la contratación laboral
			2.4.1.1. Roles y responsabilidades
			2.4.1.3. Términos y condiciones laborales
			2.4.2. Durante la vigencia del contrato laboral
			2.6.2.1. Responsabilidades de la dirección
			2.6.2.2. Educación, formación y concientización sobre la seguridad de la información

			2.6.2.3. Proceso disciplinario
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de registro de inicio seguro
SERVICIO DE CORREO ELECTRÓNICO	**Fallas de servicios de soporte (telefonía, servicios de Internet)**	**Falta de acuerdos bien definidos con terceras**	2.6.2 Gestión de la prestación del servicio por terceras partes
			2.6.2.1 Prestación del servicio
			2.6.2.2 Monitoreo y revisión de los servicios por terceros

ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
PORTAL DE INFORMACIÓN DE UNIPLEX	**Modificación no autorizada del sitio Web**	**Falta de procedimientos para cambios**	2.4.1 Antes de la contratación laboral.
			2.4.1.1 Roles y responsabilidades
			2.6.1 Procedimientos operacionales y responsabilidades
			2.6.1.1 Documentación de los procedimientos de operación
			2.6.1.2 Gestión del cambio
			2.7.1. Requisitos del negocio para el control del acceso
			2.7.1.1. Política de control de acceso
			2.7.2. Gestión del acceso de usuarios
			2.7.2.2. Gestión de privilegios

			2.7.4. Control de acceso a las redes
			2.7.4.4. Protección de los puertos de configuración y diagnóstico remoto
			2.8.5. Seguridad en los procesos de desarrollo y soporte
			2.8.5.1. Procedimientos de control de cambios
	Sitio Web no disponible	**Fallas en los acuerdos de niveles de servicio**	2.6.2 Gestión de la prestación del servicio por terceras partes
			2.6.2.1 Prestación del servicio
			2.6.2.2 Monitoreo y revisión de los servicios por terceros

ACTIVO	***Amenazas***	***Vulnerabilidades***	***Uso de la norma 27002***
SOFTWARE ESTÁNDAR	**Uso no previsto**	**Falta de políticas de seguridad**	2.1.1. Política de seguridad de la información
			2.1.1.1. Documento de la política de seguridad de la información
			2.2.1. Organización interna
			2.2.1.4. Proceso de autorización para los servicios de procesamiento de información
			2.4.1. Antes de la contratación laboral
			2.4.1.1. Roles y responsabilidades
			2.4.1.3. Términos y condiciones laborales
			2.4.2. Durante la vigencia del contrato laboral
			2.4.2.1. Responsabilidades de la dirección

			2.4.2.2. Educación, formación y concientización sobre la seguridad de la información
			2.4.2.3. Proceso disciplinario
			2.7.3. Responsabilidades de los usuarios
			2.7.3.1. Uso de contraseñas
			2.7.3.2. Equipo de usuario desatendido
			2.7.5. Control de acceso al sistema operativo
			2.7.5.1. Procedimientos de registro de inicio seguro
SOFTWARE ESTÁNDAR	**Virus de Computación, Fuerza Bruta y ataques de diccionario**	**Falta de Protección (AV) actualizada**	2.6.4 Protección contra códigos maliciosos y móviles.
			2.6.4.1 Controles contra códigos malicioso
			2.8.5. Seguridad en los procesos de desarrollo y soporte
			2.8.6. Gestión de la Vulnerabilidad Técnica
			2.8.6.1. Control de las Vulnerabilidades Técnicas
SOFTWARE ESTÁNDAR	**Falta de capacidad de restauración**	**Falta de copias de backup continuas**	2.6.5 Respaldo.
			2.6.5.1 Respaldo de la información
			2.10.1. Aspectos de seguridad de la información en la gestión de la continuidad del negocio
			2.10.1.3. Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información

SOFTWARE ESTÁNDAR	**Pérdida de Servicio**	**Actualizaciones incorrectas Instalación de SW no autorizado**	2.6.1 Procedimientos operacionales y responsabilidades.
			2.6.1.1 Documentación de los procedimientos de operación
			2.6.1.2 Gestión del cambio

			2.8.5. Seguridad en los procesos de desarrollo y soporte
			2.8.5.1. Procedimientos de control de cambios
			2.8.5.2. Revisión técnica de las aplicaciones después de los cambios en el Sistema Operativo
			2.8.5.3. Restricciones en los cambios a los paquetes de software
SOFTWARE ESTÁNDAR	**Controles de Seguridad no cumplidos**	**Falta de Políticas de Seguridad**	2.1.1 Política de seguridad de la información.
			2.1.1.1 Documento de política de seguridad de la información
			2.9.1. Reporte sobre los eventos y las debilidades de la seguridad de la información
			2.9.1.1. Reporte sobre los eventos de la seguridad de la información
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
			2.11.2. Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
			2.11.2.1. Cumplimiento con la políticas y las normas de seguridad
SOFTWARE ESTÁNDAR	**Alteración no autorizado de la configuración**	**Falta de control de acceso**	2.7.1. Requisitos del negocios para el control del acceso
			2.7.1.1. Política de control de acceso
			2.7.2. Gestión del acceso de usuarios
			2.7.2.2. Gestión de privilegios
			2.8.5. Seguridad en los procesos de desarrollo y soporte

			2.8.5.3. Restricciones en los cambios a los paquetes de software

ACTIVO	Amenazas	Vulnerabilidades	Uso de la norma 27002
	Acceso no autorizado a la información	**Falta de control de acceso**	2.5.2 Seguridad de los equipos.
			2.5.2.3 Seguridad del cableado
			2.6.6 Gestión de la seguridad de las redes.
			2.6.6.1 Controles de las redes
			2.6.6.2 Seguridad de los servicios de la red
			2.7.4. Control de acceso a las redes
			2.7.4.2. Autenticación de usuarios para conexiones externas
			2.7.4.3. Identificación de los equipos en las redes
			2.7.4.4. Protección de los puertos de configuración y diagnóstico remoto
			2.7.4.6. Control de conexión a las redes
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos
			2.11.2. Cumplimiento de las políticas y las normas de seguridad y cumplimiento técnico
MEDIOS Y SOPORTE			2.11.2.1. Cumplimiento con las políticas y las normas de seguridad
MEDIOS Y	**Robo**	**Falta de protección**	2.3.1 Responsabilidad por los activos.

SOPORTE		**física**	2.3.1.1 Inventario de activos
			2.3.1.2 Propietario de los activos
			2.3.1.3 Uso aceptable de los activos
			2.5.2 Seguridad de los equipos.
			2.5.2.3 Seguridad del cableado
			2.9.1. Reporte sobre los eventos y las debilidades de la seguridad de la información
			2.9.1.1. Reporte sobre los eventos de seguridad de la información
			2.9.2. Gestión de los incidentes y las mejoras en la seguridad de la información
			2.9.2.1. Responsabilidades y procedimientos

MEDIOS Y SOPORTE	**Análisis de tráfico**	**Falta de establecimiento de una conexión segura (VPN)**	2.6.6 Gestión de la seguridad de las redes.
			2.6.6.1 Controles de las redes
			2.6.6.2 Seguridad de los servicios de la red
			2.8.3. Controles criptográficos
			2.8.3.1. Política sobre uso de controles criptográficos
MEDIOS Y SOPORTE	**Brechas de seguridad no detectadas**	**Falta de monitoreo de la red**	2.6.2 Monitoreo
			2.6.2.4 Monitoreo del uso del sistema
			2.6.2.6 Registros del administrador y del operador
			2.6.2.7 Registro de fallas

Una vez seleccionado los controles, podemos realizar la redacción del manual de procedimiento para la implementación del PGSI en base a los controles ya seleccionados.

CAPITULO 4

4. IMPLEMENTACIÓN DEL PROYECTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE UNIPLEX

4.1. Manual de Procedimientos para la Implementación del PGSI

A continuación se describe el manual de procedimientos para implementar el PGSI en la Corporación, de los controles seleccionados anteriormente los que no se mencionan en el manual se encuentran detallados en la implementación de los mismos.

Política de Seguridad de la Información

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para el Organismo y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos del Organismo. Es importante que los principios de la Política de Seguridad sean parte de la cultura organizacional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Organismo y de los titulares de Unidades Organizativas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Organismo y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política. Mantener la Política de Seguridad de la empresa actualizada, a efectos de asegurar su vigencia y nivel de eficacia.
Establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales de UNIPLEX y el uso adecuado de los mismos.

Alcance

Esta Política se aplica en todo el ámbito del Organismo, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

La finalidad de las políticas de seguridad que se describen en el capítulo 4, es proporcionar instrucciones específicas sobre cómo mantener más seguros tanto los computadores de la empresa, (conectados o no en red), como la información guardada en ellos. La violación de dichas políticas puede acarrear medidas

disciplinarias. Para el desarrollo de las políticas, es necesario considerar las diferentes fuentes de información, que permiten el desempeño diario de las funciones de la corporación. Entre los puntos principales que se deben analizar son: Políticas de seguridad para computadores, comunicaciones

En el cual se debe establecer las directrices, los procedimientos y los requisitos para asegurar la protección oportuna y correcta de los equipos computacionales y sistemas de comunicaciones de Uniplex y el uso adecuado de los mismos.

Políticas de seguridad para redes

El propósito de este manual es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de la empresa al estar conectada a redes de computadoras.

En el desarrollo de estas políticas se debe definir los términos, condiciones y limitantes del servicio de Correo Electrónico Interno y limitantes del servicio de Internet corporativo de la empresa.

- **ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD**

Generalidades

Es necesario tener bien definido un marco de gestión para efectuar diferentes tareas tales como la aprobación de la Política, la coordinación de su implementación y la asignación de funciones y responsabilidades, para tener una eficiente administración de la seguridad de información.

Debe tenerse en cuenta que ciertas actividades de la empresa pueden requerir que terceros accedan a información interna, o bien puede ser necesaria la tercerización de ciertas funciones relacionadas con el procesamiento de la información. En estos casos se considerará que la información puede ponerse en riesgo si el acceso de dichos terceros se produce en el marco de una inadecuada administración de la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

Objetivo

- Administrar la seguridad de la información dentro de la Corporación y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.
- Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información del Organismo.

En este control es necesario definir un Comité de Seguridad que entre sus funciones deberá:

- Revisar y proponer a la máxima autoridad de la empresa para su aprobación, la Política y las funciones generales en materia de seguridad de la información.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad.

- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área.
- Acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información.
- Garantizar que la seguridad sea parte del proceso de planificación de la información.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios.
- Promover la difusión y apoyo a la seguridad de la información dentro del Organismo.
- Coordinar el proceso de administración de la continuidad de la operatoria de los sistemas de tratamiento de la información del Organismo frente a interrupciones imprevistas.

Una vez integrado el Comité, es necesario se definan las funciones de los miembros del mismo para poder para que este pueda desempeñar sus actividades y mejorar la seguridad en la empresa. En la implementación están especificados los miembros del Comité.

El Comité de Seguridad de la Información debe proponer a la Gerencia para su aprobación la definición y asignación de las responsabilidades que surjan de sus funciones.

Es necesario definir el proceso para la autorización de nuevos recursos para el procesamiento de información así como los requerimientos de Seguridad en contratos con Terceros, los principales puntos que se deben considerar lo siguiente:

a) Cumplimiento de la Política de seguridad de la información de Uniplex.

b) Protección de los activos de la Corporación, incluyendo:

- Procedimientos para proteger los bienes de la Corporación, abarcando los activos físicos, la información y el software.
- Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
- Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
- Restricciones a la copia y divulgación de información.

c) Descripción de los servicios disponibles.

d) Nivel de servicio esperado y niveles de servicio aceptables.

e) Permiso para la transferencia de personal cuando sea necesario.

f) Obligaciones de las partes del acuerdo y responsabilidades legales.

g) Definiciones relacionadas con la protección de datos.

h) Acuerdos de control de accesos que contemplen:

- Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
- Proceso de autorización de accesos y privilegios de usuarios.
- Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.

i) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.

j) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.

k) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.

l) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.

m) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.

n) Proceso claro y detallado de administración de cambios.

o) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.

p) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.

q) Controles que garanticen la protección contra software malicioso.

r) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.

- **Gestión de los Activos de Red**

Generalidades

La Corporación debe tener conocimiento sobre los activos que posee como parte importante de la administración de riesgos.

Los activos de información deben ser clasificados de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad

que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información.

Objetivo

Garantizar que los activos de información reciban un apropiado nivel de protección. Clasificar la información para señalar su sensibilidad y criticidad.
Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

- **Responsabilidad sobre los activos**

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada.

El Responsable de Networking es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la Política.

Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad de 4 meses. El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

En la implementación del manual, se especifica el inventario realizado así como los responsables de cada activo. Una vez realizado el inventario, se debe clasificar el activo, en base a tres características de la información en las cuales se basa la seguridad: confidencialidad, integridad y disponibilidad; los cuales se revisaron al inicio de este capítulo. Para clasificar la información se consideró una de las siguientes categorías:

CRITICIDAD BAJA: ninguno de los valores asignados supera el 2.
CRITICIDAD MEDIA: alguno de los valores asignados es 2
CRITICIDAD ALTA: alguno de los valores asignados es 3

Sólo el propietario de la Información puede asignar o cambiar su nivel de clasificación, cumpliendo con los siguientes requisitos previos: cambios necesarios para que los usuarios conozcan la nueva clasificación

- SEGURIDAD DE LOS RECURSOS HUMANOS

Generalidades

La seguridad de la información se basa en la capacidad para conservar la integridad, confidencialidad y disponibilidad de los activos.

Para lograr lo anterior es fundamental educar e informar al personal desde su ingreso y en forma continua, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad. Así mismo, es necesario definir las sanciones que se aplicarán en caso de incumplimiento.

Objetivo

Reducir los riesgos de error humano, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

Indicar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

Garantizar que los usuarios estén al corriente de las amenazas en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la Corporación en el transcurso de sus tareas normales.

Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información. Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Seguridad en la definición del trabajo y los recursos

Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo.

Éstas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

En la implementación se especifica el procedimiento para la proceso de selección del personal.

Términos y condiciones de la relación laboral

Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información.

Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede de la empresa y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de contrato.

Conocimiento, educación y entrenamiento de la seguridad de información

Todos los empleados de la empresa y, cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la empresa, deberán recibir una adecuada capacitación y actualización periódica en materia de la política de seguridad, normas y procedimientos para la seguridad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

El Responsable del Área de Recursos Humanos será el encargado de coordinar las acciones de capacitación que surjan de la Política.
Cada 6 meses se revisará el material correspondiente a la capacitación, a fin de evaluar la pertinencia de su actualización, de acuerdo al estado del arte de ese momento.

El personal que ingrese a la Corporación recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información, antes de serle otorgados los privilegios de acceso a los sistemas que correspondan. Además se otorgará una guía de usuario para que tengan un mejor conocimiento con respecto a las amenazas informáticas y sus posibles consecuencias dentro de la Corporación de tal manera que se llegue a concienciar y crear una cultura de seguridad de la información.

- **Seguridad Física y del Entorno**

Generalidades

La seguridad física y ambiental minimiza los riesgos de daños e interferencias a la información y a las operaciones de la Corporación. Además, trata de evitar al máximo el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.

El control de los factores ambientales permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

Gran cantidad de información manejada en las oficinas se encuentra almacenada en papel, por lo que es necesario establecer pautas de seguridad para la conservación de dicha documentación.

Objetivo

Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información del Organismo.

Proteger el equipamiento de procesamiento de información crítica del Organismo ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Organismo.

Previo a la implementación de un control de seguridad física y del entorno, es necesario que se realice un levantamiento de información de la situación actual de la Corporación en cuanto a su seguridad física para determinar las vulnerabilidades y posibles soluciones.

En puntos previos de este capítulo ya se realizó la recolección de la información necesaria para implementar los controles. En el capítulo 4 se define la implementación de los controles de seguridad física y del entorno.

- **Gestión de Comunicaciones y Operaciones**

Generalidades

Debido a los peligros existentes como software malicioso, virus, troyanos, etc. es importante que se adopten controles para prevenir cualquier tipo de amenazas.

Se debe separar los ambientes de pruebas y de operaciones, establecer procedimientos que garanticen la calidad de los procesos operativos para evitar incidentes producidos por la mala manipulación de información.

Las comunicaciones establecidas permiten el intercambio de información, se deberá establecer controles para garantizar las condiciones de confidencialidad, integridad y disponibilidad de la información que se emite o recibe por los distintos canales.

Objetivo

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones. Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.

El administrador de la red debe revisar con el encargado legal de Uniplex, todos los contratos y acuerdos con terceros, pues es necesario garantizar la

incorporación de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

En el capítulo siguiente se definen las consideraciones que se deben tener para implementar este control, así como los anexos donde se especifican la implementación que hemos realizado.

Generalidades

Es necesario establecer controles que impidan el acceso no autorizado a los sistemas de información por parte de personal diferente a los que tienen permisos, para lo cual es necesario se implementen procedimientos para controlar la asignación de privilegios de acceso a los diferentes sistemas y aplicativos de la empresa. En estos procedimientos se especifican sugerencias para mejorar el control actual de los accesos de los usuarios a diferentes niveles.

Es importante para la seguridad de la información controlar el acceso a los recursos, y protegerlos contra el acceso no autorizado, modificación o robo.

Para el caso de Uniplex se definirán políticas para el control de acceso así como los procedimientos que deben seguirse para poder implementarlos en los sistemas operativos y aplicativos. En los procedimientos considerados se debe tener en cuenta que los mismos consideren identificación, autenticación y autorización de los usuarios.

Objetivo

Entre los principales puntos que se desean cubrir con este control se tienen:

- Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.
- Controlar de mejor forma la seguridad en conexiones entre Uniplex y los proveedores externos.
- Mantener un registro de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Alcance

En el procedimiento para implementar este control, se define una política de control de acceso que se aplica a todos los usuarios internos y externos que tienen diferentes permisos para acceder a los sistemas de información, red de Uniplex, bases de datos.

Asimismo se aplica al personal técnico que define, instala, administra y mantiene los permisos de acceso y las conexiones de red, y a los que administran su seguridad.

- **Política de Control de Acceso**

  - Negar el acceso a sistemas de cuentas anónimas o usuarios no identificados
  - Limitar o monitorear el uso de cuentas con privilegios especiales
  - Suspender o retardar el acceso a sistemas, aplicaciones después de un número de intentos fallidos.
  - Remover cuentas obsoletas de usuarios que han dejado la compañía
  - Suspender cuentas inactivas después de 30 o 60 días.
  - Reforzar un criterio estricto de acceso
  - Deshabilitar las configuraciones por defecto, servicios y puertos no requeridos.
  - Reemplazar las configuraciones de contraseñas por defecto en las cuentas
    - Limitar y monitorear reglas de accesos globales
    - Forzar rotación de la contraseña
  - Forzar requerimientos de contraseñas
  - Sistemas de auditorías y eventos de usuarios y acciones, así como revisión de reportes periódicos.

Si bien el método biométrico es una forma segura de autentificación e identificación, para el caso de la empresa no aplica pues los sistemas a los cuales acceden y son de mayor riesgo es el aplicativo, al cual ingresan los proveedores que se encuentran fuera de la empresa y no resulta cómodo para los usuarios este tipo de metodología además de resultar más costoso.

Contraseñas

El usuario puede generar su contraseña, pero el sistema operativo fuerza al usuario a que el mismo cumpla con ciertos requerimientos, como por ejemplo que contenga un cierto número de caracteres, que incluya caracteres especiales, que no se relaciones con el nombre del usuario de la máquina.

Además de mantener un registro de las últimas claves ingresadas, la fecha en la que debe cambiarse.

Si una contraseña trata de ser vulnerada también puede configurarse el registro de intentos fallidos de acceso al sistema con lo cual se puede bloquear el acceso al mismo para de esta manera disminuir el riesgo debido a la vulneración de las contraseñas.

Uso de Contraseñas

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las políticas de seguridad establecidas, en las que básicamente tratan los siguientes puntos:

1. Sean fáciles de recordar.

2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión (•log on").

f) Notificar cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente. Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

Identificación y Autenticación de los usuarios

Todos los usuarios de la empresa deben tener un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En los casos que se requiere compartir un ID de usuario, tanto el administrador de la red como el responsable de cada área debe autorizar dicha compartición, así como definir el tiempo en el cual se requiere que se comparta el ID, luego del cual se debe eliminar el identificador y los privilegios del mismo.

Restricción del acceso a la información

Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación acorde al procedimiento de asignación de privilegios.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación, para lo cual el administrador de la red debe manejar los privilegios de acuerdo al perfil del usuario y con los requerimientos realizados formalmente por el responsable de cada área.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.

c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el

uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Protección de los puertos de diagnóstico remoto

Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, por lo cual lo primero que debemos determinar es el diagnóstico de que puertos se encuentran abiertos en la red.

- ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Generalidades

En este control se deben revisar las aplicaciones como puntos críticos de vulnerabilidades, es necesaria una adecuada administración de la infraestructura de base, Sistemas Operativos y Software de Base, en las distintas plataformas, para asegurar una correcta implementación de la seguridad, ya que en general los aplicativos se asientan sobre este tipo de software.

Objetivo

Con este control se pretende cubrir varios puntos de seguridad, entre los principales objetivos se tienen:

- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

Alcance

Los controles que se detallan a continuación se aplican a los sistemas informáticos, y a los sistemas operativos que integran los ambientes por el organismo de donde residen los mismos.

Para implementar un mayor control a la información confidencial o importante de los diferentes departamentos de la empresa.
Se debe entender como información confidencial a toda información que se refiere a planes de negocio, tecnología no anunciada, información financiera no pública; e información personal como son tarjetas de crédito, contraseñas.

La empresa debe tener aprobado un procedimiento de cambios aprobado por la gerencia, y los cambios deben ser documentados y comunicados a los empleados

involucrados. En la implementación se especifica el proceso para llevar a cabo un cambio.

Revisión técnica de los cambios en el sistema operativo

Toda vez que sea necesario realizar un cambio en el Sistema Operativo, los sistemas serán revisados para asegurar que no se produzca un impacto en su funcionamiento o seguridad.

Para ello, el administrador de la red debe tener un procedimiento en el cual se incluye:

a) Revisar los procedimientos de integridad y control de aplicaciones para garantizar que no hayan sido comprometidas por el cambio.
b) Garantizar que los cambios en el sistema operativo sean informados con anterioridad a la implementación. Para lo cual el administrador debe planificar el día en el cual se llevará a cabo el cambio e informarlo a los usuarios y coordinar con los responsables de cada área en caso de que ellos deban realizar algún trabajo por el cual no pueden suspender sus actividades. Estos cambios deben programarse para fines de semana donde no haya impacto en los usuarios.
c) Asegurar la actualización del Plan de Continuidad de las Actividades del Organismo.

Restricción del cambio de paquetes de Software

En caso de considerarlo necesario la modificación de paquetes de software suministrados por proveedores, y previa autorización del Responsable del Área Informática, se deberá:

a) Analizar los términos y condiciones de la licencia a fin de determinar si las modificaciones se encuentran autorizadas.
b) Determinar la conveniencia de que la modificación sea efectuada por Uniplex, por el proveedor o por un tercero.
c) Evaluar el impacto que se produce si la empresa se hace cargo del mantenimiento.
d) Retener el software original realizando los cambios sobre una copia perfectamente identificada, documentando exhaustivamente por si fuera necesario aplicarlo a nuevas versiones.
Este es un punto que debe ser analizado con todos los responsables de las áreas y el administrador de la red, deben realmente aprobar los cambios que implica varios procedimientos como son en el ámbito legal, financiero, recursos, etc.

Canales encubiertos y código

Un canal oculto puede exponer información utilizando algunos medios indirectos y desconocidos. El código malicioso está diseñado para afectar a un sistema en forma no autorizada y no requerida por el usuario.

Para lo cual es necesario que la corporación cuente con un software adecuado instalado en cada máquina de los empleados para evitar problemas debido a canales encubiertos y código troyano.

Además de las medidas implementadas con el antivirus, es necesario que previo la instalación de algún software en Uniplex se deba considerar:

a) Adquirir programas a proveedores acreditados o productos ya evaluados.
b) Examinar los códigos fuentes (cuando sea posible) antes de utilizar los programas.
c) Controlar el acceso y las modificaciones al código instalado.
d) Utilizar herramientas para la protección contra la infección del software con código malicioso, en este caso la empresa utilizó el antivirus Mcfee.

- **Gestión de Incidentes de la Seguridad de la Información**

Divulgación de eventos y de debilidades de la seguridad de la información

Es importante que la empresa tenga un procedimiento a seguir cuando se presente un incidente de seguridad en la red, pues es necesario que pueda aprender de los errores y evitar que un ataque ocurra. Por lo cual es importante que luego de cada incidente siga un procedimiento, técnicas, configuraciones necesarias para reforzar lo modificado y mejorar la seguridad.

Es necesario que se tenga un mejor control del uso apropiado de los recursos de la red, en otros términos, todos los recursos de la informática deben usarse de una

manera ética y responsable. El uso de recursos de tecnología de información puede categorizarse ampliamente como aceptable, tolerable, o prohibió:

- El uso aceptable de recursos de tecnología de información es el uso legal consistente con los requerimientos de la organización, en base a las políticas de la misma que permitan solventar los problemas de la Corporación.

- El uso tolerable es el uso legal para otros propósitos que no chocan con en la política del uso aceptable de la organización.

- El uso prohibido es el uso ilegal y todo el otro uso que son “aceptables" ni tolerables.

Administración de incidentes y mejoras de la seguridad de la información

Después que el incidente ha sido resuelto, es necesario realizar una documentación del mismo para poder determinar las experiencias aprendidas del mismo. Como resultado de un análisis posterior al reporte de incidentes, el personal de seguridad puede necesitar emitir alarmas o advertencias a todos los empleados de la empresa sobre las acciones tomar para reducir vulnerabilidades que se explotaron durante el incidente.

Entre estas alertas es importante que se especifique de forma clara:

- Asegurar que sólo personal autorizado tiene el acceso a los archivos electrónicos.

- Minimizar el riesgo de modificación desautorizado de archivos electrónicos guardando los datos sensibles en los medios de comunicación trasladables.
- Asegurar que personal apropiado se entrena para proteger los archivos electrónicos sensibles o clasificados
- Proveer del respaldo y recuperación de archivos para proteger contra la pérdida de información
- Asegurar que la seguridad de los archivos electrónicos esté incluido en los planes de seguridad de información globales de su organización.

- Gestión de Continuidad del Negocio

Generalidades

Un punto importante para toda organización, es administrar de forma ordenada las actividades necesarias para la continuidad del negocio, en este procedimiento se deben involucrar a todos los empleados de la empresa.

El plan de continuidad debe mantenerse actualizado y ser una parte integrada en los diversos procesos de los diferentes departamentos de la empresa.

Objetivo

Este control es importante para cubrir los puntos críticos de Uniplex en caso de algún desastre, a continuación se detallan los principales objetivos:

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.

- Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

a) Detección y determinación del daño y la activación del plan.

b) Restauración temporal de las operaciones y recuperación del daño producido al sistema original.

c) Restauración de las capacidades de proceso del sistema a las condiciones de operación normales.

- Asignar funciones para cada actividad definida.

Alcance

Estos controles se aplican a los críticos de Uniplex.

Aspectos de la gestión de continuidad del negocio

Al desarrollar el plan de la continuidad del negocio para la empresa, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres. Para este caso cuando se realizó en análisis de riesgos y vulnerabilidades se consideraron diferentes tipos de desastres como son:

Desastres naturales:

- Inundaciones
- Terremotos
- Fuego
- Derrumbamientos, avalanchas, y otros movimientos de la tierra

Desastres artificiales, es decir aquellos relacionados con la computación:

- Sabotaje de los sistemas informáticos, y de la información
- Ataques terroristas
- Huelgas
- Protestas
- Ataque de Negación de Servicio en los servidores de la red
- Virus, gusanos, y otros ataques informáticos

Y finalmente se debe considerar un tercer grupo:

- Faltas de la infraestructura (interrupciones para uso general, interrupciones de la energía, etc.)
- Fallas de comunicaciones (hardware interno y externo, así como software y redes)
- Interrupciones del transporte (encierros o limitaciones del aeropuerto, encierros del camino, etc.)

Una vez identificados los tipos de desastres la empresa debe seguir y desarrollar un plan para asegurar la viabilidad a largo plazo de Uniplex, es necesario que la gerencia se involucre en la elaboración del plan, pero es el Comité de Seguridad de la Información que determina que tipos de planes son aplicables pues se requiere de financiamiento de los mismos.

Las pruebas son útiles si reflejan también condiciones reales y si los resultados de la prueba se utilizan para mejorar el plan.

Es importante comenzar con un plan simple para probar y después aumentar el alcance de la prueba gradualmente. Para cada caso es importante:

- Identifique el alcance y las metas para la prueba.
- Documente el plan de prueba y los resultados.
- Repase los resultados con los participantes y prepare las lecciones aprendidas de la prueba.
- Ponga al día el plan basado en los resultados de la prueba.

Proceso de gestión de la continuidad del negocio

Para sobrevivir, la organización debe asegurar el funcionamiento de aplicaciones críticas en un tiempo razonable, frente a un desastre. Las organizaciones necesitan entrenar a sus empleados para ejecutar los planes de contingencia, para lo cual se requiere:

- Que los empleados sean consientes de la necesidad del plan
- Informar a todos los empleados de la existencia del plan y proporcionar los procedimientos para seguir en caso de una emergencia
- Entrenar al personal con las responsabilidades identificadas para cada uno de ellos, para realizar la recuperación del desastre y procedimientos de continuidad de negocio
- Dar la oportunidad para que se pueda llevar a cabo el plan de contingencia, para poder realizar un simulacro de la forma en la que se ejecuta el mismo.

Desarrollo e implantación de planes de contingencia

Al desarrollar el plan se debe tener bien definido y especificado las responsabilidades ha asignarse a cada persona responsable de un proceso determinado, para el caso de Uniplex se debe considerar los siguientes responsables:

- Personal encargado de la administración de la recuperación.- El cual debe actuar el momento en el cual se presente el desastre, y cuyo trabajo consiste en ejecutar el plan de recuperación de desastre y restaurar los procesos críticos en el menor tiempo, para este caso es el Comité de Seguridad.

- Personal operacional. Son aquellos que están encargados de la operación del negocio hasta que las cosas vuelvan a la normalidad, estas personas tienen responsabilidades cotidianas y desarrollan las mismas funciones bajo circunstancias normales.

- Personal de las comunicaciones. Personal que diseña los medios de comunicar la información a los empleados, a los clientes, y al público en general. Son los encargados de considerar qué información puede darse y por quién. Esto es crítico en los primeros días de una interrupción pues habrá una mayor demanda para la información, y ocurre en un momento en que los canales normales son interrumpidos por daños en los mismos.

Una vez que se encuentra definido el personal necesario para los diferentes procesos del plan, es necesario que se realicen pruebas del mismo. Pues un plan

que no ha sido probado puede presentar fallas en el momento de su ejecución. Las pruebas no deben ser costosas ni interrumpir la operación diaria del negocio. Entre las pruebas que se pueden considerar son:

- Prueba de papel. Esto puede ser tan simple como discutir el plan en una reunión del personal considerando sucesos actuales. Es importante documentar la discusión y utilizar cualquier lección aprendida como parte del proceso para mejorar el plan.
- Camino Estructurado. Aquí es donde el personal define diversos panoramas para supervisar el plan en equipo.

- Prueba de componentes. En esta prueba, cada parte del plan total se puede probar independientemente. Los resultados entonces se miran para considerar cómo el plan total pudo haber trabajado si todos los componentes fueron probados simultáneamente.

- Simulación. No incluye realmente la mudanza a una localización alterna sino puede incluir la simulación de interrupciones para uso general como manera de ver que tan completo es un plan.

- Ejercicio de la recuperación del desastre. En esta prueba, se activa el plan y los sistemas informáticos se cambian a sus sistemas de reserva, que pueden incluir el funcionamiento en los sitios alternativos. Esto a veces se llama una prueba "paralela" pues los sistemas de producción seguirán siendo funcionales mientras que los sistemas de la recuperación se ponen en producción para probar su funcionalidad.

Cumplimiento

Generalidades

Los controles implementados en puntos anteriores deben ser complementados con regulaciones de disposiciones legales y contractuales que están actualmente rigiendo en el país. Pero es necesario definir internamente de forma clara los requisitos normativos y contractuales pertinentes a cada sistema de información de la empresa.

Objetivos

Entre los principales puntos a cubrir se tienen:

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas al Organismo y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad del Organismo.

Alcance

Este control se aplica a todo el personal de la empresa.

- **Derechos de propiedad intelectual**

Es necesario para toda organización conocer las leyes para no tener problemas futuros debido a incumplimiento de las mismas.

La infracción a estos derechos podría dar como resultado acciones legales que derivarían en demandas penales.
Se deberán tener presentes las siguientes normas:

1998: Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

Salvaguarda de los registros de la organización

Los registros críticos de Uniplex se deben proteger contra pérdida, destrucción y posibles falsificaciones.

Para un mejor control los registros van a clasificarse dependiendo del área y el uso de cada departamento; además de detallar la forma de almacenamiento, el responsable de cada registro y el período de retención, es decir el tiempo que debe transcurrir antes de que sean destruidos.

Es necesario tener presentes las siguientes normas:

2002 - 67: De esta ley se deben considerar diferentes artículos como son:

“Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia.”

“Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros…. El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo.”

Cabe recalcar q en el nuevo decreto ejecutivo del 2009, estos artículos respecto a la ley de comercio electrónico, firmas electrónicas y mensajes de datos no han sido modificados hasta la fecha de tal manera que no ha perdido vigencia el suplemento 557 del 17 de abril del 2002. .

- **Protección de los datos y de la privacidad de la información personal**

Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.

Para mejorar este punto, en la empresa se debe redactar Compromiso de Confidencialidad, el cual deberá ser suscrito por todos los empleados.

Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate.

Es necesario tener presentes las siguientes normas:

2002 - 67: De esta ley se deben considerar diferentes artículos como son:

"Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Reformas al Código Penal

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos innumerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, serán sancionadas con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realizan por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. ....- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su

titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Al igual que los artículos 5 y 9 referidos en el ítem anterior, estos artículos no han sido sujeto a modificaciones por la actual constitución vigente en el 2009; quedando como ley vigente el suplemento 557 del 17 de abril del 2002.

Evitar el mal uso de los recursos de tratamiento de la información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

Revisiones de la política de seguridad y de la conformidad técnica Conformidad con la política de seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

4.2. Implementación del Plan de Tratamiento de Riesgos

El objetivo de este punto es tomar la acción más apropiada de tratamiento para cada uno de los riesgos identificados, en base al cuadro anterior y al capítulo anterior donde se encontraba la valoración de los riesgos:

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
Hardware Portátil	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Inautorizada copia de SW o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
PCs de oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire	Funcionamiento no adecuado del aire	Reducción

	acondicionado	acondicionado	
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados	Reducción
	Uso no previsto	Falta de las políticas	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Degradación del HW	Falta de mantenimiento adecuado	Reducción
	Inautorizada copia de SW o información propietaria	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
Servidores	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Corrupción de archivos de registros	Falta de Protección de los archivos de registro	Reducción
	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Acceso no autorizado a través de la red	Código malicioso desconocido	Reducción
	Degradación o Falla del HW	Falta de mantenimiento adecuado	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Brechas de seguridad no detectadas	Falta de monitoreo de los servidores	Reducción
	Ataque destructivo	Falta de protección física	Reducción
Equipos de Oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación

	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación o Falla de HW	Falta de Mantenimiento	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Uso no previsto	Falta de Políticas Falta de Control de Acceso	Reducción
Soporte electrónico	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad	Aceptación
	Ataque destructivo	Falta de protección física	Reducción
	Robo	Falta de atención del personal	Reducción
	Escape de información	Manipulación inadecuada de información	Reducción
Documentación y Registros.	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Pérdida de información	Errores de los empleados	Reducción
	Pérdida de información	Almacenamiento no protegido	Reducción
	Divulgación de información de clientes	Almacenamiento no protegido	Reducción
	Incumplimiento de leyes en cuanto a la información de clientes o empleados	Falta de conocimiento de los empleados	Reducción
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema	Reducción
	Contratos incompletos	Falta de control para el establecimiento de contratos	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Incapacidad de restauración	Falta de planes de continuidad del negocio	Reducción
	Modificación no autorizada de información	Insuficiente entrenamiento de empleados	Reducción
Empleados	Errores de los empleados y acciones equivocadas	Falta de conocimiento y oportuno entrenamiento	Reducción
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de	Reducción

		empleados	
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad	Reducción
Establecimientos	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Acceso no autorizado	Falta de políticas	Reducción
	Acceso no autorizado	Falta de protección física	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
Servicio de Comunicaciones	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Degradación del servicio y equipos	Falta de mantenimiento adecuado	Reducción
	Errores de configuración	Falta de conocimiento del administrador	Reducción
	Manipulación de la configuración	Falta de control de acceso	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Ataque destructivo	Falta de protección física	Reducción
	Fallas de servicios telefonía	Falta de acuerdos bien definidos con terceras partes	Reducción
Servicio de energía eléctrica	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Reducción
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Ataque destructivo	Falta de protección física	Aceptación
Servicio de correo electrónico	Errores de los usuarios	Falta de conocimiento del uso del servicio	Reducción
	Suplantación de la identidad del usuario	Falta de control de acceso	Reducción
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Uso no previsto	Falta de políticas	Reducción
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes	Reducción
	Errores de usuarios	Falta de conocimiento para el uso de la aplicación	Reducción
	Errores de configuración	Falta de capacitación del administrador del sistema	Reducción
	Escapes de información	Falta de control de acceso	Reducción

Aplicación Lotus	Errores de actualización del programa	Falta de procedimientos aprobados	Reducción
	Manipulación de la configuración	Falta de control de acceso	Aceptación
	Suplantación de identidad del usuario	Falta de control de acceso	Reducción
	Abuso de privilegios de acceso	Falta de políticas de seguridad	Reducción
	Negación de servicio	Incapacidad para distinguir una petición real de una petición falsificada	Reducción
Portal de información (Página Web de la empresa)	Modificación no autorizada del sitio Web	Falta de procedimientos para cambios	Reducción
	Negación de servicio	Falta de recursos necesarios	Reducción
	Sitio Web no disponible	Fallas en los acuerdos de niveles de servicio	Reducción
	Publicación de información incorrecta de Uniplex	Falta de procedimiento aprobados	Reducción
Suministros de Oficina	Fuego	Falta de protección contra fuego	Reducción
	Daños por agua	Falta de protección física adecuada	Aceptación
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por desastres	Aceptación
	Robo	Falta de atención	Reducción
	Robo	Falta de protección física	Reducción
Imagen de la empresa Reputación	Divulgación de datos de los clientes	Insuficiente seguridad de información de los clientes	Reducción
Paquetes o software estándar	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección(AV) actualizada	Reducción
	Spoofing, Escape de información	Falta de control de acceso	Reducción
	Falta de capacidad de restauración	Falta de copias de backup continuas	Reducción
	Uso no previsto	Falta de políticas de seguridad	Reducción
Sistemas operativos	Negación de Servicio	Capacidad insuficiente de los recursos	Reducción
	Errores de Configuración	Falta de capacitación del administrador	Reducción
	Errores de Configuración	Incompleto o incorrecto documentación del sistema	Reducción
	Virus de Computación, Fuerza Bruta y ataques de diccionario	Falta de Protección (AV) actualizada	Reducción
	Falta de capacidad de	Falta de copias de backup	Reducción

	restauración	continuas	
	Pérdida de Servicio	Actualizaciones incorrectas	Reducción
	Pérdida de Servicio	Instalación de SW no autorizado	Reducción
	Controles de Seguridad no cumplidos	Falta de Políticas de Seguridad	Reducción
	Alteración no autorizado de la configuración	Falta de control de acceso	Reducción
Medios y soporte	Acceso no autorizado a la información	Falta de control de acceso	Reducción
	Robo	Falta de protección física	Reducción
	Daños de cables	Falta de protección física	Aceptación
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)	Reducción
	Brechas de seguridad no detectadas	Falta de monitoreo de la red	Reducción

Tabla 4.1 Tratamiento de Riesgos

En el siguiente punto describimos el resultado de nuestro plan para poder implementar el Proyecto de Gestión de Seguridad de Información en base a la Norma ISO 27002 en Uniplex.

4.3. Descripción de la Implementación del PGSI Considerando los 4 Dominios Seleccionados

En el presente proyecto se analizo bajo todos los 11 controles de la norma ISO 27002, pero dándole especial realce a cuatro controles principales:

- Política de seguridad.
- Organización de la seguridad de la información.
- Gestión de Activos.
- Control del Acceso.

Las políticas de seguridad se la escogió para brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes.

La organización de la seguridad de la información, para establecer una estructura de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

La gestión de activos indica cómo lograr y mantener la protección adecuada de los activos de la organización, incluyendo todos los activos e incluir un dueño designado, también asignar la responsabilidad para el mantenimiento de los controles adecuados.

El control de acceso ya que el acceso a la información y a los procesos del negocio se debe controlar con base en los requisitos de seguridad y del negocio.

Estos controles están contemplados en base a las vulnerabilidades identificadas en la empresa se detallarán los controles que ayudarán a cubrir estas vulnerabilidades, los demás controles no se consideraron mucho debido a que no dan una mayor solución a los riesgos.

El resultado final se lo muestra en la implementación de los controles la cual contiene un manual de contingencia en caso de emergencias de todo tipo, manual para usuario el cual contempla todo ámbito de posible alerta y fallas tanto de hardware como demás aspectos.

4.4. Implementación de los Controles Seleccionados Acorde al Manual de Procedimientos

Política de Seguridad de la Información

Documento de política de seguridad de la información

1.- Seguridad lógica Identificación

Para dar de alta un usuario al sistema debe existir un procedimiento formal, por escrito, que regule y exija el ingreso de los siguientes datos:

- Identificación del usuario, deberá ser única e irrepetible,
- Password, debe ser personal e ingresado por el usuario,
- Nombre y apellido completo,
- Grupo de usuarios al que pertenece,
- Fecha de expiración del password,
- Fecha de anulación de la cuenta,
- Contador de intentos fallidos,
- Autorización de imprimir,
- Autorización de ingreso al área de usuarios.

Deben asignarse los permisos mínimos y necesarios para que cada usuario desempeñe su tarea.

Deberá restringirse el acceso al sistema o la utilización de recursos en un rango horario definido, teniendo en cuenta que:

- Las cuentas de los usuarios no deben poder acceder al sistema en horarios no laborales, de acuerdo al grupo al que pertenezcan,
- Durante las vacaciones o licencias las cuentas de usuarios deben desactivarse,

La contraseña asociada al acceso de un identificador de usuario a un computador significa la primera verificación de su identidad, permitiendo posteriormente el acceso al computador y a la información que allí reside. Para su protección y de los recursos de Uniplex debe mantener su contraseña de verificación de identidad en secreto, no compartirla con persona alguna.
Nota: La contraseña de disco duro es usada para proteger su equipo contra accesos no autorizados, mas no es una contraseña de verificación.

El administrador del sistema deberá realizar un chequeo mensual de los usuarios del sistema, comprobando que existen solo los usuarios que son necesarios y que sus permisos sean los correctos.

El área de recursos humanos deberá comunicar al administrador los cambios de personal que se produzcan. Luego de esta notificación el Administrador de Sistemas debe revocar rápidamente la cuenta o los privilegios de un usuario cuando reciba una orden de un superior.

Cuando un empleado es despedido o renuncia a la empresa, debe desactivarse su cuenta antes de que deje el cargo.

El sistema deberá finalizar toda sesión interactiva cuando la terminal desde donde se esté ejecutando no verifique uso durante un período de cinco minutos, deberá deslogear al usuario y limpiar la pantalla.

Las PC´s deben tener instalado un protector de pantalla con contraseña.

Se debe bloquear el perfil de todo usuario que no haya accedido al sistema durante un período razonable de tiempo.

Se deberá impedir la existencia de perfiles de usuarios genéricos, en todos los sistemas operativos y en el sistema informático de la Empresa. Es decir se prohíbe el uso de cuentas anónimas o de invitado (guest) y los usuarios deben entrar al sistema mediante cuentas que indiquen claramente su identidad. Esto también implica que los administradores de sistemas no deben entrar inicialmente como root o administrador, sino primero empleando su propio ID y luego mediante set user id para obtener el acceso como root o administrador.

Se deberá minimizar la generación y el uso de perfiles de usuario con máximos privilegios. Estos privilegios, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsable de la administración o de la seguridad de los sistemas.

Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

La solicitud de una nueva cuenta o el cambio de privilegios debe ser hecha por escrito y debe ser debidamente aprobada.

No debe concederse una cuenta a personas que no sean empleados de la empresa a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

Contraseñas

Las reglas de contraseña listadas a continuación están de acuerdo a los requerimientos y estándares internacionales.
La contraseña de verificación de identidad no debe ser trivial o predecible, y debe:

• Ser de al menos 8 caracteres de longitud
• Contener una combinación de caracteres alfabéticos y no alfabéticos (números, signos de puntuación o caracteres especiales) o una combinación de al menos dos tipos de caracteres no alfabéticos.
• No contener su user ID como parte la contraseña.

Sistemas y aplicaciones de la empresa que contengan información clasificada UNIPLEX Confidencial requieren que Ud. cambie la contraseña al menos cada tres meses (90 días). Para los casos en los cuales los sistemas o aplicaciones no cuenten con controles técnicos que obliguen al cambio de contraseña, es su responsabilidad cumplir con este requerimiento. Cuando cambie la contraseña debe seleccionar uno(a) nuevo(a). El password ingresado sea diferente a los últimas cinco utilizados.

Bloquear el perfil de todo usuario que haya intentado acceder al sistema en forma fallida por más de cinco veces consecutivas.

El usuario debe poder modificar su password cuantas veces considere necesario, sin seguir ningún procedimiento formal de aviso.

La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.

Las contraseñas predefinidas que traen los equipos nuevos tales como routers, switchs, etc., deben cambiarse inmediatamente al ponerse en servicio el equipo.

El usuario no debe guardar su contraseña en una forma legible en archivos en disco, y tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.

2 - Seguridad de comunicaciones

Topología de red

Deberá existir documentación detallada sobre los diagramas topológicos de la red.

Deberán existir medios alternativos de transmisión en caso de que alguna contingencia afecte al medio primario de comunicación.

Con respecto a la utilización del correo electrónico deben almacenarse datos sobre:

- Correo entrante y saliente,

- Hora de envío,
- Contenido del mail,
- Asunto del mail,
- Archivos adjuntos,
- Reporte de virus de cada parte del mail,
- Direcciones de máquina destino y fuente,
- Tamaño del mensaje.

Con respecto a la utilización de la red informática deben almacenarse datos sobre:

- Ancho de banda utilizado y cuellos de botella en el tráfico de red.
- Tráfico generado por las aplicaciones,
- Recursos de los servidores que utilizan las aplicaciones,
- El estado de cada aplicación, (en cola, ejecutándose, esperando una respuesta),
- Intentos de intrusión,
- Uso de los protocolos,
- Solicitudes de impresión de datos de la empresa.

Todos los cambios en la central telefónica (NBX) y en los servidores y equipos de red de la empresa, incluyendo la instalación de el nuevo software, el cambio de direcciones IP, la reconfiguración de switchs, deben ser documentados y debidamente aprobados, excepto si se trata de una situación de emergencia.

Todo esto es para evitar problemas por cambios apresurados y que puedan causar interrupción de las comunicaciones, caída de la red, denegación de servicio o acceso inadvertido a información confidencial.

Propiedad de la información

Con el fin de mejorar la productividad, Uniplex promueve el uso responsable de las comunicaciones en forma electrónica, en particular el teléfono, el correo de voz, el correo electrónico, y el fax. Los sistemas de comunicación y los mensajes generados y procesados por tales sistemas, incluyendo las copias de respaldo, se deben considerar como propiedad de la empresa y no propiedad de los usuarios de los servicios de comunicación.

Uso de los sistemas de comunicación

Los sistemas de comunicación de la empresa generalmente sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional es permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y además no interfiera con la productividad del empleado ni con las actividades de la empresa.

Conexiones externas

La conectividad a Internet será otorgada para propósitos relacionados con el negocio y mediante una autorización de la Gerencia.

Debe asegurarse que la totalidad del tráfico entrante y saliente de la red interna, sea filtrado y controlado por un firewall prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.

Todas las conexiones a Internet de la empresa deben traspasar un servidor Proxy una vez que han traspasado el firewall.

Deben documentarse los servicios provistos a través de Internet y definirse las responsabilidades en cuanto a su administración. No se publicarán en Internet datos referidos a las cuentas de correo de los empleados, deberán exhibir cuentas especiales asignadas a cada área de la empresa.

Cada vez que se establezca una vía de comunicación con terceros (personal de mantenimiento externo, fábricas, proveedor de servicios de Internet, etc.), los mecanismos de transmisión y las responsabilidades de las partes deberán fijarse por escrito.

El uso de Internet debe ser monitoreado periódicamente. Si existe alguna razón para creer que la seguridad está siendo violada, Uniplex puede revisar el contenido de las comunicaciones de Internet.

El acceso casual a los mensajes de correo electrónico por los administradores y similares, se considera una violación a la política de seguridad de la información.

Sin embargo, la Gerencia tiene el derecho de examinar cualquier información, sin previo consentimiento o notificación del empleado, en caso que se considere que se está utilizando inadecuadamente el equipamiento de la compañía.

Información personal sensitiva

Es importante señalar que hay una categoría de Información Personal (PI) / Datos personales (PD) llamada Información Personal Sensitiva (SPI) que puede requerir cuidados adicionales atendiendo a las leyes propias de los países. SPI es un elemento de información que podría ser usada indebidamente perjudicando a la persona financiera, laboral o socialmente.

Información Personal Sensitiva incluye:

- número de identificación personal (ej. Numero del Seguro Social)
- número de licencia de conducir
- número de cuenta bancaria
- número de tarjeta de crédito o débito en combinación con cualquier código de seguridad
- password o código de acceso que podría permitir acceso a cuentas financieras personales
- Información relacionada a la condición natural de la persona tal como su raza u origen étnico, opinión política, membrecía de organizaciones mundiales, creencias filosóficas o religiosas, información relativa al estado de salud física o mental, enfermedad, minusvalía, defectos patológicos o tratamientos médicos, actividad u orientación sexual, records criminalísticas, incluyendo convicciones, decisiones penales y alguna otra información colectada en procesos de administración de justicia relacionada con ofensas o relacionado con comisiones debido a supuestas ofensas, información biométrica o genética, necesidades de bienestar social o beneficios o asistencia recibidos por

bienestar social, ya sea que toda o parte de la información descrita arriba directa o indirectamente.

Para toda Información Personal Sensitiva de los empleados de la empresa, de nuestros clientes y otra de carácter individual clasificada Confidencial se debería cumplir mínimo con lo siguiente:

- No almacene Información Personal Sensitiva sin una razón válida de negocio para hacerlo.
- Si tiene una necesidad válida de negocio para almacenar Información Personal Sensitiva en su estación de trabajo u otro medio magnético, esta información debe estar criptografiada.

Si su estación de trabajo o medio magnético conteniendo Información Personal Sensitiva es perdido, robado o se sospecha ha comprometido su seguridad, Ud. debe inmediatamente reportar el incidente y especificar que tipo de Información Personal Sensitiva ha sido expuesta.

No envíe información Confidencial Uniplex a sitios Internet que ofrecen servicios de traducción.

Cuando imprima información Confidencial Uniplex, Ud. debe protegerla contra robo o acceso no autorizado. (El termino printers incluye: impresoras, ploters y otros dispositivos usados para crear impresiones de salida). La información Confidencial de la empresa sólo puede ser impresa en un área controlada con acceso permitido sólo a personal con razón de negocio válido, o una instalación atendida donde la información impresa sea entregada sólo a su

propietario o también en una impresora con la facilidad de captura que Ud. controle o atienda personalmente.

Ud. puede usar una impresora ubicada en un espacio interno de la empresa, pero debe recoger su información Confidencial Uniplex dentro de los 30 minutos siguientes.

Configuración lógica de red

Cuando conecte su equipo a una red interna de la empresa, se debe considerar varios puntos:

1. No se presente (ej. Enmascarado) o identifique como si Ud. fuera otro usuario en la red. No ejecute programas de monitoreo de tráfico (Ej. "sniffer" o similares) sin la debida autorización explícita de la gerencia y la aprobación del administrador de la red.

2. No ejecute pruebas de seguridad o programas contra cualquier sistema o servidor Intranet u otros que Ud. controle directamente sin la debida y explicita autorización gerencial. No agregue cualquier dispositivo que amplíe la infraestructura de la red Uniplex (ej. dispositivos tales como Switches, Bridges, Routers, Hubs, modems, wireless access points, etc.) por cualquier motivo sin la debida autorización del administrador de la red.

3. Deberá asegurarse que la dirección IP de la empresa sea un número variable y confidencial.

Correo

Deberá existir un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.
Todas las cuentas de correo que pertenezcan a la empresa deben estar gestionadas por una misma aplicación. Esta debe asociar una cuenta de correo a una PC en particular de la red interna.

El correo electrónico no debe ser utilizado para enviar cadenas de mensajes, no debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la empresa.

Los datos que se consideraron “confidenciales” o “críticos” deben encriptarse. Debe existir un procedimiento de priorización de mensajes, de manera que los correos electrónicos de prioridad alta sean resguardados.

Deberá asignarse una capacidad de almacenamiento fija par cada una de las cuentas de correo electrónico de los empleados.

Antivirus

En todos los equipos de la empresa se debe instalar y correr el antivirus actualizado, el mismo que debería cumplir con lo siguiente:

- Detectar y controlar cualquier acción intentada por un software viral en tiempo real.

- Periódicamente ejecutar el "scanning" para revisar y detectar software viral almacenado en la estación de trabajo.
- Hacer una revisión al menos diaria para actualizar la definición del software antivirus.
- Debe ser un producto totalmente legal (con licencia o Software libre).

No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora de Uniplex a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

Deberá existir un procedimiento formal a seguir en caso que se detecte un virus en algún equipo del sistema.

Firewall

Deberá instalarse y correr un firewall personal en su estación de trabajo, El firewall debe cumplir con los siguientes criterios básicos:

- Las redes detectadas deben ser tratadas como desconocidas y no confiables.
- Alertar a los usuarios ante nuevos programas solicitando acceso a la red
- Impedir el acceso a sistemas no autorizados.
- Que el firewall del cliente tenga la versión mas reciente disponible.
- Debe ser un producto totalmente legal (con licencia)

El firewall de la empresa debe presentar una postura de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, habilitando los necesarios.

El encargado de mantenimiento debe controlar periódicamente la configuración del firewall y los servicios de red, documentando los resultados de dichas pruebas.

Ataques de red

Toda la información que se considere confidencial deberá encriptarse durante la transmisión, o viajar en formato no legible.

Deberá utilizarse una herramienta que monitoree la red, con el fin de evitar el ataque de denegación de servicio (DoS).

Para disminuir el riesgo de sniffing, la red de la empresa deberá segmentarse física y/o lógicamente.

Con el fin de disminuir la posibilidad de spoofing el firewall deberá denegar el acceso a cualquier tráfico de red externo que posea una dirección fuente que debería estar en el interior de la red interna.

Los archivos de passwords y datos de usuarios no deberán almacenarse en el directorio por default destinado a tal fin. Además deberán estar encriptadas utilizando encriptación en un solo sentido (“one way”), con

estrictos controles de acceso lógico, de manera de disminuir la posibilidad de ataques.

3 - Seguridad de las aplicaciones

Software

No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que se haya sido comprobado en forma rigurosa y que esté aprobado su uso por el Departamento de Informática.

Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita, a menos que haya sido previamente aprobado por el Departamento de Informática.

Deben mantenerse registros de todas las transacciones realizadas en la base de datos, de manera que éstas puedan revertirse en caso de surgir un problema. Los registros de la base de datos no se borrarán físicamente, sino que deberán marcarse como eliminados.

Deberá existir un responsable en cada área de la empresa, que responda por la información que se maneja en dicho sector. Deberá definir la

clasificación de los datos y los controles de acceso que son necesarios, junto con el administrador del sistema.

Control de aplicaciones en PC’s

Se deberá generar un procedimiento donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.

Antes de hacer un cambio en la configuración de los servidores se deberá hacer un backup de la configuración existente. Una vez que el cambio ha resultado satisfactorio deberá almacenarse la configuración modificada.

Se deberán documentar no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se les realicen.

Deberán generarse historiales y así calcular datos estadísticos de los cambios realizados y los errores reportados.

En el momento en que un nuevo usuario ingrese a la empresa, se lo deberá notificar y deberá aceptar que tiene prohibida la instalación de cualquier producto de software en los equipos.

Control de datos en las aplicaciones

Deberán protegerse con controles de acceso las carpetas que almacenen los archivos de las aplicaciones, y solo el administrador de sistemas tendrá acceso a ellas.

Ciclo de vida

Antes de realizar alguna modificación en el sistema, deberá realizarse un análisis del impacto de este cambio.
Se deberá implementar una gestión de configuración, y deberán documentarse los cambios desarrollados en las aplicaciones.

Deberá existir un documento formal de solicitud de cambios, donde quede reflejado el motivo y la solicitud del cambio, allí se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el administrador de sistemas. La documentación de los cambios debe incluir:

- Sistema que afecta,
- Fecha de la modificación,
- Desarrollador que realizó el cambio,
- Empleado que solicitó el cambio,
- Descripción global de la modificación.

Los contratos con terceros deberán contener una cláusula que indique “Derecho de auditar el desempeño del contratado”.

Se deberá informar por escrito la importancia de la seguridad de la información a todo el personal contratado, terceros y consultores. El administrador del centro de cómputos, junto con los directivos, serán quienes:

Especifiquen los requerimientos de seguridad,

Determinen los pasos a seguir en caso que no se respete lo establecido en el contrato,

Establezcan cláusulas sobre confidencialidad de la información,

Exijan al tercero en cuestión que informe posibles brechas de seguridad existentes.

Con respecto a la contratación de terceros para el desarrollo de aplicaciones, éste deberá entregar a la empresa:

Aplicación ejecutable,

Código fuente de la aplicación,

Documentación del desarrollo,

Manuales de uso.

4 - Seguridad física

Los computadores de la empresa sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las

medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática
No se permite fumar, comer o beber mientras se está usando un PC.

Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la Compañía se requiere una autorización escrita.
La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

Control de acceso físico al centro de cómputos

Se deberá asegurar que todos los individuos que entren a áreas restringidas se identifiquen y sean autenticados y autorizados para entrar.

Cualquier persona ajena a la empresa que necesite ingresar al centro de cómputos deberá anunciarse en la puerta de entrada, personal de sistemas

designado deberá escoltarlo desde la puerta hacia el interior del edificio, acompañándolo durante el transcurso de su tarea, hasta que éste concluya.

El área del centro de cómputos donde se encuentran los servidores, el switch central y demás equipamiento crítico solo debe tener permitido el acceso a los administradores.

Deberán existir guardias de seguridad en permanente monitorización, durante el horario laboral. Se deberán ubicar en el exterior y el interior de la empresa.
Los servidores de red y los equipos de comunicación (NBX, routers, etc.) deben estar ubicados en locales apropiados, protegidos contra daños y robo. Debe restringirse severamente el acceso a estos locales y a los cuartos de cableado a personas no autorizadas mediante el uso de cerraduras y otros sistemas de acceso.

Control de acceso a equipos

Los siguientes controles de seguridad deben ser activados en todas las estaciones de trabajo (workstation) personales con el fin de ayudar a protegerlas contra el robo de la información sensible que dicho equipo pueda contener:

1. Activar la contraseña de disco duro (hard disk password) en los parámetros del BIOS.

2. Configurar la contraseña para proteger el teclado y la pantalla (keyboard/screen lock) que se active automáticamente luego de un período de inactividad. El intervalo de inactividad no debe ser mayor a 15 minutos.
3. Si Ud. conecta su estación de trabajo a una red fuera de la CMS, en la que la administración de niveles de acceso no es controlada (ej. Ud. esta en un cliente y requiere hacer logon a un dominio de Windows administrado por el cliente), entonces toda la información clasificada Confidencial debe ser criptografiada.

Cualquier dispositivo externo que no se encuentre en uso, deberá permanecer guardado bajo llave dentro del centro de cómputos.

El administrador deberá realizar chequeos periódicos para comprobar:

La correcta instalación de los dispositivos de los equipos,
Su buen funcionamiento,
Sus números de series corresponden con los datos registrados por el administrador al momento de la instalación

Si su portátil no puede ser asegurada físicamente de otra forma (ej: guardarla en un cajón o gaveta del escritorio bajo llave, dentro de una oficina, o llevarla consigo), entonces debe asegurarla con un cable de seguridad o anclaje físico.

Mantenga el equipo en su poder todo el tiempo que sea posible, cuando esté fuera de las premisas de la empresa.

En los viajes aéreos, no despache su portátil con el equipaje, y esté alerta de la posibilidad de robo cuando vaya a través de los puntos de control de los aeropuertos.

No debe dejar su portátil dentro de un vehículo desatendido por un período largo de tiempo.

Si debe dejar su portátil en un vehículo desocupado, asegúrela al cuerpo del vehículo dentro del baúl.

Si debe dejar su portátil en un hotel, guárdela en una caja fuerte de haber una disponible.

Si no hay caja fuerte y posee el cable de seguridad, utilice ese mecanismo.

Dispositivos de soporte

Deberán existir los siguientes dispositivos de soporte en la empresa:

Aire acondicionado y Calefacción: en el centro de cómputos la temperatura debe mantenerse entre 19º C y 20º C.

Matafuegos: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para extinguir incendios en equipos eléctricos de computación, deberán estar instalados en lugares estratégicos de la

empresa, el centro de cómputos deberá contar con uno propio ubicado en la habitación de los servidores.

Alarmas contra intrusos: deberán contar con una alarma que se active en horarios no comerciales. Ésta deberá poder activarse manualmente en horarios laborales ante una emergencia.

UPS: (Uninterruptible power supply) deberá existir al menos un UPS en el centro de cómputos que atienda a los servidores, con tiempo suficiente para que se apaguen de forma segura.

Luz de emergencia: deberá existir una luz de emergencia que se active automáticamente ante una contingencia.

Todos estos dispositivos deberán ser evaluados periódicamente por personal de mantenimiento.

Deberán existir procedimientos detallados a seguir por el personal en caso de emergencias, indicando responsables, quiénes deben estar adecuadamente capacitados.

Cableado estructurado

Se deberá documentar en planos los canales de tendidos de cables y las bocas de red existentes.

Deberá medirse periódicamente nivel de ancho de banda de red ocupado. Si este nivel excede un mínimo permitido, deberán tomarse las acciones correctivas necesarias.

Ante un corte del suministro de energía eléctrica deberán apagarse los equipos del centro de cómputos de forma segura, como medida de prevención.

5.- Administración del centro de cómputo

El equipo de sistemas debe hacer hincapié en la concienciación de todos los usuarios, generando una cultura de la seguridad, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concienciación debe ser renovado y transmitido a los usuarios en forma anual.

Los usuarios solicitarán asesoramiento o servicios al centro de cómputos a través de mails, de manera que se genere un registro de los trabajos efectuados por los empleados del centro de cómputos y de las solicitudes de los empleados.

Deberá existir un procedimiento para realizar la publicidad de políticas, planes o normas de la empresa y sus modificaciones.

Los administradores deberán informar en tiempo de suspensiones en el servicio necesarias por mantenimiento, especificando fecha, hora y duración de la suspensión.

Deberá generarse un inventario detallado donde se describan los sistemas de información y de los equipos de cómputos utilizados en la organización. Deberá asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.

Capacitación

Se debe obtener un compromiso firmado por parte del personal respecto al cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no-divulgación de información de la organización, el cuidado de los recursos, la utilización de software sin licencia y el reporte de situaciones anormales. Debe confirmarse este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.

Asegurar que los empleados reciban capacitación continua para desarrollar y mantener sus conocimientos competencia, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido a fin de lograr un desempeño eficaz.

Respaldos

Se deberá asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.

Los archivos de backup deben tener un control de acceso lógico de acuerdo a la sensibilidad de sus datos, además de contar con protección física.

Deben generarse copias de respaldo de las configuraciones de los servidores, documentando las modificaciones realizadas para identificar las distintas versiones. Se deberá establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores.

Se deberá generar una copia de respaldo de toda la documentación del centro de cómputos, incluyendo el hardware, el software, la cual deberá ser de acceso restringido y estar físicamente en un lugar distinto a los centros de procesamiento.

Documentación

Deberá generarse un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, normas, estándares,

procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el centro de cómputos.

Deberá existir un registro de los eventos, errores y problemas del hardware y el software utilizados en las operaciones de procesamiento de datos.

Deberán existir una documentación y un registro de las actividades del centro de cómputos (procesos normales, eventuales y excepcionales) que se desarrollan diariamente, que incluya como mínimo el detalle de los procesos realizados.

Revisión del sistema

La empresa debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad de forma de asegurar la integridad, exactitud y disponibilidad de la información. Para ello deben existir:

Herramientas que registren todos los eventos relacionados con la seguridad de la información procesada por los centros de cómputos de la empresa.

Herramientas que analiza los registros generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.

Procedimientos de revisión de los eventos registrados, a cargo de un empleado designado por el administrador, de forma de detectar anomalías y tomar las acciones correctivas necesarias.

Se deberán registrar, mediante logs de auditoria, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo:

Fecha y hora del evento,
Fuente (el componente que disparó el evento),
ID del evento (número único que identifica el evento),
Equipo (máquina donde se generó el evento),
Usuario involucrado,
Descripción (acción efectuada y datos asociados con el evento).

Se deberán analizar periódicamente los siguientes eventos específicos como mínimo:

Controles de acceso y permisos de los usuarios,
Uso de recursos informáticos,
Intentos de ingreso al sistema fallidos.

Aspectos Organizativos para la Seguridad

Organización Interna

Para administrar la seguridad de información se crea el Comité de Seguridad de la Información, integrado por el representante de cada área. A continuación se indica la conformación del mismo:

Área/Dirección	Representante
Área de sistemas	Administrador de la red (Networking–Software)
Área de ventas	Gerente de cuenta
Dirección administrativa	Jefe Administrativo Financiero
Auditoría interna	Auditor interno
Legal	Asesor jurídico

Tabla 4.2 Conformación del Comité de Seguridad de la Información

- **ASIGNACIÓN DE RESPONSABILIDADES SOBRE SEGURIDAD DE LA INFORMACIÓN**

El Director Ejecutivo es el encargado de asignar las funciones relativas a la Seguridad Informática del Organismo al Administrador de la red, en adelante el “Responsable de Seguridad Informática”, quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Organismo, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la Política.

A continuación se detallan los procesos de seguridad, indicándose en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

Proceso	**Responsable**
Seguridad del Personal	Coordinador de sucursal
Seguridad en las comunicaciones y operaciones	Administrador de la red
Control de acceso	Administrador de la red

Tabla 4.3 Procesos de Seguridad

Proceso de autorización de recursos para el tratamiento de la información

Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas del Organismo.

El uso de recursos personales de procesamiento de información en el lugar de trabajo puede ocasionar nuevas vulnerabilidades. En consecuencia, su uso será evaluado en cada caso por el Responsable de Seguridad Informática y deberá ser autorizado por el Responsable del Área Informática y por el responsable del área al que se destinen los recursos.

- **Gestión de los Activos de Red**

Inventario de Activos

A continuación se hace un inventario de los recursos informáticos dentro de Uniplex:

DEPARTAMENTO RESPONSABLE	ACTIVO	DESCRIPCIÓN	DETALLES DE LA RESPONSABILIDAD
Administrador de la red (Networking)	6 Equipos de cómputo	Laptop, CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	El administrador es responsable del mantenimiento y actualización de los servidores a excepción del de Lotus y el de Desarrollo.
Administrador de la red (Networking)	Software	Sistemas Operativos (Windows 2003, XP)	
Administrador de la red (Networking)	Software	Antivirus, Camara IP, Lotus	
Administrador de la red (Networking)	Software	Ios e imágenes de equipos de red	
Administrador de la red (Networking)	Software	Monitoreo de red, Administración de NBX	
Ventas	2 Equipos de cómputo	Laptop, Impresora, mouse, parlantes, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Ventas	Software	Sistemas Operativos (Windows 2003, XP)	
Ventas	Software	Antivirus, Lotus	
Recepción / Cobranzas	4 Equipos de cómputo	Laptop, CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD, Impresora, Scanner, Fax, Base Celular	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware.
Recepción/ Cobranzas	Software	Sistemas Operativos (Windows 2003, XP)	
Recepción / Cobranzas	Software	Antivirus, Lotus	
SP Software	6 Equipos de cómputo	Laptop, CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware, actualización y mantenimiento de los servidores Lotus y Desarrollo
SP Software	Software	Antivirus, Lotus, Lotus Admin, Lotus Designer	
SP Software	Software	Sistemas Operativos (Windows 2003, XP)	
NCR	5 Equipos de cómputo	Laptop, CPU, monitor, teclado, mouse, parlantes, UPS, unidad de CD, ATM	Son responsables de la protección física de los equipos, reportar fallas en el Software o Hardware
NCR	Software	Sistemas Operativos (Windows 2003, XP)	

NCR	Software	Antivirus, Lotus, Aptra	

Tabla 4.4 Inventario de Activos

- **SEGURIDAD DE LOS RECURSOS HUMANOS**

Las responsabilidades de cada empleado se definen en el momento de su contratación, a continuación se especifica la selección de personal propuesta para la empresa. La implementación de este método está en consideración del departamento de Recursos Humanos de Uniplex, para que el departamento en conjunto con la directiva de la Organización apruebe el mismo.

Capacitación del Usuario

En cuanto a la capacitación para el usuario, en el ANEXO A se establece una guía para el usuario que los empleados deben tener presente para no incurrir en fallas de seguridad.

Mecanismos para promover la comunicación

En el caso que se necesite informar a todo el personal de alguna debilidad con respecto a la seguridad dependiendo de la complejidad de la situación se optará como primera instancia el correo electrónico interno y si el caso lo amerita se convocará a una reunión en la cual intervendrá el Comité de Seguridad junto con el personal de la Corporación necesario.

Seguridad Física y del Entorno

La seguridad física actualmente está implementada en un modelo de defensa por capas, los controles físicos deben trabajar juntos en la arquitectura, es decir, si una capa falla, otras capas protegerá el recursos físico. Las capas están implementadas dentro del perímetro. Por ejemplo: se tendrá una valla, luego las paredes, luego el guardia, luego la tarjeta de acceso, luego el candado en el caso de una laptop. Esta serie de capas protegerán los recursos más sensibles.

La seguridad necesita proteger todos los recursos de la organización, incluyendo personas y hardware. La seguridad debe fortalecer la productividad ya que provee un ambiente seguro. Esto permite a los empleados enfocarse en sus tareas, en lo posible no permitir que la seguridad física se transforme en un hueco de seguridad.

Las vulnerabilidades con respecto a la seguridad física tienen relación con destrucción física, intrusos, problemas del ambiente y los empleados que han perdido sus privilegios causen daños inesperados de datos o sistemas.

Instalaciones

Los materiales de construcción y la composición de la estructura han sido evaluados por las características de protección. La construcción de la infraestructura asegura que el edificio no colapse.

Como se indico anteriormente la puerta del cuarto de servidores se puede abrir fácilmente con cualquier tarjeta, razón por la cual se cambiará la puerta, para que cumpla con las siguientes características de seguridad:

- Material resistente, como: madera, aluminio
- Resistente a ingreso forzado
- Cerradura resistente

Además en la puerta del cuarto de servidores se colocará un rótulo de zona de acceso restringido para evitar acceso no autorizado.

Es necesario procedimientos de seguridad para ayudar a proteger la Empresa de actividades devastadoras. Muchas veces estos procedimientos de protección usan componentes de seguridad que son parte del ambiente y por consiguiente no necesitan gastos extras. Los procedimientos que se han considera incluyen copias de respaldo de los datos críticos (**ANEXO B**), componentes de seguridad que ya son parte de los sistemas operativos, y la solicitud de mayor colaboración por parte del guardia actual de Uniplex para que permanezca en una sola área atento a cualquier fallo de seguridad.

La seguridad física debería ser complementada con la seguridad contra fuego.

Hay estándares nacionales y locales para prevenir, detectar y suprimir el fuego.

En la Corporación se utilizará detectores de fuego activados por el humo, ya que son dispositivos que dan señales de alerta tempranamente. Este

detector produce un rayo de luz a través de un área protegida y si el rayo es obstruido, la alarma asume que es humo y sueña. En la figura 1 se ilustra como el dispositivo trabaja.

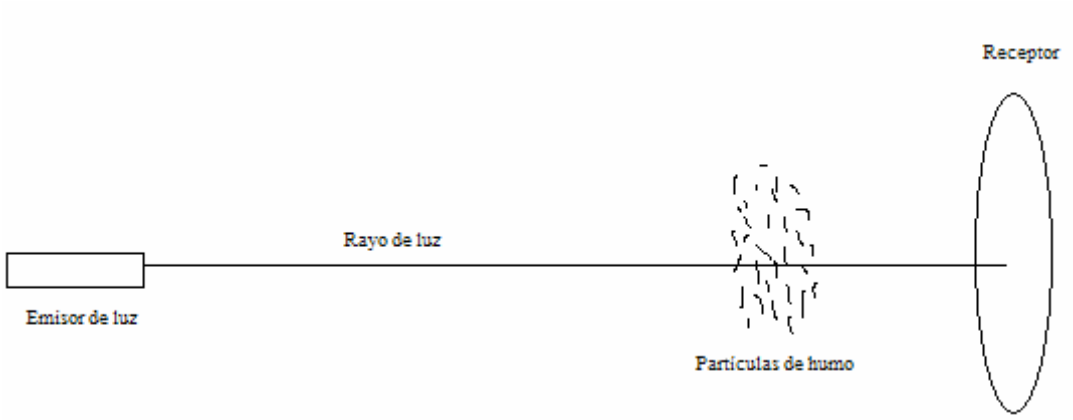


Figura 4.2 Funcionamiento de detector de humo

Se colocarán detectores de fuego en el cuarto de servidores, otra cerca al área de la Asistente ejecutiva y otros censores cerca de la Recepción, de tal manera que se trate de cubrir todas las instalaciones de Uniplex.

Es importante conocer qué tipo de fuego y que se debería hacer apara suprimir el fuego. En la tabla siguiente se indica los tipos de fuego.

Clase	Tipos de fuego	Elementos del fuego	Métodos de supresión
A	Combustible común	Productos de madera, papel	Agua
B	Líquido	Petróleo y productos derivados	Gas (Halon) o CO2
C	Eléctrico	Equipos eléctricos	Gas (Halon) o CO2
D	Metales combustibles	Magnesio, sodio, potasio	Polvo seco

Tabla 4.5 Tipos de Fuego

En la empresa se utilizará extintores portátiles para suprimir el fuego clase C, y dependiendo de la gravedad de la situación se procederá a llamar a la estación de bomberos más cerca para eliminar el fuego con el agua.

PERÍMETRO DE SEGURIDAD

La primera línea de defensa trata el control del perímetro para prevenir acceso no autorizado a Uniplex. Actualmente en la empresa esta defensa trabaja de la siguiente manera: Cuando la empresa es cerrada todas las puertas son aseguradas con un mecanismo de monitoreo en posiciones estratégicas para alertar de actividades sospechosas. Cuando la empresa está en operación, la seguridad es más complicada porque se debe distinguir el acceso de personas autorizadas de las personas no autorizadas. En la figura se ha identificado el único acceso, esta debe ser apropiadamente protegida, actualmente esta puerta esta asegurada en horas laborables, mediante un mecanismo eléctrico que solo permite el acceso desde adentro, debido a que la empresa esta aislada del resto del conglomerado el acceso es exclusivamente para clientes o empleados de la misma, no pudimos realizar el cambio de la puerta por otra de mayor seguridad, el costo de nuestra propuesta se adjunta en el análisis económico, la misma que consideraba cambiar la actual puerta por una puerta con cerradura electrónica la cual se podrá abrir con tarjetas electrónicas que serán otorgadas a miembros de la empresa y para visitantes existirá un timbre y la recepcionista procederá a abrirla desde su lugar de trabajo.

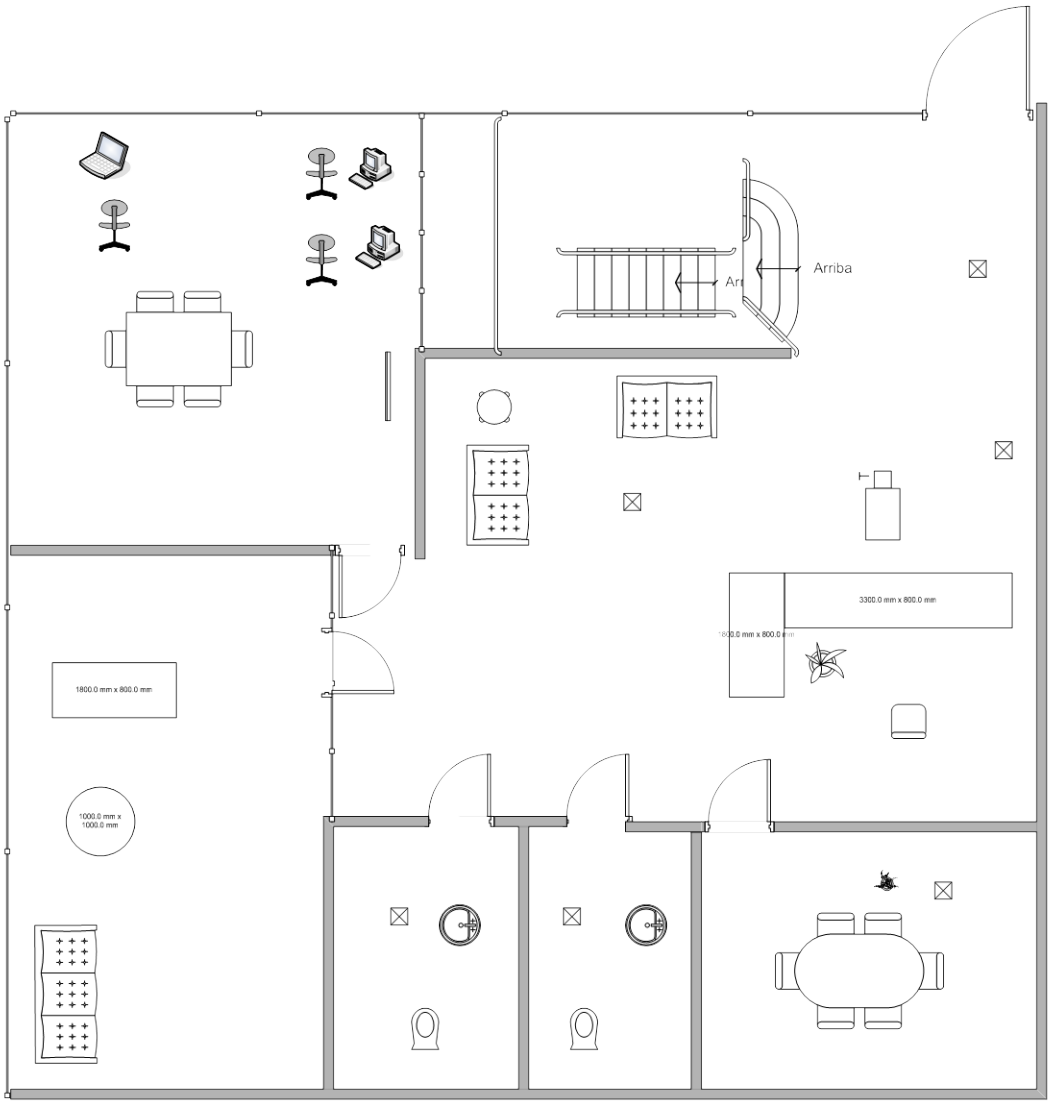


Figura 4.3 Esquema físico de las instalaciones de Uniplex

Las cerraduras y llaves son los mecanismos de control de acceso más barato pero de gran importancia para prevenir cualquier acceso no autorizado.

- **CONTROLES FÍSICOS DE ENTRADAS**

Los controles de acceso físico tendrán las siguientes características:

a) Supervisar a los visitantes de la Corporación y registrar la fecha y horario de su ingreso y egreso, esta tarea será realizada por el guardia de seguridad. Sólo se permitirá el acceso mediando propósitos específicos y autorizados.

b) Implementar el uso de una identificación unívoca visible para todo el personal del área protegida e instruirlo acerca de cuestionar la presencia de desconocidos no escoltados por personal autorizado y a cualquier persona que no exhiba una identificación visible.

SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS

Se definen los siguientes sitios como áreas protegidas de la Corporación, para lo cual se consideró el tipo de información manejada por cada área.

ÁREAS PROTEGIDAS
Cuarto de servidores
Recepción
Coordinación de sucursal / Ventas
NCR / Netwroking
SP Software

Tabla 4.6 Áreas Protegidas

Se establecen las siguientes medidas de protección para áreas protegidas:

a. Ubicar las instalaciones críticas en lugares a los cuales no pueda acceder personal no autorizado.

b. Ubicar las funciones y el equipamiento de soporte, por ejemplo: impresoras, fotocopiadoras, máquinas de fax, adecuadamente dentro del área no protegida para evitar solicitudes de acceso, el cual podría comprometer la información.

c. Establecer que las puertas y ventanas permanecerán cerradas cuando no haya vigilancia.

d. Restringir el acceso público a las guías telefónicas y listados de teléfonos internos que identifican las ubicaciones de las instalaciones de procesamiento de información sensible.

e. Almacenar la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, para evitar daños ocasionados ante eventuales contingencias en el sitio principal: en la caja de seguridad que tiene la Corporación con el Banco.

Desarrollo de Tareas en Áreas Protegidas

Para complementar la seguridad en la las áreas protegidas, se establecen los siguientes controles:

a) Dar a conocer al personal la existencia del área protegida, o de las actividades que allí se llevan a cabo, sólo si es necesario para el desarrollo de sus funciones.

b) Evitar la ejecución de trabajos por parte de terceros sin supervisión, como por ejemplo: trabajos de limpieza.

c) Bloquear físicamente las áreas protegidas desocupadas.

d) Prohibir comer, beber y fumar dentro de las instalaciones de procesamiento de la información.

Suministros de Energía

El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a) Actualmente se cuenta con un suministro de energía ininterrumpible (APS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la empresa.

b) Una vez que esté el APS activo, la central eléctrica con la que cuenta el edificio debe ingresar a funcionar hasta que se haya solucionado el problema, es necesario mantener un contacto de forma inmediata con la empresa eléctrica para que se solucione el problema lo más pronto posible.

Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a) Someter el equipamiento a tareas de mantenimiento preventivo, el responsable del área informática mantendrá listado actualizado del

equipamiento con el detalle de la frecuencia en que se realizará el mantenimiento preventivo.

b) Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

c) Registrar todas las fallas supuestas o reales y todo el mantenimiento preventivo y correctivo realizado.

A continuación se indica el período aconsejable para realizar los mantenimientos en los equipos de la red.

Equipo	Frecuencia de mantenimiento	Personal autorizado
Servidores	4 meses	Administrador de la red (Networking)
Estaciones de trabajo	6 meses	Administrador de la red (Networking)
Impresoras	6 meses	Administrador de la red (Networking)
Central telefónica	12 meses	Administrador de la red (Networking)

Tabla 4.7 Períodos de Mantenimiento Preventivos

Seguridad de los equipos fuera de los locales de la Organización

La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Corporación para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

Se respetarán permanentemente las instrucciones del fabricante respecto del cuidado del equipamiento. En Uniplex se protegerá con candados a las computadoras portátiles para evitar que sean robadas cuando se movilicen fuera de las premisas de la empresa.

GESTIÓN DE COMUNICACIONES Y OPERACIONES

DOCUMENTACIÓN DE PROCEDIMIENTOS OPERATIVOS

Se documentarán y mantendrán actualizados los procedimientos operativos y sus cambios serán autorizados por el administrador de la red.

En los anexos se encuentran detallados los procedimientos operativos para la implementación de los controles propuestos como son los necesarios para la administración de la red, controles criptográficos, seguridad en los servidores, respaldos, etc. En los cuales se detallan: instrucciones para la ejecución de cada tarea, procesamiento y manejo de información, requerimientos del sistema.

Control de Cambios Operacionales

El responsable del área informática será el encargado de implementar los cambios operacionales y de comunicaciones; previo a una justificación que explique las razones y cómo mejorará en la productividad de la empresa.

Este procedimiento de control de cambios contemplarán los siguientes puntos:

a) Identificación y registro de cambios significativos.
b) Evaluación del posible impacto de dichos cambios.
c) Aprobación formal de los cambios propuestos.
d) Planificación del proceso de cambio.

e) Prueba del nuevo escenario.

f) Comunicación de detalles de cambios a todas las personas pertinentes.

g) Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto de los mismos.

Planificación y Aceptación del Sistema.

Planificación de la Capacidad

El Responsable del Área Informática, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación tomando en cuenta los nuevos requerimientos de los sistemas y proyectar las futuras demandas, para garantizar un procesamiento y almacenamiento adecuados. Para lo cual, debe recopilar información previa de los requerimientos de software y hardware para la implementación del sistema o proceso que se piensa desarrollar.

Aceptación del Sistema

Para la aprobación del sistema se debe considerar los siguientes puntos:

a) Verificar si la capacidad de las computadoras están acorde con los requerimientos actuales y futuras proyecciones.

b) Garantizar la recuperación ante errores.

c) Preparar y poner a prueba los procedimientos operativos de rutina según normas definidas.

d) Garantizar la implementación de un conjunto acordado de controles de seguridad.

e) Asegurar que la instalación un nuevo sistema no afecte negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento.

Protección Contra Software Malicioso.

Controles contra Software Malicioso

Estos controles deberán considerar las siguientes acciones:

a) Prohibir el uso de software no autorizado por la Corporación.

b) Instalar y actualizar periódicamente software de detección y reparación de virus, examinado computadoras y medios informáticos, para esto se implementará el software de anti-virus Mcfee (**ANEXO C**).

c) Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles.

d) Revisar periódicamente el contenido de software y datos de los equipos de procesamiento que sustentan procesos críticos de UNIPLEX, investigando formalmente la presencia de archivos no aprobados o modificaciones no autorizadas (políticas de control de acceso).

e) Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos de origen incierto, o en archivos recibidos a través de redes no confiables.

f) Redactar procedimientos para verificar toda la información relativa a software malicioso, garantizando que los boletines de alerta sean exactos e informativos.

g) Concientizar al personal acerca del problema de los virus y sus posibles consecuencias (**ANEXO A**).

- **Gestión Interna de Respaldo**

Recuperación de la Información

El Responsable de la Seguridad de Información dispondrá y controlará la realización de dichas copias. Los sistemas de resguardo deberán probarse periódicamente, asegurándose que cumplen con los requerimientos de los planes de continuidad de las actividades de la Corporación. Para los procedimientos del resguardo de información, se considerarán los siguientes puntos:

a) Almacenar en una ubicación remota copias recientes de información de resguardo junto con registros exactos y completos de las mismas y los procedimientos documentados de restauración, a una distancia suficiente como para evitar daños provenientes de un desastre en el sitio principal.

b) Asignar a la información de resguardo un nivel de protección física y ambiental según las normas aplicadas en el sitio principal. Extender los mismos controles aplicados a los dispositivos en el sitio principal al sitio de resguardo.

c) Verificar y probar periódicamente los procedimientos de restauración garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

Para el resguardo de la información ver **ANEXO B**, donde se considera el respaldo de los servidores para el Plan de Contingencia.

- **Gestión de la Seguridad de Red.**

Controles de Red

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a) Para establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos (**ANEXO D**)
b) Implementación de controles especiales para mantener la disponibilidad de los servicios de red y computadoras conectadas (**ANEXO E**)
c) Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

- **Utilización de los Medios de Información**

Gestión de Medios Removibles

Se deberán considerar las siguientes acciones para la administración de los medios informáticos removibles:

a) Eliminar de forma segura los contenidos, si ya no son requeridos, de cualquier medio reutilizable que ha de ser retirado o reutilizado por la empresa.

b) Almacenar todos los medios en un ambiente seguro y protegido, de acuerdo con las especificaciones de los fabricantes o proveedores.

- **Intercambio de Información.**

Mensajería Electrónica

Se debe documentar normas claras con respecto al uso de correo electrónico:

- Todo empleado de la Corporación puede solicitar y disponer de una cuenta de correo electrónica activa.

- El Área de Sistemas hará la configuración de la cuenta de correo en la computadora asignada al funcionario solicitante.

- La activación de las cuentas de correo Corporativo es centralizada, encargándose de esta el responsable de Sistemas (SP Software) previa autorización del Jefe Administrativo. La activación sigue las políticas dadas por el presente documento.

- Para activar el correo electrónico, se deberá enviar dicha solicitud por escrito y debe ser debidamente aprobada.
- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- No debe concederse cuentas de correo electrónico a personas que no sean empleados de la empresa a menos que estén debidamente autorizados, en cuyo caso la activación durará el tiempo que duré la permanencia de la(s) personas en la Institución, para lo cual se requerirá la notificación respectiva del área administrativa.
- Cuando un empleado es despedido o renuncia a la Institución, debe desactivarse la cuenta de correo correspondiente, para lo cual se requerirá la notificación respectiva por parte del área administrativa.

Entender al correo electrónico como una herramienta más de trabajo provista al empleado a fin de ser utilizada conforme el uso al cual está destinada, faculta al empleador a implementar sistemas de controles destinados a velar por la protección y el buen uso de sus recursos.

Esta facultad, sin embargo, deberá ejercerse salvaguardando la dignidad del trabajador y su derecho a la intimidad. Por tal motivo, el Organismos debe informar claramente a sus empleados: a) cuál es el uso que UNIPLEX espera que los empleados hagan del correo electrónico provisto por el organismo; y b) bajo qué condiciones los mensajes pueden ser objeto de control y monitoreo.

Uso del Correo Electrónico Corporativo

- Es responsabilidad del usuario del correo electrónico hacer buen uso de su cuenta entendiéndose por buen uso:

- El uso de su cuenta para actividades institucionales administrativas de la Corporación Metropolitana de Salud.
- Leer diariamente su correo y borrar aquellos mensajes obsoletos para liberar espacio en su buzón de correo
- El uso de un lenguaje apropiado en sus comunicaciones
- No permitir que segundas personas hagan uso de su cuenta de correo
    - Cada usuario es responsable de respaldar sus correos en su equipo personal.
    - La cuenta de correo tiene un límite de 15 MB de capacidad para cada correo enviado o recibido, en caso de que por situación estrictamente laboral requiera ampliarse el limite permitido, el usuario deberá presentar la solicitud respectiva la misma que será aprobada por el Jefe del área SP Software.

Restricciones

El usuario que tenga acceso a una cuenta de correo electrónico de UNIPLEX se compromete a NO usar este servicio para:

- Fines comerciales, políticos, particulares o cualquier otro que no sea el laboral o de investigación para la Institución.

- Enviar SPAMS de información (correo basura) o enviar anexos (archivos adjuntos) que pudiera contener información nociva para otro usuario como virus o pornografía.

- Enviar o recibir contenido ilegal, peligroso, amenazador, abusivo, tortuoso, difamatorio, vulgar, obsceno, calumnioso, que atente contra el derecho a la intimidad, racial, étnico o de cualquier otra forma ofensiva.

- Enviar o recibir cualquier anuncio no solicitado o no autorizado, materiales promociónales, correo de solicitación ("junkmail", "spam"), cartas en cadena ("chain letters), esquemas de pirámides ("pyramid schemes") o cualquier otra forma de solicitud.

- Diseminar virus, caballos de troya, gusanos y otros tipos de programas dañinos para sistemas de proceso de la información de la empresa.

- Congestionar enlaces de comunicaciones o sistemas informáticos mediante la transferencia o ejecución de archivos o programas que no son de uso de la Institución.

- Falsificar encabezados o cualquier otra forma de manipulación de identificadores para desviar el origen de algún contenido transmitido por medio del Servicio.

- Enviar o recibir por correo electrónico algún contenido que no tiene derecho a transmitir por ley o por relación contractual o fiduciaria (tal como información interna, de propiedad y confidencial adquirida o entregada como parte de las relaciones de empleo o bajo Reglamentos de confidencialidad).

- Acechar o de cualquier otra forma hostigar a usuarios de correo electrónico.

La implementación de seguridad en el Servidor de Correo Electrónico se observa en el **ANEXO F**

El proceso de implementación de las políticas de acceso e implementación de seguridad mediante contraseñas se especifica se encuentran adjuntas en el **ANEXO G.**

- **Contraseñas**

Para reforzar la seguridad en las contraseñas se ha establecidos varios métodos de administración de los mismos en el servidor de dominio reforzando su seguridad y fortaleza para lo cual se ha establecido varios procesos.

En el **ANEXO F** se especifica la forma de reforzar los controles para las contraseñas.

Para la revisión de los privilegios de los usuarios se debe realizar el siguiente procedimiento:

1.- Cada trimestre del año, el administrador de la red enviará una nota por correo electrónico al encargado de cada área de los usuarios bajo su responsabilidad para que el gerente valide los permisos que tiene cada usuario para acceso a la red y al aplicativo.

2.- El gerente debe validar dicha información, y enviar la contestación de la nota al administrador de red, debe elegir entre las siguientes opciones:

- Mantener

- Eliminar
- Cambio de Jefe de Área
- Cambio de privilegios

3.- Dependiendo de las opciones, el administrador de la red debe ejecutar el procedimiento siguiente:

- En caso de mantener, no se debe realizar ningún cambio sobre el perfil del usuario
- Cuando el jefe de área seleccione la opción eliminar, el administrador de la red debe eliminar el perfil del usuario, en caso de algún reclamo el correo es el respaldo de dicha medida.
- En caso de que se solicite Cambio de Jefe de Área, el administrador debe enviar la información de dichos usuarios a los responsables correspondientes, para que validen los privilegios de los mismos.
- En caso de que se especifique cambio de privilegios, el administrador debe cambiar los privilegios de dicho perfil acorde a las especificaciones del responsable del usuario.

Es necesario que en Uniplex se adopten medidas necesarias para proteger los equipos y la información que se encuentren en ellos cuando el usuario no se encuentre en su puesto de trabajo para lo cual se requiere:

1.- El usuario debe dejar su sesión bloqueado para que no puedan acceder a su información

2.- Cuando el usuario maneje documentación confidencial, debe guardarla bajo llave en su puesto de trabajo,

3.- En caso de usuarios de equipos portátiles, se debe dejar el computador asegurado al puesto de trabajo, en todo momento.
4.- Todo tipo de contraseñas, claves de acceso deben estar debidamente protegidos. En caso de tener algún documento electrónico donde se almacene información personal de claves, contraseñas. El mismo debe tener protección adicional como es el caso de una contraseña de seguridad.

Para poder realizar un control adecuado de los puestos de trabajos de los usuarios y de la seguridad de la información que manejan, se debe realizar semestralmente el siguiente procedimiento por parte del administrador de la red:

1.- En conjunto con el responsable de cada área, realizar la inspección de los puestos de trabajo, una vez finalizada la jornada laboral.
2.- Revisar que no se encuentre documentación de información confidencial, como plan de negocio, información personal, información financiera sin la debida protección
3.- Revisar que unidades externas no contenga información confidencial sin la protección necesaria.
4.- Revisar que las máquinas de los usuarios se encuentren correctamente apagadas, o sesiones bloqueadas en caso de que el empleado no se encuentre en la misma.
5.- Reportar al gerente o responsable del área por nota, el incumplimiento o expuesto de seguridad que haya encontrado. Identificando el expuesto de seguridad y el usuario responsable del mismo.

- **Política de Utilización de los Servicios de Red**

Las conexiones no seguras a los servicios de red pueden afectar la seguridad de toda la Institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El administrador de la red es el responsable de otorgar los permisos tanto a servicios como recursos de la red, únicamente de acuerdo al pedido formal del responsable de cada unidad.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad de la empresa.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.
b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

Para este control se implementó la asignación el procedimiento de asignación de privilegios.

Autenticación de Usuarios para Acciones Externas

Las conexiones externas son de gran potencial para accesos no autorizados a la información del Organismo. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. Para poder implementar una mejora en la seguridad del ingreso desde el internet a nuestra red, en específico al aplicativo que se encuentra en el servidor Lotus, se implementó el protocolo de encripción SSL en el servidor, para que esta se combine con la seguridad propia del software y evitar accesos no autorizados (**ANEXO H**)

Protección de los puertos (PORTS) de Diagnóstico Remoto

Para poder determinar cuáles realmente requieren estar abiertos y cuales deben estar cerrados, en este caso vamos a trabajar con una herramienta que nos permita determinar cuáles puertos se encuentran abiertos. Para nuestro caso proponemos pasos tanto para los servidores así como los equipos en Windows, con la ayuda de una herramienta que realice este chequeo además de la administración de la red, ver **ANEXO I**. Además se establece el procedimiento para deshabilitar servicios y puertos innecesarios en los servidores.

Configuración de Acceso por Defecto

Para asegurar que no exista alguna equivocación por parte del administrador del sistema, por defecto se configuran a los usuarios como usuario estándar, es decir sin privilegios de instalación de programas, modificación de archivos de red, desinstalación de programas y sin acceso a los sistemas y aplicaciones.

Al igual debe suceder con los módems y switch se configuran listas de control de acceso que por defecto bloqueen todo y solo permitan el paso de lo que se configura.

Monitoreo de Control de Acceso

Para tener un control más adecuado de la red, identificación de vulnerabilidades en la misma, que puedan conllevar a problemas de control de acceso en el **ANEXO J** se muestra la configuración que realizamos para la implementación de un firewall que nos permitirá utilizar las ventajas del sistema operativo Linux de un servidor para un mayor control de acceso. Así como también se indica en el **ANEXO K** la implementación del aplicativo MRTG que nos permitirá llevar un control del tráfico de la red para determinar un posible problema debido a un incremento considerable en el tráfico de la red.

- **Adquisición, Desarrollo, y Mantenimiento de Sistemas de Información**

Se pueden establecer políticas para el manejo de información crítica que incluya controles criptográficos sobre la misma, a continuación se indica el procedimiento que se debe seguir:

1. En todas las máquinas se debe tener instalado el aplicativo de encripción PGP (**ANEXO D**), pues es un software muy útil sobre todo en redes de mediano tamaño.
2. Al momento que se desee enviar o transportar información confidencial, se debe utilizar el aplicativo PGP para encriptar dicha información.
3. La clave que se utilice para la encripción de la información se debe enviar únicamente a las personas que van a intercambiar la información encriptada. De ser necesario transmitir la información a otras personas es necesario que la persona que envíe el documento utilice diferentes claves de encripción para los diferentes destinos para que no haya la posibilidad de intercepción y recepción de información por parte de personas no autorizadas.
4. El intercambio de claves se debe realizar mediante un correo electrónico previo al envío de la información confidencial.

El procedimiento que se debe seguir para un control de cambios es el siguiente:

1.- SOLICITUD DE CAMBIO: El requerimiento de solicitud de cambios debe presentarse al responsable de la unidad, y presentarle las actividades que se van a realizar en el cambio.

2.- APROBACION DEL CAMBIO.- los requerimientos individuales de cambio deberían justificar la razón y claramente identificar los beneficios y las posibles fallas del cambio. La directiva debe analizar el requerimiento de cambio y posiblemente solicitar mayor información antes de que el cambio sea aprobado.

3.- DOCUMENTACION DEL CAMBIO.- Cuando el cambio es aprobado, debe empezar una documentación donde se vaya identificando todos los pasos que se siguieron hasta finalizar el cambio.

4.- PRUEBAS y PRESENTACION.- El cambio debe ser completamente probado para cubrir algún resultado inesperado.

5.- IMPLEMENTACION.- Cuando un cambio es completamente probado y aprobado, se programa el desarrollo para la implementación, el cual debe constar del procedimiento de monitoreo del mismo.

6.- DOCUMENTACION DE CONTROL DE CAMBIOS.- Los cambios que deben ser documentados son:

- Instalación de nuevas computadoras
- Instalación de nuevas aplicaciones
- Implementación de configuraciones diferentes
- Instalación de parches y actualizaciones
- Nuevas tecnologías integradas
- Políticas, procedimientos actualizados.
- Nuevos dispositivos conectados a la red.

Restricción del Cambio de Paquetes de Software

Para evitar que los usuarios puedan modificar, sin autorización previa cualquier tipo de software, las cuentas de los empleados en el dominio no tienen permisos para realizar ninguna de estas actividades, así como tampoco pueden instalar ningún tipo de software ni remover sin previa solicitud al administrador de red y sin autorización del responsable de cada área.

Canales Encubiertos y Código Troyano

El antivirus que van a implementar en la empresa cuenta con características necesarias para detectar código troyano y canales encubiertos, por lo cual es necesario la implementación de las especificaciones realizadas para mantener el antivirus actualizado y realizar un chequeo constante de la máquina. En el **ANEXO C** se especifica la forma de configurar el antivirus en cada máquina para mantener protegidos a los usuarios.

- **Gestión de Incidentes de la Seguridad de la Información**

Divulgación de Eventos y de Debilidades de la Seguridad de la Información

Cuando un incidente ha sido reportado, se pueden tomar diferentes acciones como son:

- Validar que efectivamente el incidente se ha producido
- Examinar archivos y registros para detalles del ataque
- Determinar si puede garantizarse una acción legal
- Reevaluar o modificar la seguridad de red de las computadoras en general.

Las pautas siguientes ayudan a las organizaciones a entender y responden a los varios niveles de uso de la computadora impropio.

Molestia.- Estas ofensas generalmente muestran una falta de consideración de otros usuarios de la computadora, pero no amenaza retiro o integridad de la computadora o viola cualquier principio ético. En otros términos, el individuo mostró el juicio pobre simplemente. La organización debe responder emitiendo al usuario un verbal, copia electrónica, o hardcopy que advierte que su o sus acciones no eran aceptables.

Ética cuestionable.- Estas ofensas involucran a menudo violaciones dónde las ética de acciones son cuestionables o cuando el retiro de una persona o integridad de la computadora fueron violadas. La organización podría responder suspendiendo la cuenta del usuario o acceso de la computadora hasta una sesión formal con un Información Tecnología personal miembro se ha asistido. Una copia de la Internet acceso política de la organización debe darse al usuario con el área específica o la ofensa resaltó.

Criminal.- es cuando un usuario compromete una ofensa que requiere la investigación por local, declaración, o la entrada en vigor de la ley estatal.

Cualquier usuario que compromete una ofensa delictiva debe comisar todos los derechos a los privilegios de la computadora de la organización. Cualquiera y toda la información pedidas por local, declare, o la entrada en vigor de la ley federal debe proporcionarse. Si el usuario se encuentra culpable de la ofensa bajo la investigación, debe darse por terminado el contrato con el mismo.

A continuación se detallan los pasos para iniciar el proceso de reportes de incidentes de seguridad encontrados en Uniplex:

Objetivo:	Responder apropiada y rápidamente ante un incidente o "issue" de seguridad.
Roles:	Identificar al responsable del área donde se ha generado un incidente de seguridad y trabajar de forma conjunta con el administrador de la red.
Inputs:	Reporte de incidente o "issue"
Outputs:	• Comunicación del incidente • Respuesta ante el incidente • Investigación del incidente • Planes de acción correctivos • Reporte de mediciones • Mejora de los procesos
Consideraciones:	La fuente y calificación de severidad del incidente determina las acciones a seguir.

Tabla 4.8 Proceso de Reportes de Incidentes

Análisis del Incidente.- Los incidentes de seguridad son reportados por diferentes personas en la organización. Por lo cual es necesario que todos los incidentes reportados involucren al administrador de la red y el responsable de cada área. Para que de forma conjunta se puedan definir el procedimiento a seguir para los diferentes problemas.

Reporte del incidente.- Evaluado el incidente con el Administrador local del servicio, se realiza un registro del incidente para que se pueda hacer un seguimiento hasta la solución del mismo. Los pasos necesarios para reportar el incidente son los siguientes:

1.- Determinar si el incidente representa un serio problema como son: acceso no autorizado a información confidencial, alteración de la integridad de un servidor, negación de servicio, alteración de un servicio Web, penetración al sistema, destrucción de datos, fraude, crimen, etc.

2.- Contactar al administrador de la red para reportar el problema

3.- Describir el problema

4.- El administrador del sistema debe inmediatamente registrar el incidente en un archive para identificar información relacionada a cada evento.

5.- EL administrador conjuntamente con el responsable de cada área deben realizar el procedimiento necesario para mitigar dicho incidente en caso de existir. Estos procedimientos dependen del tipo de incidente, pues por ejemplo en caso de una vulnerabilidad en un sistema operativo debido a un virus en la red se debe eliminar el virus. Informar los procesos que deben seguir los usuarios para que el daño no se propague en la red.

Administración de Incidentes y Mejoras de la Seguridad de la Información

En este procedimiento se debe considerar:

- Como inició el incidente

- Que fallas o vulnerabilidades fueron explotadas
- Como ganaron el acceso
- Como se dieron cuenta del problema
- Como se resolvió temporalmente el incidente
- Si los procedimientos de la resolución de incidentes existentes eran adecuados o requieren la actualización

- Gestión de Continuidad del Negocio

Aspectos de la Gestión de Continuidad del Negocio

Al desarrollar el plan de la continuidad del negocio para la empresa, se debe considerar los parámetros sobre los cuales se va a desarrollar el mismo para poder los desastres.

Proceso de Gestión de la Continuidad del Negocio

Los responsables de cada área, deben determinar las aplicaciones críticas de las mismas y desarrollar procedimientos regulares para mantener respaldos continuos de los procesos críticos de cada área. El plan de contingencia de cada proceso debe considerar como mínimo:

- La administración de los recursos críticos, en caso de ser necesaria la implementación del plan de contingencia.

- Identificar los riesgos. Cada riesgo debe identificarse con qué pasos sería necesario detenerlo, pues es más barato evitar la crisis que repararla; por lo cual todos los planes deben tener un enfoque de prevención.
- Documentar el impacto de una pérdida extendida a los funcionamientos y funciones de negocio.
- Debe ser un plan entendible, fácil usar, y fácil para mantener por todos los miembros de la organización.

Desarrollo e Implantación de Planes de Contingencia

El plan de contingencias desarrollado para aplicar en Uniplex se adjunta en el **ANEXO B**

Cumplimiento

Cumplimiento con los Requisitos Locales

Derechos de Propiedad Intelectual

Entre los controles que recomienda la Norma ISO 27002 se considera que los empleados únicamente utilicen material autorizado por la organización.

Uniplex solo debe autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

Salvaguarda de los Registros de la Organización

Los registros críticos de la empresa se deben proteger contra pérdida, destrucción y posibles falsificaciones, los formularios que se pueden utilizar para mantener un control de los registros es:

Tipo de Registro	Sistema de Información	Período de Retención	Medios de Almacenamiento	Responsables

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.

b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.

c) Mantener un inventario de programas fuentes de información clave.

d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

- **PROTECCIÓN DE LOS DATOS Y DE LA PRIVACIDAD DE LA INFORMACIÓN PERSONAL**

Para este control se redactó un Conducta que deberían cumplir los empleados, la copia firmada del compromiso será retenida en forma segura por la empresa.

(**ANEXO L**). A través del Compromiso de Confidencialidad se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado

- **REVISIONES DE LA POLÍTICA DE SEGURIDAD Y DE LA CONFORMIDAD TÉCNICA**

CONFORMIDAD CON LA POLÍTICA DE SEGURIDAD

El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad, este período como mínimo debe ser cada 6 meses. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.

b) Proveedores de sistemas.

c) Propietarios de información.

d) Usuarios.

4.5. Costos Referenciales para la Implementación del Sistema

Una vez que hemos concluido la implementación del Proyecto de Gestión de Seguridad de Información en Uniplex, presentamos los costos referenciales tomando en cuenta que se trata de una empresa pública sin fines de lucro, se consideró todos los costos involucrados para mejorar la seguridad en la organización en base al previo análisis, no todas las soluciones propuestas han sido implementadas, debido al costo que estas representan, pero se ha dado un análisis para estas soluciones en caso de que la corporación las requiera en un futuro cercano.

Para el análisis económico consideramos 2 grupos principales de costos:

COSTO EN EL DISEÑO.- Este es el costo al inicio del análisis de la situación actual de la Organización, documentación para el diseño, recursos invertidos antes de la implementación del sistema.

COSTO EN LA IMPLEMENTACIÓN.- Es el costo incurrido y propuesto como resultado del estudio de las amenazas y vulnerabilidades, y los controles propuestos para minimizar los mismos.

A continuación describimos los valores para cada uno de los costos anteriores:

- **Costo en el Diseño**

Aquí se consideran los valores de los elementos necesarios previos a la implementación del PGSI. Los valores que se consideraron son:

1.- Personal.- Es el costo de las personas que trabajamos en el proyecto, considerando el tiempo invertido, la investigación involucrada, así como los recursos personales necesarios para poder realizar el diseño del PGSI y recopilar la información necesaria.

2.- Varios.- Para el PGSI es necesario tener conocimiento de la norma completa para seguir con las recomendaciones que se indican para la implementación, por lo cual fue necesario adquirir las normas para proseguir con el diseño.

En la etapa de diseño no fue necesario ningún tipo de Hardware o Software, pues lo que realizamos fue la obtención de la información necesaria de la situación actual de la empresa y su respectivo análisis.

A continuación la tabla donde se consideran los costos antes mencionados

RECURSO	DESCRIPCION	CANTIDAD	COSTO TOTAL ($)
Personal	Viáticos y Comisiones por dos meses	2	1000
Varios	Documentación de Norma ISO 27002	1	100
TOTAL			1100

Tabla 4.9 Costos de Diseño

- **Costo en la Implementación**

En estos costos se consideran los valores de los elementos necesarios para la implementación del PGSI. Estos valores son los siguientes:

1.- Personal.- Es el costo de las personas que trabajamos en el proyecto, considerando el tiempo invertido, capacidad intelectual, así como los recursos personales necesarios para poder realizar la implementación del PGSI

2.- Hardware.- El hardware necesario es principalmente para cubrir el control de la seguridad física de la corporación, así como un equipo para mejorar la seguridad en la red de la empresa

3.- Software.- La mayoría de Software que utilizamos en nuestra implementación es libre, o software con licencia que ya se encuentra en UNIPLEX. Esto lo realizamos para minimizar al máximo los gastos y aprovechar de mejor forma los recursos disponibles. Las soluciones con Software con costo no se han podido implementar porque no se pudo invertir en los mismos, pero los ponemos en consideración para referencia de la Organización.

A continuación la tabla donde se consideran los costos antes mencionados:

RECURSO	DESCRIPCION	CANTIDAD	COSTO TOTAL ($)
Personal	Viáticos y Comisiones por tres meses	2	1500
Hardware	Extintores Clase C	3	1110
	Candados para portátiles	6	150
	Disco Duro para respaldos de Servidores	1	250
	Sistema de Badgets para seguridad física, tanto Hardware como Software	1	11620
	Firewall	1	2097
Software	PGP	1	239
TOTAL			16966

Tabla 4.10 Costos en la Implementación

- **Costo Total**

Una vez realizado el análisis de los costos de diseño e implementación del PGSI podemos obtener el costo total para la empresa:

RECURSOS	COSTO TOTAL ($)
Costo en Diseño	1100
Costo en la Implementación	16966
TOTAL	18066

Tabla 4.11 Costos Referenciales

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. El Sistema de Gestión de Seguridad de Información se define para cada departamento en base a los riesgos a que esté expuesta y los aspectos intrínsecos de su funcionamiento, y debe alinearse con la actividad de la organización; para realizar de forma estructurada, sistemática y metódica la gestión de la seguridad de Tecnologías de Información.

2. Es necesario definir los responsables de cada recurso de la organización y de su protección, siendo conveniente delimitar claramente el área de responsabilidad de cada persona para que no existan huecos ni problemas de definiciones claras de responsabilidades.

3. Las medidas para evitar accesos no autorizados y daños en los sistemas suelen ser barreras físicas y de control de cualquier tipo, pero también la ausencia de información sobre lo que contiene un área segura y la falta de signos externos que puedan hacer adivinar su contenido.

4. Una adecuada monitorización del uso de los recursos de la red permiten determinar posibles cuellos de botella que derivarían en fallos del sistema y de seguridad, dando tiempo a planificar las ampliaciones o actualizaciones del sistema con la suficiente antelación.

5. No es necesario extender el PGSI a toda la organización, pues lo primordial es centrarse en los procesos principales de la organización donde se concentra la mayor parte de las actividades relacionadas con la gestión de información, que suele coincidir con las áreas de sistemas de información donde la seguridad de la información que se gestiona es crítico para el desarrollo de las actividades de negocio.

6. Para poder manejar y responder de forma clara a incidencias de seguridad, es necesario tener especificado un proceso de notificación de incidencias de forma que este sea claro y conocido por todos los empleados de la organización para de esta forma minimizar la probabilidad de recurrencia en el problema.

7. La seguridad para los medios de almacenamiento de información deben ser consideradas en las políticas de seguridad, estableciendo los procedimientos para protección contra robo, daño o acceso no autorizado y procedimientos para su destrucción o borrado total cuando no vayan a ser utilizados de nuevo.

8. Se deben definir y documentar las reglas y derechos de acceso a los recursos del sistema de información para cada usuario o grupo de usuarios en una declaración de política de accesos. Esta política debe ser coherente con la clasificación de los activos y recorrer exhaustivamente el inventario de recursos.

9. Es de gran importancia limitar la asignación de privilegios que permitan evitar los controles de acceso estándar ya que son la principal

vulnerabilidad, por lo que deberán estar perfectamente identificados, asignarse sobre la base de la necesidad de uso y evento por evento y a un identificador de usuario distinto al de uso habitual. Los privilegios tienen que revisarse de forma periódica para evitar la existencia de privilegios que ya no son necesarios.

10. Para determinar el alcance del PGSI se utilizó el método de las eclipses en la cual está implícita los procesos de la empresa y de esa manera permite tener una perspectiva más clara de los procesos indispensables que ayuden a cumplir con los objetivos de negocio y por ende la identificación de los activos de información que forman parte de estos procesos.

11. La planificación es una parte crucial para una adecuada implementación del PGSI, en donde se analiza el negocio para determinar los activos más importantes, posteriormente se realiza un análisis de los riesgos que las amenazas y vulnerabilidades pueden generar, los cuales serán gestionados con controles apropiadamente implementados y criterios establecidos.

12. Una de las bases fundamentales es el apoyo de la alta gerencia, ya que se requiere un cambio de cultura y concientización hace necesario el impulso constante de la Dirección.

13. Para la implantación de un estándar para la seguridad de la información es necesario contar con una política de seguridad adecuada. La política poner de manifiesto el compromiso de la dirección en relación a la protección de la información y establecer el marco general de seguridad para el negocio y su objetivo de negocio.

14. Es primordial la elección del método de análisis de riesgos, este debe ser elegido de acuerdo a las características del negocio, para nuestro caso se escogió GMIS ya que se ajusta las características de la norma ISO 27002.

15. Una de las ventajas de la norma ISO 27002 es que puede ser implementada tanto en empresas pequeñas como en grandes organizaciones.

16. Se debe tomar en cuenta que el objetivo de la evaluación del riesgo es identificar y valorar los riesgos a los cuales los sistemas de información y sus activos están expuestos, para identificar y seleccionar los controles adecuados que minimicen los riesgos identificados.

17. Para el establecimiento de la seguridad de la información se consideran tres pilares fundamentales: tecnología, procesos y las personas: Las empresas comúnmente invierten grandes sumas de dinero en tecnología y definición de procesos, y se han descuidado del personal de la empresa convirtiéndose así en el eslabón más débil de la cadena de seguridad, por esta razón es fundamental concienciar y fomentar la cultura de la seguridad de la información.

18. La seguridad de la información no se debe considerar como un aspecto solo tecnológico sino de tipo organizacional y de gestión, es decir organizar la seguridad de la información e implementar la seguridad en base a los requerimientos de la empresa.

RECOMENDACIONES

1. Identificar de forma clara cuales son los activos y asignarles un grado de protección según su criticidad, indicando como debe ser tratado y protegido; para de esta forma mantener una adecuada protección de los activos.

2. Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar con un PGSI es permanente para lo cual es necesario de un proceso continuo, más no de acciones puntuales

3. Documentar los procedimientos operativos, cualquiera que sea su tipo, detallándose para cada tarea sus requerimientos de programación, interdependencias con otros sistemas, tareas de mantenimiento previstas y procedimientos de recuperación ante incidentes.

4. Es aconsejable que se aumente el personal que administra el departamento de IT, pues al implementar el PGSI se incrementan las responsabilidades y al recaer en una sola persona se vuelve complicada la ejecución de las diferentes tareas.

5. Se deben definir el comité de recuperación ante contingencias, para que se pueda definir de forma clara las funciones y responsabilidades de cada miembro ante desastres.

6. Es recomendable que el desarrollo de cualquier sistema de gestión de seguridad de información respete las normas y leyes vigentes del país, como son por ejemplo el respeto a los derechos de propiedad intelectual.

7. Se recomienda la implementación de la norma 27002 porque a más de proteger la empresa, permite mejorar la imagen al exterior.

8. La seguridad de la información debe ser considerada como un proceso de mejoramiento continuo y no un estado estático, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la empresa.

ANEXOS

ANEXO A

GUÍA PARA LOS USUARIOS

Contraseñas

Estas son las llaves de la información electrónica. Alguien puede leer la información que no está protegida con contraseñas. Si usted escoge contraseñas débiles, es posible que alguien las adivine o descifrarlas. Algunas pautas para contraseñas fuertes:

- Abra el diccionario en una página aleatoria y seleccione una palabra larga (por ejemplo de 4 sílabas). Use esta palabra pero inserte el número de página en la mitad de esta. Por ejemplo si <menesteroso> en la página 164 de su diccionario, su contraseña es <menes164teroso>. (Si olvidó su password, usted debe recordar el número de página que usted seleccionó.
- Escoja una frase que signifique algo para usted. Por ejemplo “mi cebra se llama Spot y y tiene 9 años”. Esta puede ser escrita así en una contraseña <mcsllS&t9a>. Esta es una contraseña muy fuerte porque usa letras, números y caracteres especiales.

Con las contraseñas se debe cumplir:

- Usar al menos 8 caracteres en la contraseña.
- Estar seguro de cambiar las contraseñas regularmente, por ejemplo cada mes.

- Si un empleado abandona su cargo, se debe cambiar su vieja contraseña inmediatamente.
- Use una contraseña para cada aplicación, nunca use la misma en todas las aplicaciones.

Por otro lado, hay cosas que nunca debe hacer con las contraseñas:

- Nunca escriba su contraseña
- Nunca use su nombre, el nombre de su compañero, el nombre de sus hijos, cumpleaños o algo más acerca de usted o su familia que sean conocidas o pueden ser fácilmente descifradas con un poco de ingeniería social.
- Nunca use códigos especiales que sean relacionados con usted, por ejemplo: su número de teléfono, su número de cédula, el número de licencia del Software, o cualquier cosa que pueda ser descifrada por alguien.
- Nunca use los mismos números o letras, por ejemplo <1111111>, en un password o nunca use la contraseña <contraseña> porque eso lo primero que un hacker intentaría hacer.
- Nunca comparta su contraseña con otras personas.
- Nunca use las contraseñas que vienen preestablecidas con un Software, esta contraseña debe ser cambiada.
- Nunca tenga almacenado en su PC “Recordar contraseñas”, esta manera es fácilmente recuperada.

En resumen, trate su contraseña con cuidado, escoja una fuerte y cámbiela regularmente

Virus, Gusanos y Troyanos

Cualquier software antivirus podrá actuar porque todos trabajan más o menos de la misma manera y hacen la misma clase de trabajo. Lo más importante es simplemente usar uno.
Lo que la mayoría de personas no considera es que el software antivirus debe ser actualizado. Esto significa periódicamente actualizar porque todos los días se escriben nuevas versiones y estas están disponibles.

Si usted no instala un SW Antivirus y no lo actualizada, usted esta 100 % garantizado que tarde o temprano será víctima de un virus.

Cualquier SW Antivirus que usa, usted debe instalarlo para verificar automáticamente los nuevos datos. De esta manera, si usted tiene nuevos datos en un disket, un CD o a través de Internet, el SW chequeará los virus antes de que usted pueda ser víctima de cualquier daño.

La regla de oro es que si cualquier virus afectó archivos o datos, estos deben ser destruidos. Algún antivirus exigirán desinfectar los archivos, pero esto nunca es garantizado. Lo más seguro es que destruya el archivo con el virus. Si es el correo electrónico, destrúyalo sin abrirlo.

Spam

Usted puede pensar que ésta es simplemente una molestia, pero desafortunadamente tiene sus peligros también. Spam puede ser:

- Un frente para un fraude
- Un correo electrónico en cadena
- Contiene código oculto que alterará las configuraciones en su computadora (por ejemplo: dirigirle a usted a un sitio porno)
- Contiene código oculto el cual convierte su computadora en una parada spam (por ejemplo: una gran cantidad de spam es enviada desde su computadora a otras computadoras), envía el spam a todas las direcciones de sus clientes y con una nueva copias de spam ataca.

Hay algunas reglas que usted necesita seguir con el correo electrónico spam y si sigue estos consejos minimizará cualquier riesgo:

- Si el correo electrónico obviamente no tiene ningún valor, ni es relevante para usted o su empresa, solo bórrelo sin abrirlo.
- Nunca responda al correo electrónico spam. Su dirección de correo electrónico ha sido recogido de alguna manera y ellos no saben si usted realmente existe.
- Si usted contesta, usted estará confirmando su existencia y usted conseguirá mucho más del correo spam.
- No hacer clic en cualquiera que diga “haga clic aquí para quitar su nombre de nuestra lista del envío”. Normalmente es un truco. Usted no será removido, usted solo confirmará su existencia.
- No dar su dirección de correo electrónico a cualquiera, excepto a personas en las usted pueda confiar.

- Esto es muy difícil de ejecutar en un negocio, porque usted quiere que su dirección de correo electrónico esté ampliamente disponible. Puede considerar dos direcciones de correo electrónico uno públicamente disponible y otro para uso personal.
- Si un sitio de Internet le pide su dirección de correo electrónico, haga una valoración de riesgos rápida. ¿Es una organización legítima que tiene establecida una reputación? ¿Es alguien que usted nunca ha escuchado antes o no tiene una dirección física de la empresa en el sitio Web? Recuerde que el embustero planea aparentar una empresa legítima.
- Sitios de Internet que le prometen removerlo de la lista de direcciones spam generalmente no lo hacen. Nunca los use.

Spyware

Estos son pequeños programas que se insertan en el sistema de la computadora para recoger secretamente la información sobre usuarios / empresa sin que ellos lo sepan.

Esto es principalmente para anunciar los propósitos, puede recoger información sobre direcciones de correo electrónico e incluso las contraseñas y detalles de tarjetas de crédito. Recientemente ha habido advertencias oficiales sobre spyware que se usan para recoger información sensible comercial, por ejemplo: detalles del contrato.

Spyware no es una buena idea y el usuario cuidadoso trata de restringirlo o quitarlo completamente. Hay dos paquetes buenos disponibles del Internet, los cuales removerá el spyware. Los dos paquetes son gratis para el uso personal, pero se espera que las empresas paquen por estos paquetes. Ellos son:

- Lavasoft's <Ad-aware>
- Spybot

Es recomendable que se descargue los dos paquetes, y los ejecute al menos una vez a la semana. Usted se sorprenderá cómo ellos encuentran. (No se olvide, que también estos paquetes deben ser actualizados.

Parches

Los parches son poco conocidos pero son muy importantes y están relacionados con los virus y el hacking. Todos los softwares tienen problemas y defectos. En la mayoría de casos, los defectos son minoritarios, es así que estos son ignorados y probablemente no tendrán impacto en el negocio. Mientras que otros defectos son demasiados importantes para ser ignorados.

Todos los productores de software proveen parches. Si tiene una computadora que no está conectada a ningún sitio probablemente no necesitará preocuparse por los parches mientras su computadora está trabajando correctamente.

El problema principalmente tiene relación con el sistema operativo del computador.

Este es el programa básico que corre en el corazón del computador. Usted probablemente usa alguna versión de Microsoft Windows, Linux. Todos los sistemas operativos necesitan actualizarse de un tiempo a otro. Pero muchas aplicaciones también necesitan ocasionalmente parches.

Si no tiene actualizado su software, tiene el riesgo de que el software falle o en el caso de browser o email un software malicioso corrompa su computador, o un usuario malicioso tenga acceso a su computador.

La mayoría de proveedores de software proporcionan un servicio de notificación vía email a sus clientes cuando un nuevo parche está disponible. Estas notificaciones pueden ser de criticidad baja y ser actualizadas en cualquier tiempo o pueden tener criticidad alta y deben se actualizadas inmediatamente. La continuidad del negocio puede depender de esto.

La mayoría de proveedores de software ofrecen automáticamente actualizaciones vía Internet.

Backup

El respaldo es el proceso de tomar una copiar de los datos electrónicos, como una copia de archivos contables. Es necesario que usted realice un respaldo continuo de su información, pues el momento menos pensado fallos en los equipos pueden ocasionar la pérdida de su información. Debe considerar lo siguiente:

- Un respaldo formal y eficiente evitará que amenazas naturales o no intencionadas deje de funcionar su negocio. Usted puede copiar datos a:

- Cinta (un antiguo método pero aún es considerado parque puede ser rehusado)
- Un duplicado disco duro (preferiblemente uno removible)
- Un CD o un DVD

Usted debe considerar hacer múltiples respaldos para datos críticos. Un apropiado respaldo debería considerar lo siguiente:

- Al final de cada día - respaldo de todos los archivos que han cambiado en el día
- Al final de cada semana – respaldo de todas las aplicaciones (cuentas, correspondencia, etc)
- Al final de cada mes – respaldo del sistema operativo

Si usted tiene que restaurar la computadora después de una falla catastrófica, se deberá usar el respaldo de “fin de mes” para restaurar el sistema operativo, luego se usará el respaldo de “fin de semana” para restaurar las aplicaciones y finalmente se usará el respaldo de “fin de día”. De cualquier manera, usted ha reconstruido el sistema completo. Si cualquiera de los respaldos no puede ser leído, usted puede usar un respaldo previo y empezar de ahí.

Uno de los mayores problemas con respaldos ocurre cuando el propietario olvide rotular la información apropiadamente.

Robo de Información e Identidad

Para un negocio es de vital importancia tener la información almacenada apropiadamente, esto incluye papeles o copias electrónicas.

Un individuo puede robar su ID para realizar algún fraude. Mientras usted no es responsable por el fraude perpetrado por otros, el problema después del robo de un ID es recuperar credibilidad con bancos y otras organizaciones financieras.

Algunas cosas que no debe hacer:

- Nunca de información personal en Internet, vía e-mail, en el teléfono o por cartas a menos que usted esté seguro que la comunicación es confiable.
- Recuerde que los bancos nunca preguntan a los usuarios confirmar su password o código de acceso vía email así que no proporciones esta información.

Cualquier evento extraño debe ser reportado inmediatamente para ser investigado.

ANEXO B

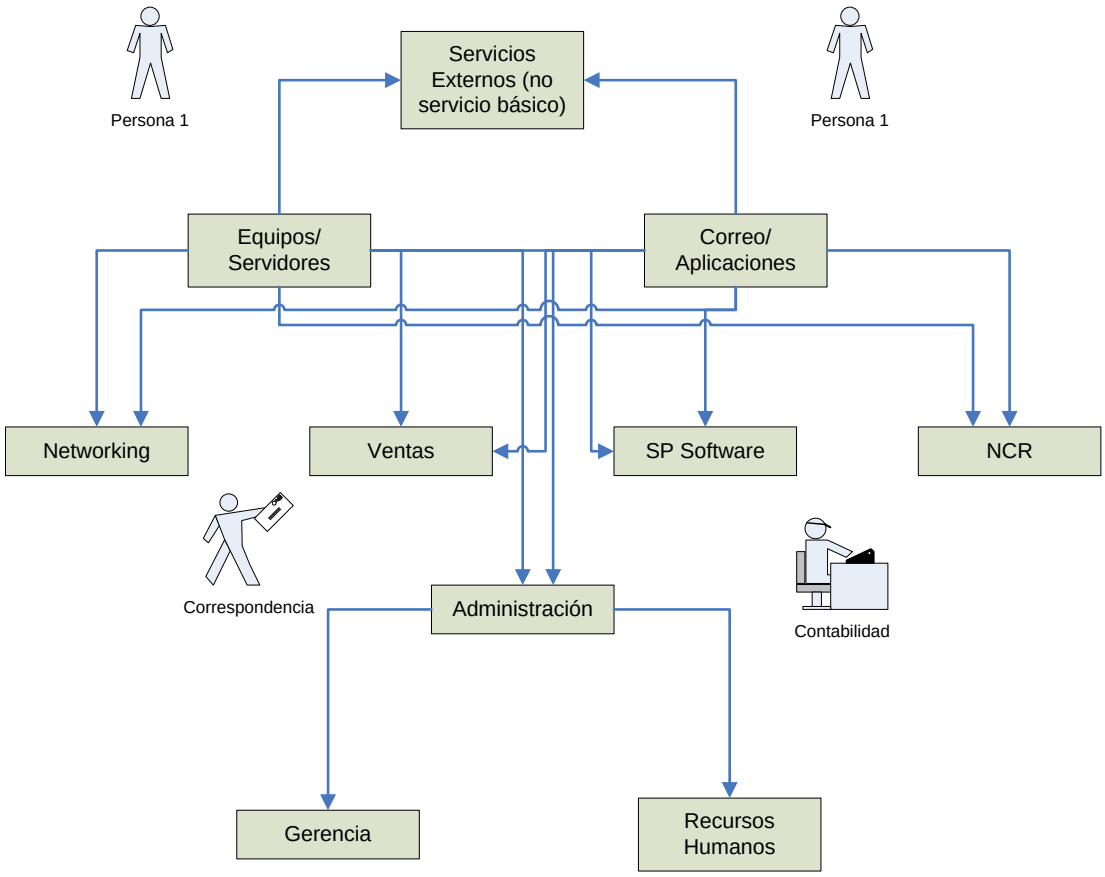
PLAN DE CONTINGENCIA

Este plan de contingencia establece procedimientos para que la empresa se recupere de interrupciones. Los siguientes objetivos han sido establecidos para este plan.

- Maximizar la efectividad de las operaciones del plan contingencia a través de un plan establecido.
- Identificar las actividades, recursos y procedimientos requeridos para poder desarrollar las actividades de Uniplex.
- Asignar responsabilidades en ese plan de contingencia y proveer guías para recuperación durante una interrupción de las operaciones normales.
- Asegurar una buena coordinación con entidades que participarán en las estrategias del plan de contingencia.

DESARROLLO

Para la asignación de prioridades de los módulos fue considerando un giro en el negocio y la importancia de cada módulo para cumplir con los objetivos del negocio.



MODULO	CRITICIDAD
Equipos/Servidores	Alta
Correo/Aplicaciones	Alta
NCR	Media
Networking	Media
SP Software	Media
Ventas	Media

Administración	Media
Gerencia	Media
Recursos Humanos	Baja
Servicios Externos (no servicio básico)	Baja

Cabe indicar que la prioridad de los módulos determinará el orden en el cual se deberán habilitar. A continuación se detallan los puntos a considerarse en el plan de contingencia así como les responsables de cada proceso.

Contingencia	a. Falla Eléctrica
AFECTA A	Seguridad del Edificio
DESCRIPCIÓN	Corte del suministro eléctrico(<4 horas)
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Baja
PERSONAL A SER INFORMADO	Jefe de Networking
ACCIONES	Verificar el tiempo de carga del UPS del centro de cómputo. Apagar servidores que no son de servicio crítico como es el caso del Servidor de Desarrollo, de bases de datos. • Comunicar al encargado • Verificar el funcionamiento • Comunicar de el cambio de corriente al personal que usa el sistema Ver :Contingencia (Temperatura Ambiente)
RECOMENDACIONES	• Tener vigente el contrato de mantenimiento del UPS del cuarto de servidores. • Adquirir una planta eléctrica propia para la empresa

Contingencia	A1. Falla Eléctrica
AFECTA A	Corte del suministro eléctrico programado por entidades estatales
DESCRIPCIÓN	Corte del suministro eléctrico(<4 horas)
TIEMPO DE FALLA (horas)	+ 4
CRITICIDAD	Alta
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	Verificar el tiempo de carga del UPS del centro de cómputo. Apagar servidores que no son de servicio crítico

	como es el caso del Servidor de Desarrollo, de bases de datos.. • Comunicar al encargado • Verificar el funcionamiento • Comunicar de el cambio de corriente al personal que usa el sistema Ver :Contingencia (Temperatura Ambiente)
RECOMENDACIONES	• Tener vigente el contrato de mantenimiento del UPS del cuarto de servidores. • Adquirir una planta eléctrica propia para la empresa

Contingencia	b. Inundación
AFECTA A	Seguridad del Edificio
DESCRIPCIÓN	El centro de computo se encuentra ubicado en las instalaciones de un antiguo cuarto, en el primer piso, muy cercano al área de servidores, se encuentra instalado un lavamanos, en el segundo piso sobre el centro de computo se encuentra ubicado un baño, los continuos cortes de agua pueden ocasionar que se olvide una llave de agua abierta lo que ocasionaría una posible inundación que afecte directamente a los equipos principales de Uniplex, ocasionando pérdidas totales o parciales, que interrumpan las actividades hasta solucionar el problema.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Alta
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Apagar el suministro de corriente eléctrica • Ubicar la posible causa de la inundación • Utilizar el ultimo respaldo existente e importar la base de datos en el servidor de respaldo • Informar a los prestadores de lo sucedido y comunicarles el tiempo aproximado que demorará el reestablecimiento del servicio. • Habilitar la red inalámbrica para que se pueda autorizar vía telefónica las prestaciones requeridas.
RECOMENDACIONES	• Inmediata: Retirar el lavamanos que se encuentra fuera del centro de cómputo. • Reubicar el centro de cómputo y dotar de todas las seguridades recomendadas para su operación como: o Piso falso o Rack de servidores o Alarmas • Tener en vigencia la póliza de seguros de Equipos Informáticos.

Contingencia	c. Incendio
AFECTA A	Seguridad del Edificio
DESCRIPCIÓN	El incendio puede iniciarse en instalaciones cercanas y propagarse a Uniplex ocasionando graves daños.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Alta
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Utilizar el último respaldo existente e importar la base de datos en el servidor de respaldo. • Informar a los prestadores de lo sucedido • Habilitar la red inalámbrica para que se pueda autorizar vía telefónica las prestaciones requeridas. • Reclamar la reposición de los equipos a la aseguradora.
RECOMENDACIONES	• Inmediata. Dotar al centro de computo como al edifico de detectores de humo. • Dotar al centro de computo de los debidos extintores de incendio • Contar con una póliza de incendio

Contingencia	d. Emisión de ceniza volcánica
AFECTA A	Seguridad del Edificio
DESCRIPCIÓN	Debido a que el Ecuador se encuentra rodeado por volcanes activos, Guayaquil puede estar afectado por la caída de ceniza volcánica, material que afecta al normal funcionamiento de los equipos eléctricos.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Media
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Informar a todo el personal de la empresa el comunicado de las entidades estatales sobre la inminente caída de ceniza en el Distrito Metropolitano de Guayaquil • Sellar las ventanas del edificio • Apagar los equipos de Computación Personales y desconectar los mismos de las tomas eléctricas • Proteger los equipos computacionales con cobertores plásticos • Apagar el aire acondicionado del centro de

	computo. • Apagar los servidores de Dominio y Correo • Realizar un respaldo total de la base de datos • Apagar los equipos que no sean necesarios Ver :Contingencia (Temperatura Ambiente)
RECOMENDACIONES	Sellar la ventana que se encuentra en el centro de computo

Contingencia	e. Falla Disco Duro Servidor Correo (Lotus)
AFECTA A	Integridad del centro de cómputo
DESCRIPCIÓN	Reporte del sistema de falla de un disco duro del servidor de base de datos. El sistema automáticamente se recupera debido al funcionamiento del RAID-5+1. Si un disco falla, los datos pueden reconstruirse debido a que los datos se almacenan en los arreglos de disco
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Media
PERSONAL A SER INFORMADO	Jefe de Networking / Jefe de SP Software
ACCIONES	• Solicitar al Jefe Administrativo Financiero la adquisición de un Disco de Similares características. • Informar a todos los usuarios internos y externos de Uniplex sobre la suspensión del servicio para el reemplazo del disco duro en el servidor de Base de Datos.
RECOMENDACIONES	• Mantener vigente el contrato de mantenimiento de los servidores. • Revisión semanal de los logs para detectar fallas en el sistema.

Contingencia	f. Falla del enlace de Comunicaciones de las sucursales
AFECTA A	Integridad del centro de cómputo
DESCRIPCIÓN	Falla del canal de comunicación de Ecuanet, que permite a los prestadores de salud acceder a los sistemas de Uniplex en forma remota.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Alta
PERSONAL A SER INFORMADO	Jefe de Networking
ACCIONES	• Resetear el Modem • Verificar el Servidor de dominio o Si esta encendido

	o Cable de red o Funcionamiento Tarjeta de red • Comunicarse con Ecuanet, e informarse sobre el tiempo necesario para recuperar el enlace. • Informar a toda la organización sobre la caída del enlace y del tiempo necesario para su recuperación.

Contingencia	g. Temperatura Ambiente
AFECTA A	Integridad del centro de cómputo
DESCRIPCIÓN	Mal funcionamiento del aire acondicionado. Generaría problemas con los servidores ocasionando daño en los mismos.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Media
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Comunicar al Gerente de sucursal del mal funcionamiento del aire acondicionado • Comunicarse con el responsable del mantenimiento del aire acondicionado • Apagar los equipos que no son indispensables en el centro de computo • Tener abierta la puerta del centro de computo • Poner en funcionamiento un ventilador convencional que proporcione ventilación al centro de computo
RECOMENDACIONES	• Tener vigente el contrato de mantenimiento del aire acondicionado • Adquirir un ventilador convencional • Tener en vigencia la póliza de seguros de Equipos Informáticos.

Contingencia	h. Robo
AFECTA A	Integridad del centro de cómputo
DESCRIPCIÓN	Perdidas totales o parciales de los servidores de Uniplex.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Alta
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Informar el tiempo de suspensión del sistema a los usuarios internos y externos de Uniplex. • Activar el equipo de respaldo que sustituirá al servidor de correo Lotus. • Restaurar el último respaldo de la información de la base de datos.

	• Reestablecer el servicio • Informar a los usuarios la fecha hasta la cual se recuperaron los datos. • Comunicar al Gerente del robo de los servidores para la adquisición de un nuevo servidor de datos.
RECOMENDACIONES	• Restringir el acceso restringido al centro de cómputo. • El centro de cómputo debe permanecer cerrado. • La puerta del centro de cómputo debe brindar las debidas seguridades de acceso. • La llave solo debe tener la persona responsable del centro de cómputo y una copia el Gerente. • Cambiar la chapa de seguridad del centro de cómputo o dotar de un equipo de acceso electrónico. • Si personas no autorizadas deben acceder al centro de cómputo se deberá informar al Jefe de Networking de Uniplex el horario, día y hora de su acceso. • Tener en vigencia la póliza de seguros de Equipos Informáticos..

Contingencia	i. Virus Informáticos
AFECTA A	Integridad de los datos
DESCRIPCIÓN	Perdidas totales o parciales de la información o de los servicios brindados por la red (Datos, Internet, correo, impresión)
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Alta
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Informar la suspensión de los servicios afectado por virus informáticos. • Excluir a la máquina afectada de la red de datos. • Ejecutar el software de antivirus en la máquina afectada. • Eliminar los virus de los archivos contaminados. • Informar a la empresa encargada de mantenimiento de equipos y soporte técnico sobre el particular. • Reestablecer el servicio
RECOMENDACIONES	• Adquirir un software de antivirus, que sea capaz de revisar automáticamente a todas las estaciones de trabajo, según la última versión de base de datos (virus) liberada en el Internet. El antivirus debe tener la facilidad de ser administrado a través de una consola central que permitirá monitorear el funcionamiento de todos los equipos de la red. • Establecer políticas de uso y acceso del Internet. • Definir políticas de seguridad de la información.

	• Mantener vigente el contrato de soporte técnico del software de antivirus informático.

Contingencia	j. Ataques Internos
AFECTA A	Integridad de los datos
DESCRIPCIÓN	Perdidas totales o parciales de la información de los servidores de datos o equipos del personal de Uniplex.
TIEMPO DE FALLA (horas)	Indeterminado
CRITICIDAD	Media
PERSONAL A SER INFORMADO	Jefe de Networking / Gerente de Sucursal (ventas)
ACCIONES	• Informar el tiempo de suspensión del servicio a los usuarios internos y externos de Uniplex, según sea el caso. • Restaurar el último respaldo de la información de la base de datos. • Reestablecer el servicio • Informar a los usuarios la fecha hasta la cual se recuperaron los datos.
RECOMENDACIONES	• Cumplir la política de respaldos. • Las claves y contraseñas son personales, no deben ser transferidas o difundidas a otras personas, no deben ser colocadas en lugares visibles. • Los usuarios son responsables de cada uno de sus contraseñas y claves, tanto para Windows como para los Sistemas. • Configurar el sistema para que las claves sean cambiadas automáticamente cada 45 días.

Anexos

Directorio Telefónico Personas Involucradas en el plan (Anexo 2)

Nombre	Empresa	Teléfono
Ing. Noralma Moreta	Uniplex	087270860
Ing. Jesús León	Uniplex	087270864
Ing José Patiño	Uniplex	087270871
Ing. Pedro Moncada	Uniplex	084660200
NOC Datos	Ecuanet	2562577 – 2687610

Nombre	Dirección	Teléfono

Cuerpo de Bomberos	Av. 9 de Octubre y Boyacá	25333666
Policía	Av.de las Américas junto al estadio Modelo	100

Respaldos

Objetivo: Salvaguardar la integridad y seguridad de los datos, adoptándose las precauciones técnicas para su almacenamiento y recuperación.

Es necesario sacar respaldos de los servidores de bases de datos, del aplicativo en cintas que luego pueden ser transportados a una oficina secundaria para almacenar esta información, en caso de algún fallo en la oficina principal.

Estos respaldos de los servidores son diarios, la principal ventaja es que el costo de implementación es bajo pues únicamente se requiere sacar respaldos diarios de la información de los servidores e información importante de máquinas de usuarios o departamentos.

Pero una de las desventajas es la dependencia del daño de la oficina central pues si es un daño mayor no se va a poder realizar una reposición rápida de la información.

Es necesario que se realice de forma constante la revisión del plan y del proceso del planeamiento, aunque, no es un substituto para probar el plan. La revisión del proceso es importante pues ayuda a asegurarse de que el plan es completo y de que han examinado y se han traído a todas las áreas de la compañía en el proceso.

EQUIPOS DE USUARIOS

Los respaldos son los medios más comunes para asegurar la disponibilidad de los datos en PCs. Es necesario que los usuarios mantengan un respaldo semanal de sus datos a fin de que puedan recuperar su información en caso de que se requiera una contingencia, los medios en los cuales los usuarios pueden sacar respaldos de su información son:

Disquetes

CD, DVD

Discos Externos (Portables)

BASES DE DATOS

Estructura

Usuario	Contenido
Clientes de Sybase	Servidor de pruebas
Equipos de Comunicaciones	NBX, Switch Principal 3Com
Antivirus	Servicio centralizado
Servidor de Dominio	Windows 2003 Server

- **Procedimiento para realizar backups en los servidores Sybase**

Ejp: RESPALDO Y RESTAURACION: ARBOR

Proceso : **Backups - I.Back-Arbor**

Generalidades:

Descripción/Propósito: El proceso de backups de Arbor se encarga de resguardar la información utilizada por la aplicación Arbor. Los datos de Arbor se almacenan en dos bases de datos, una de catálogo y otra de información transaccional.

Políticas:

BACKUPS PERIODICOS

BASES DE DATOS

- Ambientes implementados por base de datos -

DEMO : Por única vez un BACKUP de la base de datos de catálogo de tipo database.
Por única vez un BACKUP de la base de datos de transacciones de tipo database.
Backups no reciclables.

CONFIGURACION: Un primer backup de tipo database de la base de datos de catálogo
Un primer backup de tipo database de la base de datos de transacciones.
Una vez por día de tipo database de la base de datos de catálogo. (Periodo de configuración del proyecto)
Una vez por día de tipo database de la base de datos de transacciones. (Periodo de pruebas del proyecto)
Una vez por día un backup de tipo log de la base de datos de transacciones, a realizarse al mediodía (Almacenado en un file system en un disco distinto al que aloja al file system del device de datos de la base de transacciones). (Periodo de prueba de aplicaciones)
Backups del día viernes se guardan y los demás se reciclan.
Los archivos de backups de log serán reciclados luego de una semana de su realización.

DATA
CONVERSION :Un primer backup de tipo database de la base de datos de catálogo

Un primer backup de tipo database de la base de datos de transacciones

Un backup de tipo database de la base de datos de catálogo luego de finalizados los procesos de conversión

Un backup de tipo database de la base de datos de transacciones luego de finalizados los procesos de conversión

No se reciclan.

PROD : Una vez por día de la base de datos de transacciones de tipo database. Será extraído a las 23:00 pm.

Una vez por día de la base de datos de catálogo de tipo database. Será extraído a las 23:00 pm.

2 veces por día un backup de tipo log de la base de datos de transacciones

Uno a las once del día de tipo backup, truncate and log Uno a las quince del día de tipo backup, truncate and log

Es importante ajustar el tamaño del log, de acuerdo a las transacciones que se realicen entre los transaction backups para que este permita realizar a los usuarios su trabajo sin interrupciones. Por llenado de log.

Backup del viernes se guardan y los demás se reciclan

Los archivos de log serán reciclados una semana luego de su realización.

EJECUTOR : Operador de Sistemas

<u>BASES DE DATOS DEL MOTOR DE DATOS (MASTER DATABASE)</u>

FRECUENCIA : Luego de la configuración final.

Cada vez que :

- Se creen ó borren bases de datos
- Inicializen devices de base de datos
- Añadan nuevos dump devices
- Usar cualquier comando para mirroring de devices
- Crear o dropear system stored procedures, si están guardados en la master
- Crear, dropear o modificar un segmento
- Añadir nuevos logins al sql server

<u>BASES DE DATOS SYBSYSTEMPROCS</u>

FRECUENCIA : Cada vez que :

- Se cree ó borre algún procedure a esta base de datos. Solo se podrán borrar los store procedures que no sean del motor de base de datos.

EJECUTOR : Operador de Sistemas

Backups no se reciclan

SISTEMA OPERATIVO

FRECUENCIA : Una vez por mes
EJECUTOR : Operador de Sistemas

BACKUPS ESPECIALES

El equipo de Facturación puede solicitar backups adicionales de acuerdo a sus requerimientos. Debiendo atenderlos directamente el responsable, quién se encargará de solicitar la ejecución del backup.

MEDIO A UTILIZAR

- Disco
- Cintas

ALMACENAMIENTO

A cargo del área de sistemas como responsables:

- Backups: María Fernanda Yépez.

Los backups diarios se almacenan en caja fuerte, de modo que se los tiene disponibles a todo momento. Los backups semanales y mensuales se depositan en el casillero del Banco del Pichincha, Ag. La Prensa. y en la caja fuerte de BellSouth, ubicada en las Bodegas Parkenor.

NOMENCLATURA

Etiquetas Las etiquetas de los backups deberán contener :

<Servidor>
<Base de datos>
<Fecha >
<Tipo de respaldo>
<Tipo de reciclaje>

Por ejemplo :

kenan
TEST_CAT
Respaldo mensual
01/10/98
Rentención indefinida

Archivos generados automáticamente para los backups de las bases

<Base de datos> + <fechaYY/MM/DD>.dmp

Por ejemplo :
test_cat1998Mar14.dmp

UBICACIÓN DE BACKUPS

Servidor	Base de Datos	Ubicación	Tamaño	Hora
R50	PRODUCCION	/dumps/custadm.dmp		24:00
	CUSTADM	/dumps/custadm.log		(1 x día)
R50	PRODUCCION	/dumps/catalog.dmp		24:00
	CATALOG	/dumps/catalog.log		(1 x día)

EJECUCIÓN DE BACKUPS

La ejecución de los backups será de dos tipos :

a) Backup de tipo database
b) Backup de tipo trasaction log

Backup de tipo database

a) Modo manual

Pasos

1. Ingrese al server manager y digite sa y el password respectivo.
2. Ubique la cinta en el dispositivo respectivo
3. Revise que el dump device exista. De no ser asi creélo antes de proceder
4. Verifique que su base de datos este correcta. Para esto :
   Elija la tabla específica
   Haga click derecho y seleccione la opción consistency. Elija overall database y observe de haber algún error. De existir errores corríjalos antes de proceder con el backup.
5. Elija la base de datos respectiva. Haga click derecho y elija la opción de backup
6. En la pantalla de backup elija el tipo database y el dump device que va a utilizar para backapear. Elija además el servidor de backup SYB_BACKUP y las características de la cinta a utilizar en términos de densidad y tamaño de bloque.
7. Elija la opción notificar al cliente.
8. Nombre la etiqueta según la nomenclatura.

b) Modo automático

Pasos

1. Cree un script que ejecute dicho backup. El script necesario deberá ser de la forma :

Dump database <nombre de la database catalog> to “<tape_device>”.
Dump database <nombre de la database custadm> to “<tape_device>”.
Crear un programa que diga lo siguiente
isql -Usa -Ppassword -i <nombre del script>
Añadir como proceso cron el programa anterior con programación diaria a las doce de la noche y el usuario de mail del operador de backups.

2. Ubique la cinta en el dispositivo respectivo, antes de las doce de la noche.
3. Al día siguiente recoja la cinta
4. Revise que el proceso de backup haya terminado
5. Nombre la etiqueta según la nomenclatura.

Backup de tipo transaction log

Pasos

1. Cree un script que ejecute dicho backup. El script necesario deberá ser de la forma :

Dump database <nombre de la database catalog> to “<tape_device>”.
Dump database <nombre de la database custadm> to “<tape_device>”.
Crear un programa que diga lo siguiente
isql -Usa -Ppassword -i <nombre del script>
Añadir como proceso cron el programa anterior con programación diaria a las doce de la noche y el usuario de mail del operador de backups.

2. Ubique la cinta antes de las doce de la noche.
3. Al día siguiente recoja la cinta
4. Revise que el proceso de backup haya terminado
5. Nombre la etiqueta según la nomenclatura

a) Tipo automático

Deberá existir un cron que se encargue de extraer los backups diariamente. Las características de estos backups son como siguen :

Pasos

1. Ubicar la cinta a utilizar y probarla
2. Dejarla en el dispositivo de cinta que realizará el backup antes de las 23:00 horas en que correrá el backup.
3. Revisar el archivo log del proceso de backup. De existir algún problema deberá recurrir al proceso manual descrito arriba luego de corregir los problemas que existían.
4. Revisar la cinta al dia siguiente : dicha cinta deberá contener los backups de las tres bases de datos mencionadas anteriormente.

PRUEBA DE BACKUPS

La prueba de backups deberán ser realizadas al menos una vez por semana por los Operadores de Sistemas, de acuerdo al esquema general de Políticas de Backup

Pasos

1. Testear la calidad de la cinta a utilizar
2. Recuperar el backup en la base de datos intermedia de acuerdo a procedimientos descritos (sin backups de la situación actual).
3. De encontrar errores, volver a realizar el backup, corrigiendo la situación presentada. De no poderse notificar al soporte local de su base de datos.

RECUPERACION DE BACKUPS

La restauración de algún backup la realizará el área de Sistemas a pedido del equipo de Arbor, o de acuerdo al cronograma de backup establecido. Los usuarios podrán solicitar la recuperación de algunos objetos, para lo cual el área de sistemas realizará el load respectivo de dichos objetos.

Existen tres tipos de recuperaciones requeridas :

a) Solicitud de recuperación de base de datos completa a una fecha.
b) Solicitud de recuperación de tabla y contenidos de una fecha
c) Solicitud de recuperación de objetos estáticos (triggers, store procedures, rules, defaults, views) de la base de datos.

a) Solicitud de recuperación de base de datos completa a una fecha

- Deberá realizarse un backup de la base de datos antes de realizar dicha restauración.
- De no estar seguro de los contenidos a obtener en dicho backup. Deberá restaurar la base de datos en un ambiente transitorio.

b) Solicitud de recuperación de tabla y contenidos de base de datos a una fecha

- Deberá restaurarse el backup de la base de datos en un ambiente transitorio
- Permitir la revisión de contenidos de la tabla en el ambiente transitorio.
- Confirmar el deseo de recuperar o no la tabla.

c) Solicitud de recuperación de objetos de base de datos a una fecha

- La recuperación de objetos estáticos de la base de datos se hará mediante la corrida de los scripts del directorio /arbor/site_specific/dba/sybase/catalog
  /arbor/site_specific/dba/sybase/customer
  /arbor/site_specific/dba/sybase/admin, dependiendo de la base de datos que aloje al objeto respectivo.

En diferentes directorios se pueden encontrar los objetos de cada base. La estructura de directorio es la que sigue :

Inits	:	Inicialización de tablas
keys	:	Indices
proc	:	Store procedures
sysmsgs	:	Mensajes de sistema

trig : Trigger
view : Vistas
defaults : Defaults
perm : Permisos
rule : Reglas
tables : Tablas
users : Usuarios

Recuperación de objetos estáticos

Pasos

1. Ubiquese en el directorio correcto, de acuerdo a la base de datos y objeto que desee recrear.
2. Ejecute el script del objeto indicando base de datos, usuario y password respectivo.

Recuperación de base de datos completa

Pasos

1. Conseguir la aceptación de la restauración de datos de la fecha que se planea restaurar.
2. Elegir el momento adecuado en coordinación con el usuario.
3. Proceder a extraer un backup de la situación anterior a la restauración
4. Notificar usuarios con al menos diez minutos de antelación.
5. Verificar usuarios ejecutando en isql sp_who.
6. Notificar usuarios con tres minutos de antelación nuevamante.
7. Al cabo de los tres minutos proceder a matar transacciones de dicha base de datos, con el comando kill.
8. Ubicar la cinta en el dispositivo respectivo.
9. Poner la base de datos en modo monousuario.
    - Ingresar al server manager con usuario sa
    - Elegir la base de datos respectiva
    - Hacer click derecho y elegir options.
    - Verifique el check box, en la opción single_user_mode, de no estar proceda a elegirlo.
    - Elija la base de datos nuevamente, click derecho y opción checkpoint.
10. Presionar click derecho en la base de datos y elegir restore
11. Elija el modo database y el dump device respectivo donde se encuentra el backup a restaurar.
12. Proceda con la restauración.
13. Proceda a verificar la restauración.
14. De no estar ok proceda a restaurar el backup extraído.

Recuperación de objetos

Pasos

1. Ubicar la cinta en el dispositivo respectivo.
2. Poner la base de datos intermedia en modo monousuario.
    - Ingresar al server manager con usuario sa
    - Elegir la base de datos respectiva

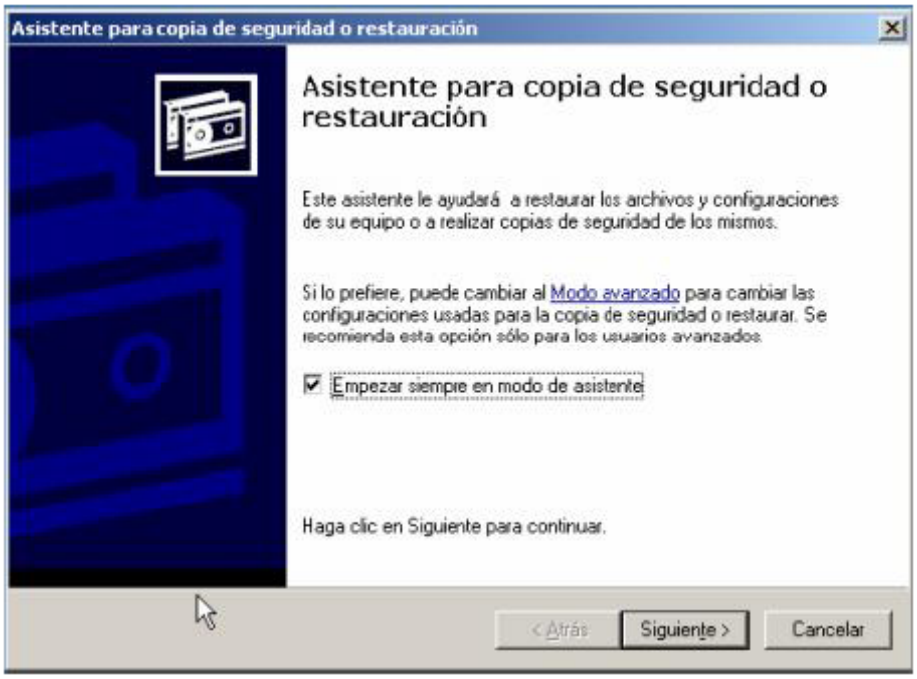
- Hacer click derecho y elegir options.
- Verifique el check box, en la opción single_user_mode, de no estar proceda a elegirlo.
- Elija la base de datos nuevamente, click derecho y opción checkpoint.

3. Presionar click derecho en la base de datos y elegir restore
4. Elija el modo database y el dump device respectivo donde se encuentra el backup a restaurar.
5. Proceda con la restauración.
6. Proceda a verificar la restauración. De estar mala corrija lo necesario y vuelva a intentarlo.
7. Consulte el objeto deseado y verifique que este correcto.
8. De estarlo conectese a la base que desea actualizar.
9. Digite delete from <tabla>
10. Digite insert into <tabla> select * from <base de datos intermedia>..<tabla>

- **Procedimiento para realizar backups en los servidores Windows 2003**

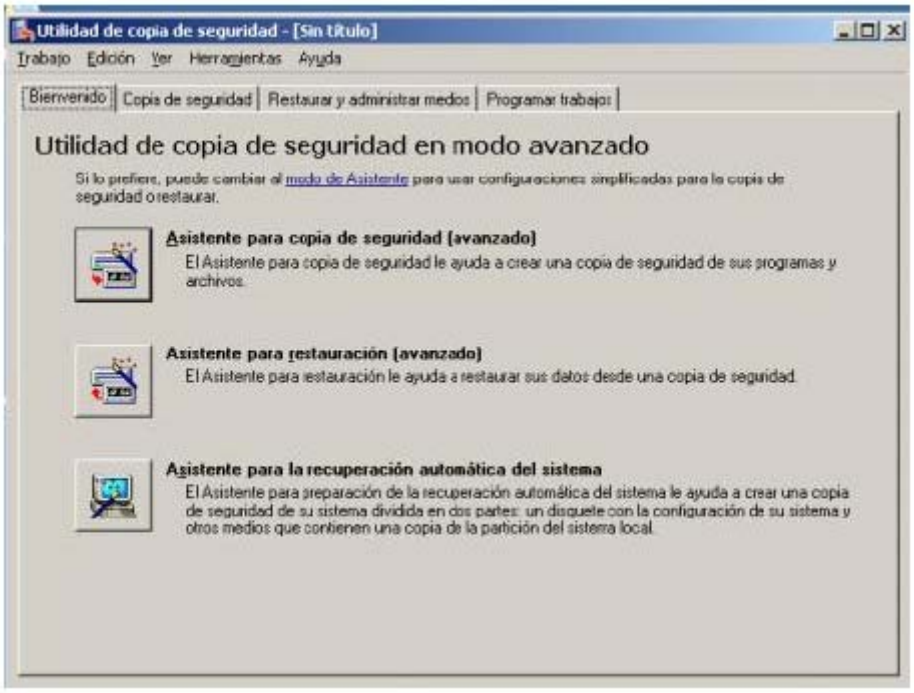
En Windows 2003 existe una herramienta para realizar respaldos, el cual puede ser accedido mediante su nombre ejecutable Ntbackup. Para poder facilitar recobrar la información en caso de algún daño en los servidores de Windows, vamos a utilizar esta herramienta para realizar respaldos de los mismos. A continuación se detallan los pasos para la configuración:

La primera vez que se corre esta utilidad mostrará la siguiente pantalla:



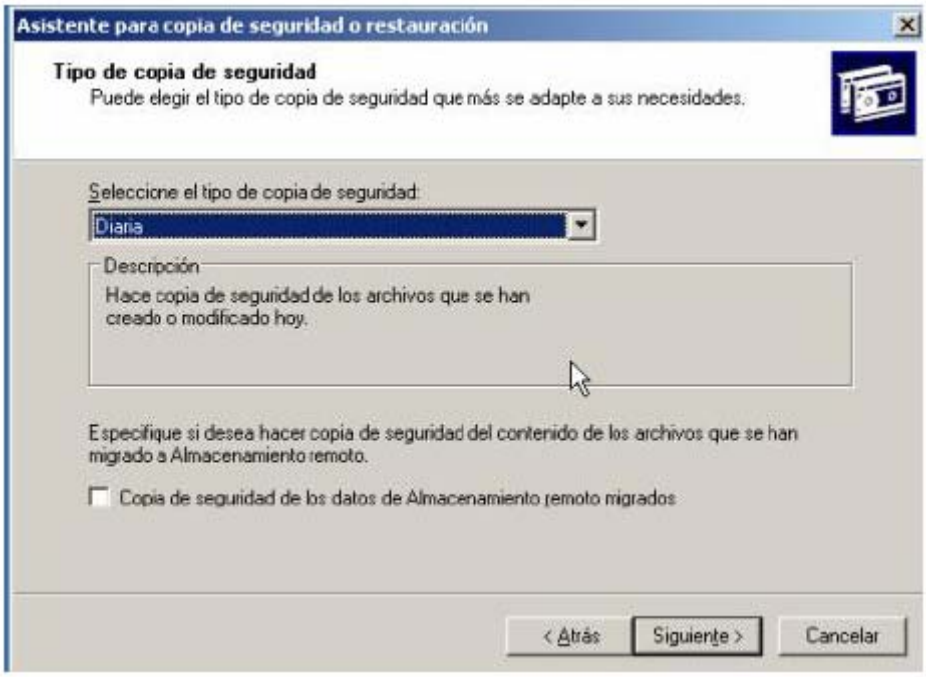
Respaldo o restauración

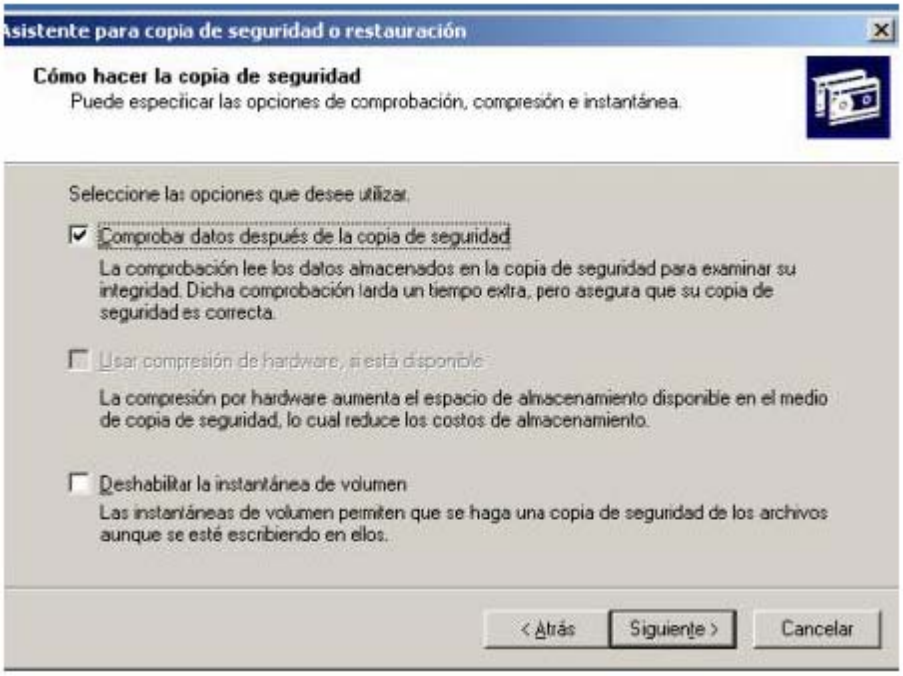
Esta herramienta se la puede utilizar tanto para sacar respaldos como para restaurar la Información.



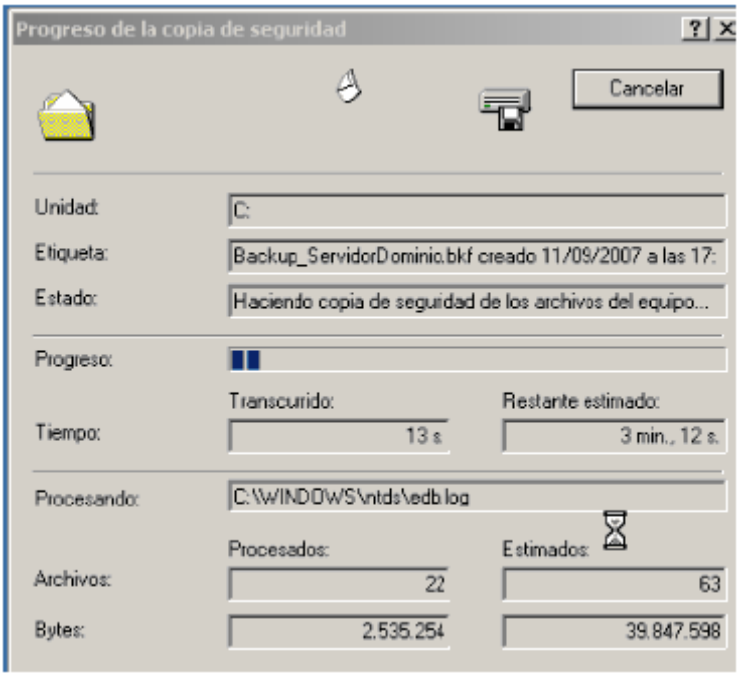
Para optimizar espacio en el disco duro de respaldo no se ha escogido la opción de respaldar toda la información de lo servidores, se respaldará únicamente la unidad donde se encuentre la información crítica del servidor de dominio y el de correo.

Windows 2003 permite sacar respaldo en cualquier tipo de dispositivos, para este caso se utilizará un disco duro de 500 GB para guardar las copias de backups, estos archivos se guardarán con extensión .bkf. Además se han considerado las siguientes opciones adicionales que ayudan a garantizar una apropiada copia de seguridad:

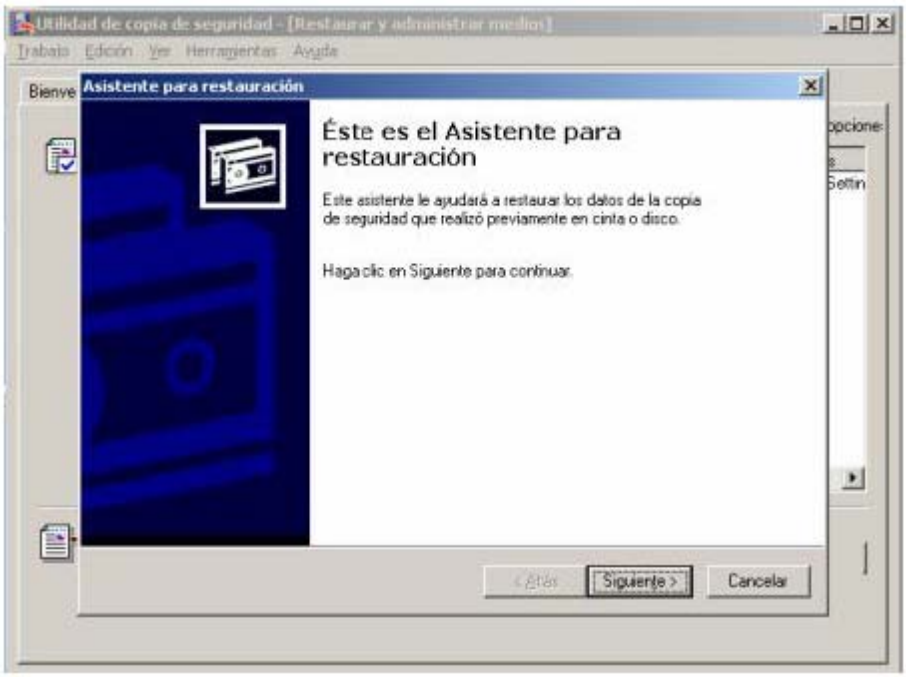

Asistente para copia de seguridad o restauración
Tipo de copia de seguridad
Puede elegir el tipo de copia de seguridad que más se adapte a sus necesidades.
Seleccione el tipo de copia de seguridad:
Diana
Descripción
Hace copia de seguridad de los archivos que se han creado o modificado hoy.
Especifique si desea hacer copia de seguridad del contenido de los archivos que se han migrado a Almacenamiento remoto.
Copia de seguridad de los datos de Almacenamiento remoto migrados
< Atrás
Siguiente >
Cancelar


Asistente para copia de seguridad o restauración
Cómo hacer la copia de seguridad
Puede especificar las opciones de comprobación, compresión e instantánea.
Seleccione las opciones que desee utilizar.
Comprobar datos después de la copia de seguridad
La comprobación lee los datos almacenados en la copia de seguridad para examinar su integridad. Dicha comprobación tarda un tiempo extra, pero asegura que su copia de seguridad es correcta.
Usar compresión de hardware, si está disponible
La compresión por hardware aumenta el espacio de almacenamiento disponible en el medio de copia de seguridad, lo cual reduce los costos de almacenamiento.
Deshabilitar la instantánea de volumen
Las instantáneas de volumen permiten que se haga una copia de seguridad de los archivos aunque se esté escribiendo en ellos.
< Atrás
Siguiente >
Cancelar

El proceso de obtener el respaldo se muestra de la siguiente manera:

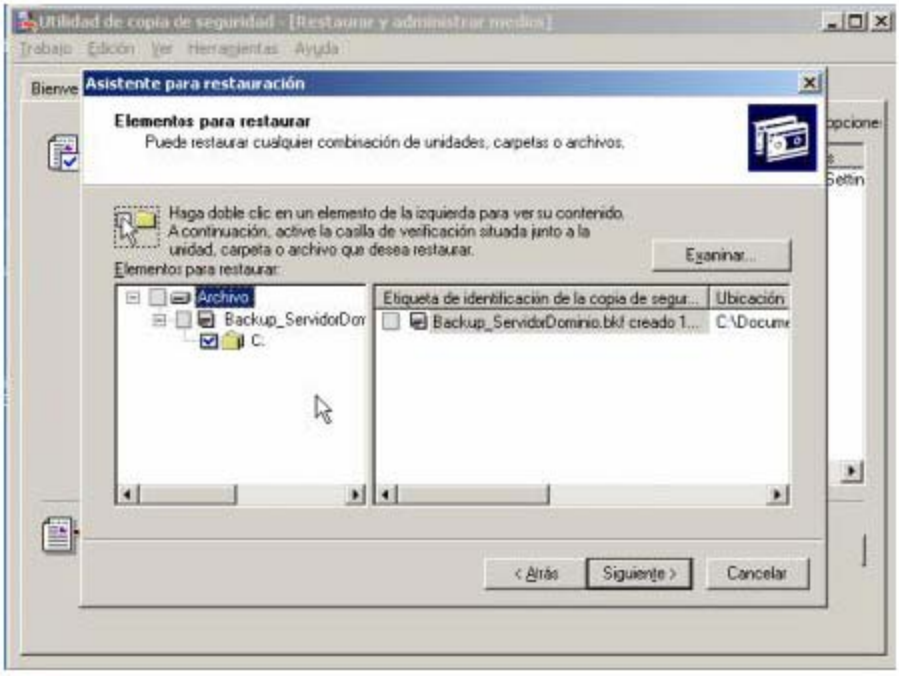


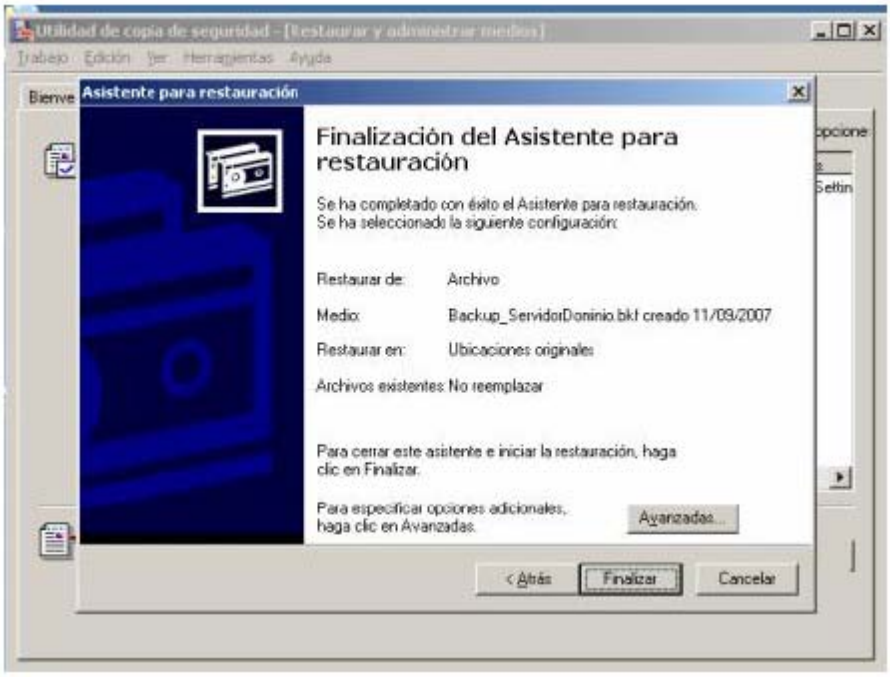
Para restaurar la información se utiliza el asistente de restauración, el cual puede ser accedido mediante el ejecutable Ntbackup.exe, y escoger la opción restaurar información

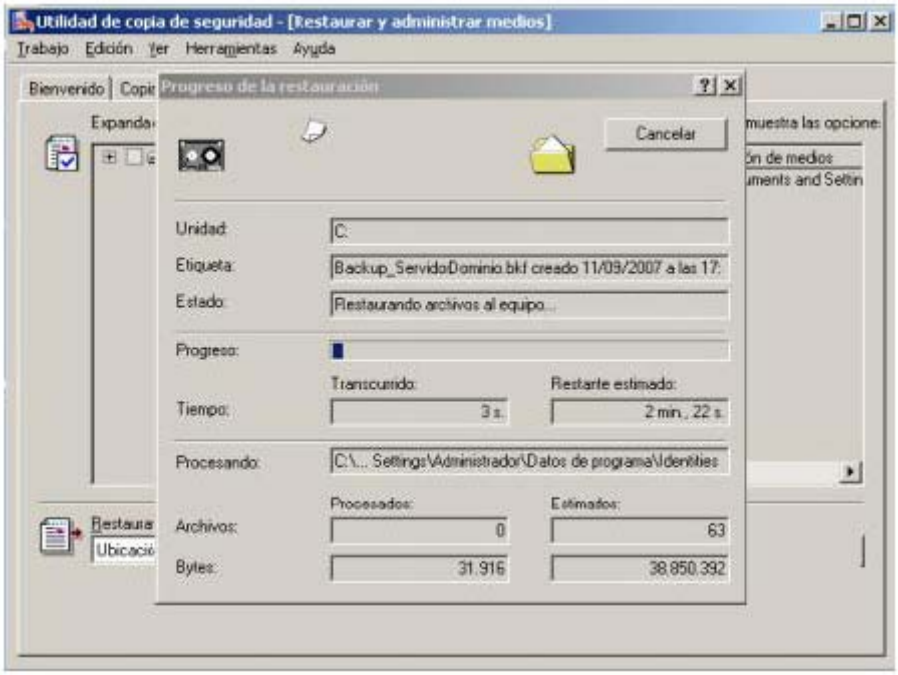


A continuación se escoge la información a ser restaurada, poniendo un visto en esta información, en este caso serán restauradas en las ubicaciones originales.

Finalmente esta pantalla indicará que la operación se ha finalizado con éxito.







Este procedimiento de respaldo es necesario configurarlo la primera vez, luego de lo cual el respaldo se irá almacenando diariamente en el disco de backups, el mismo que tiene que ser

verificado semanalmente por el administrador de red, para comprobar el funcionamiento adecuado del disco y de la programación de respaldo.

Procedimiento de Importar Base de Datos

1. Subir la base de datos de la siguiente manera:

Crear los usuarios: cms, auditoria, consulta

Ejecutar el comando: imp system file="Nombre del archivo .dmp" full=y

log=imp.log commit=y ignore=y

Revisar el archivo del log de importación

Compilar procedimientos almacenados y triggers de ser necesario

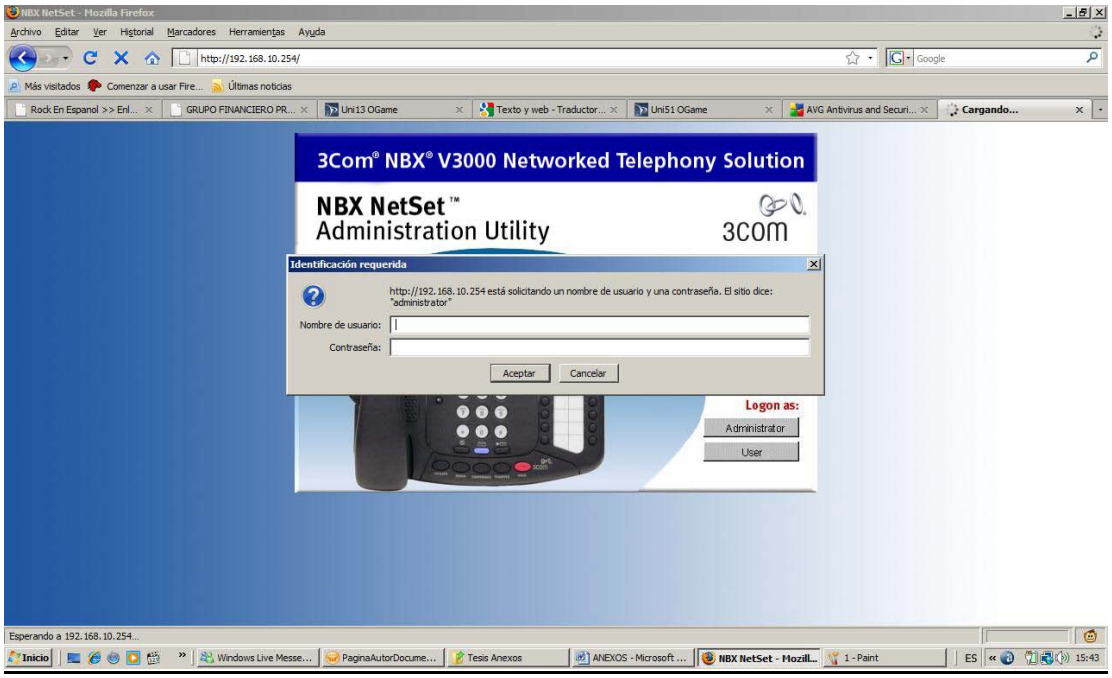
2. Recuperar los programas ejecutables en los directorios correspondientes

- **Procedimiento para realizar backups en los equipos de comunicación**

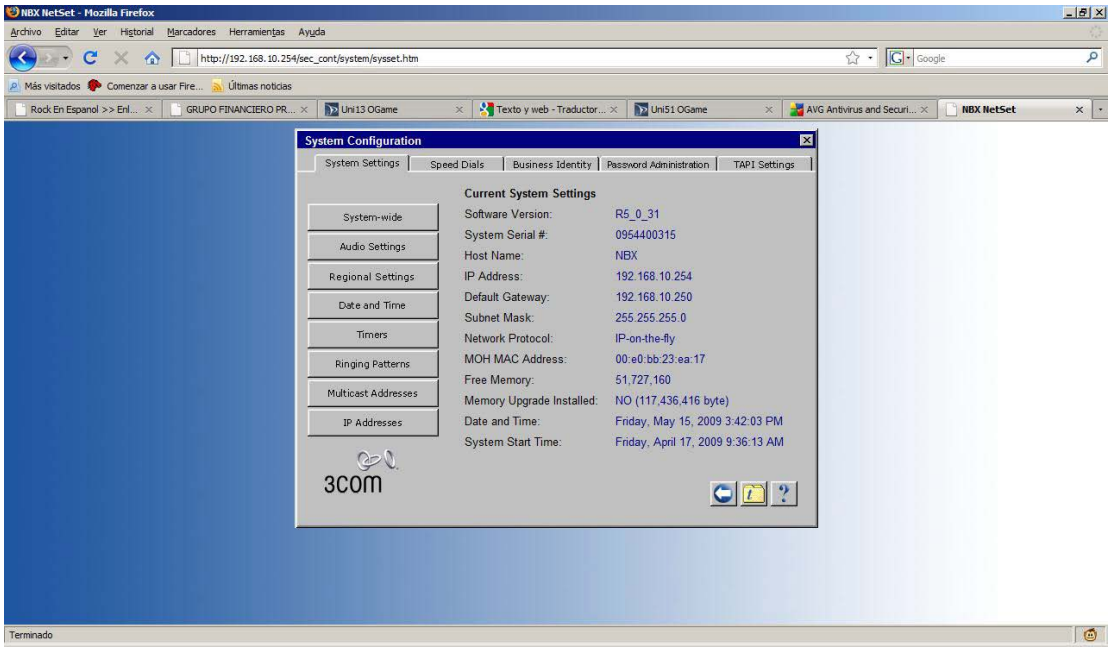
BackUp NBX

Tanto el manejo del equipo como la realización de los respaldos es via browser.

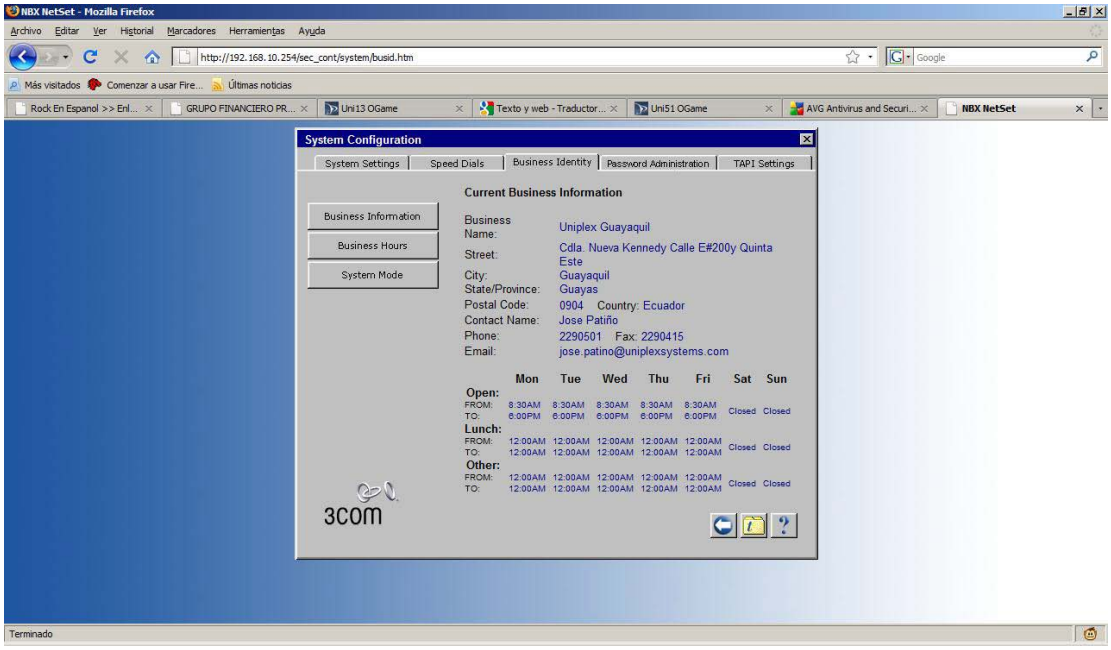
1. Lo primero es poner la dirección: 192.168.10.254
2. Poner la clave Administrator



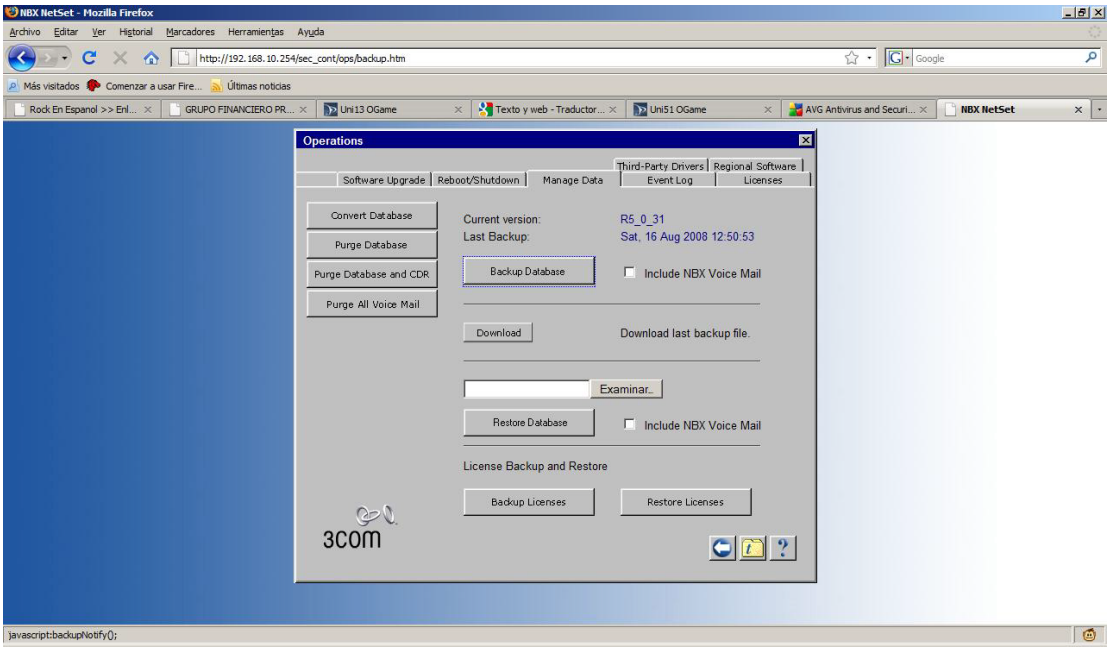
3. Luego dar click en la opción Systems Settings la cual proporciona una general descripción del equipo.

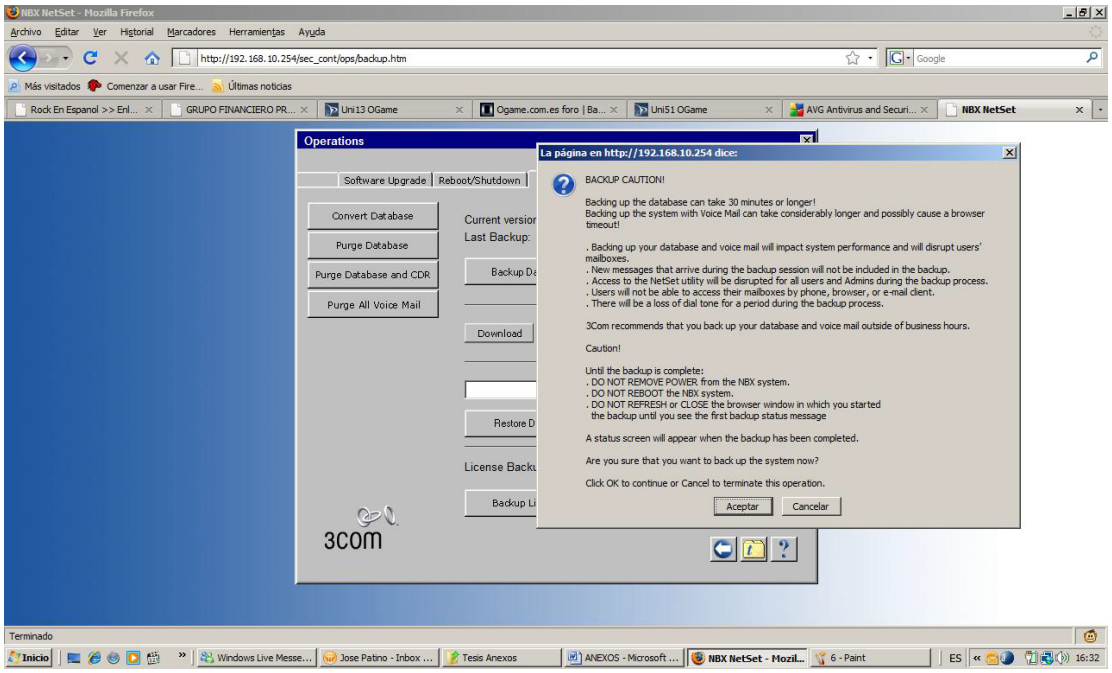


4. Luego dar click en la opción Business Identify la cual tiene la configuración de la zona horaria y la dirección del administrador en caso de falla

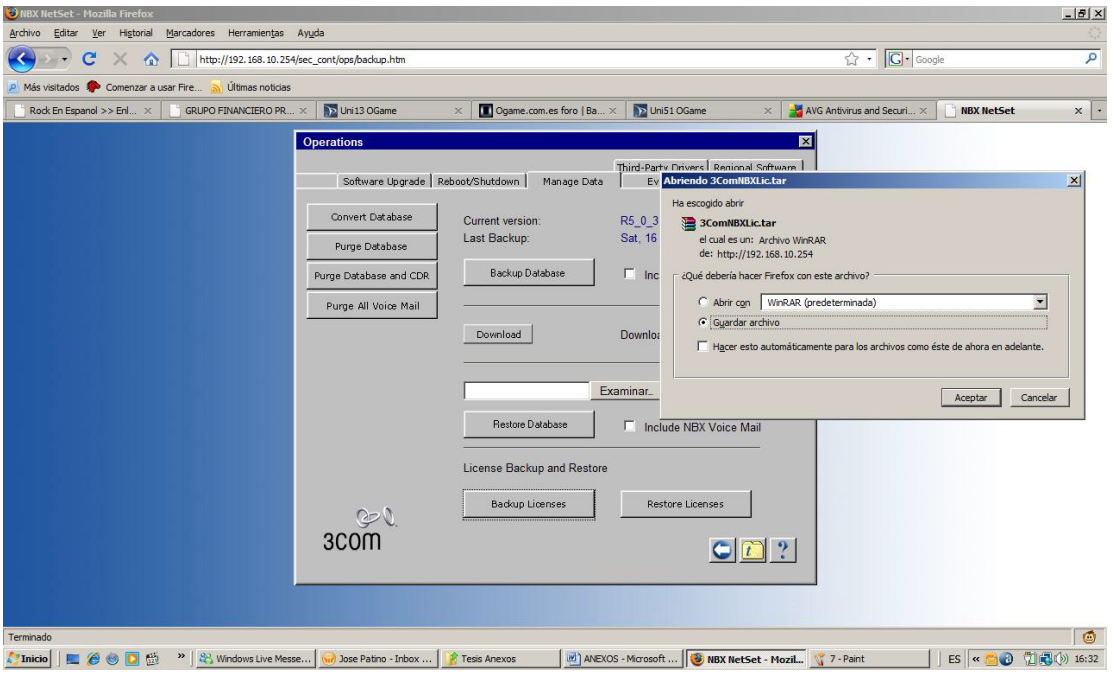


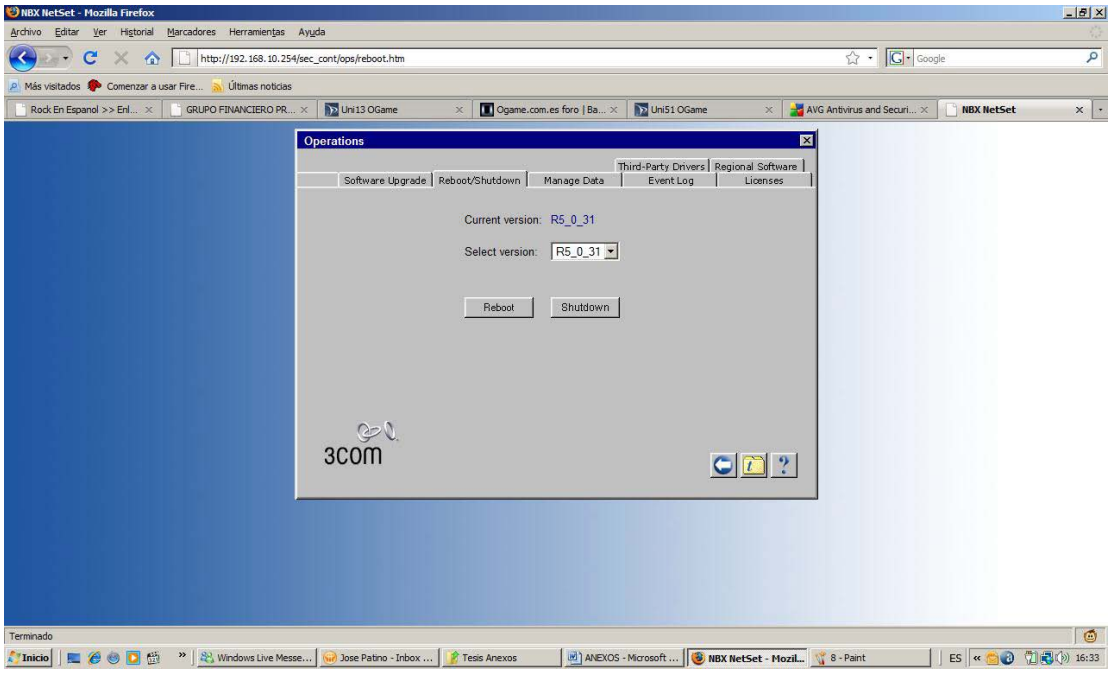
5. Luego dar click en la Operations en la opción manage data escogiendo la opción BackUp Database, el cual nos abrirá una ventana la que se debe escoger aceptar.



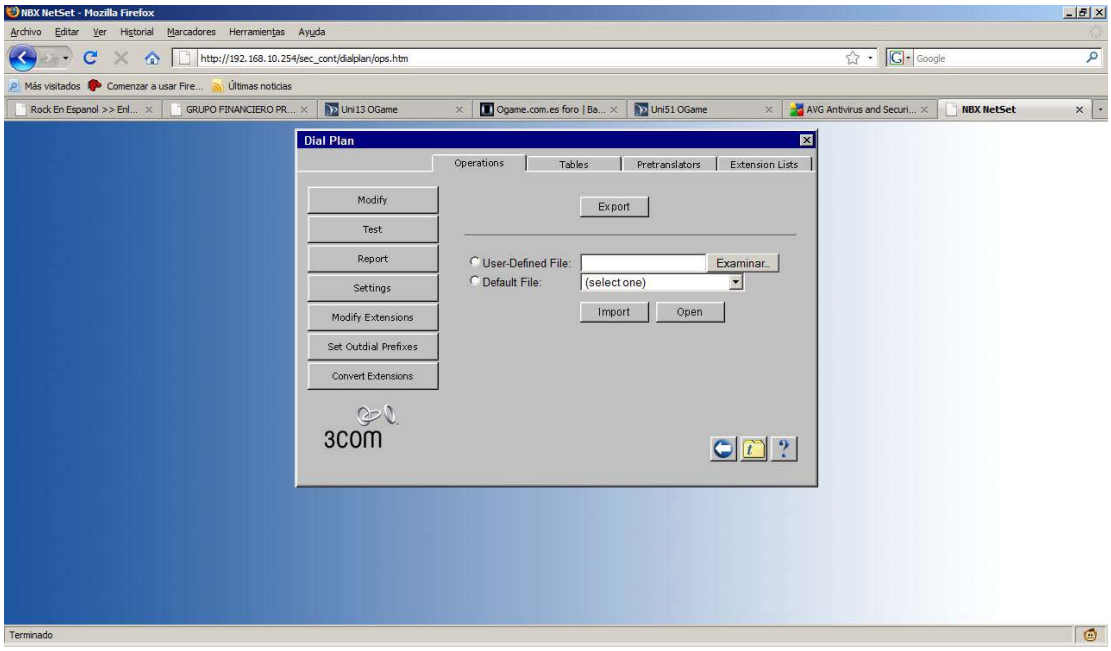


6. Luego dar click en la Operations en la opción manage data escogiendo la opción BackUp License, el cual nos abrirá una ventana la que se debe escoger donde uno quiere guardar los datos (localidad).

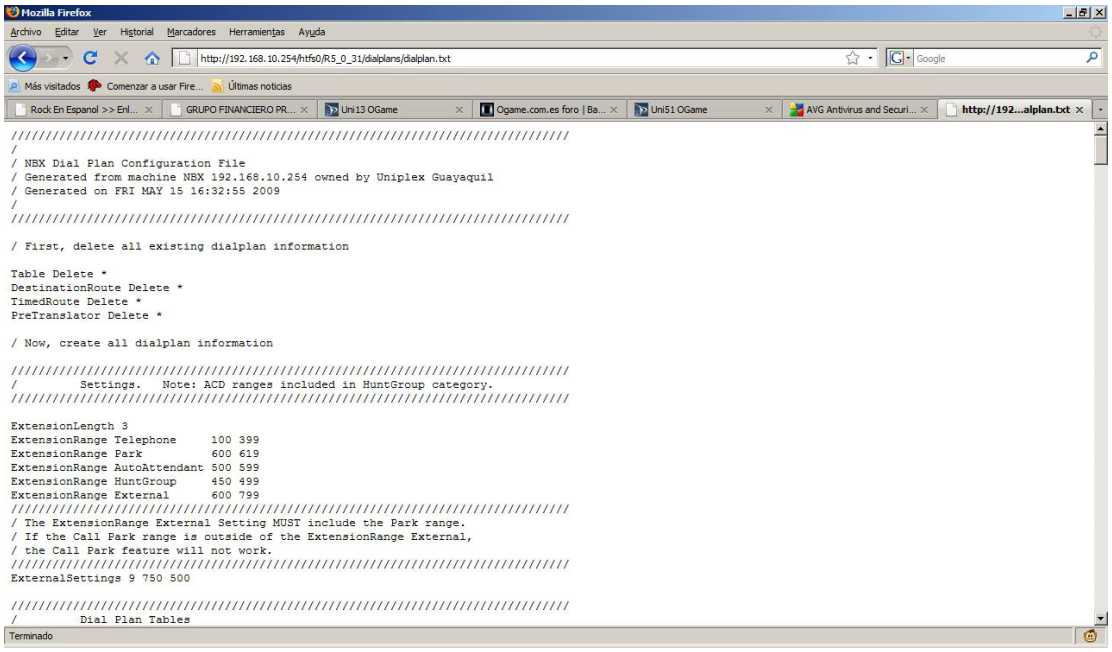




7. Luego de respaldar se procede a reiniciar el equipo, bajo ningún concepto se debe apagar el equipo mientras esta respaldando la información, eso ocasionaría una corrupción grave en el sistema (muchas de las veces irreparable).



8. Se respalda el Dial Plan el cual maneja todo el enrutamiento de usuarios y líneas externas además de configuraciones adicionales, se debe escoger export, lo cual nos abre en archivo web este plan de marcado, y se guardara como pagina web.



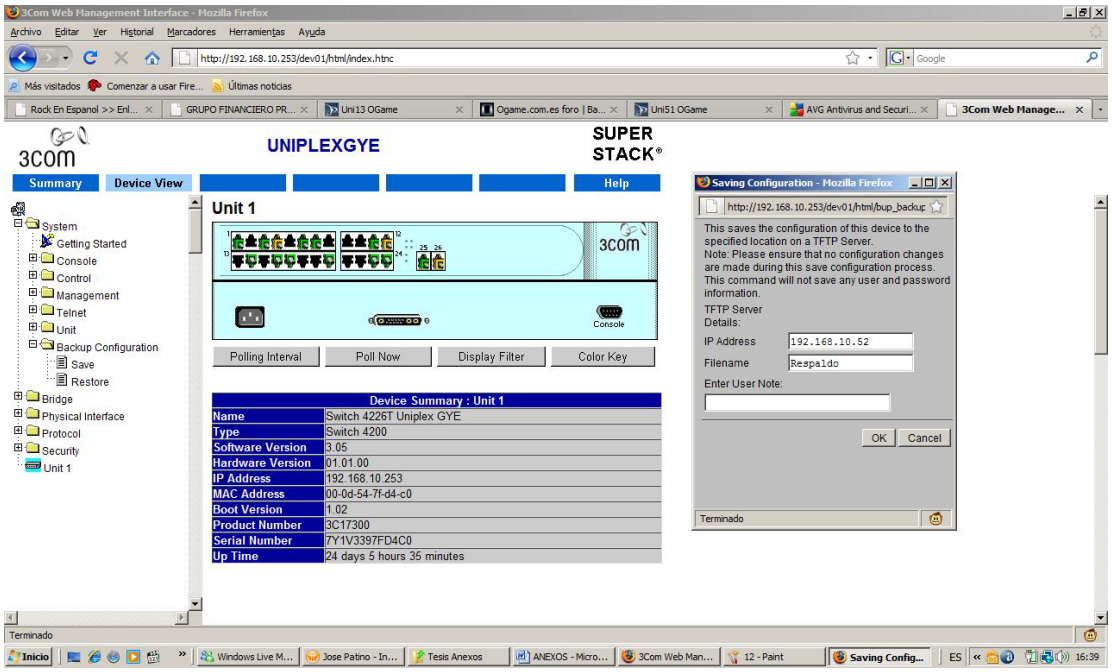
9. Por último para restaurar las configuraciones hay que escoger en cada una de las opciones de Backup la opción que se encuentra junto a ella la cual es Restore, para el dial plan la opción que está debajo de export o sea import.

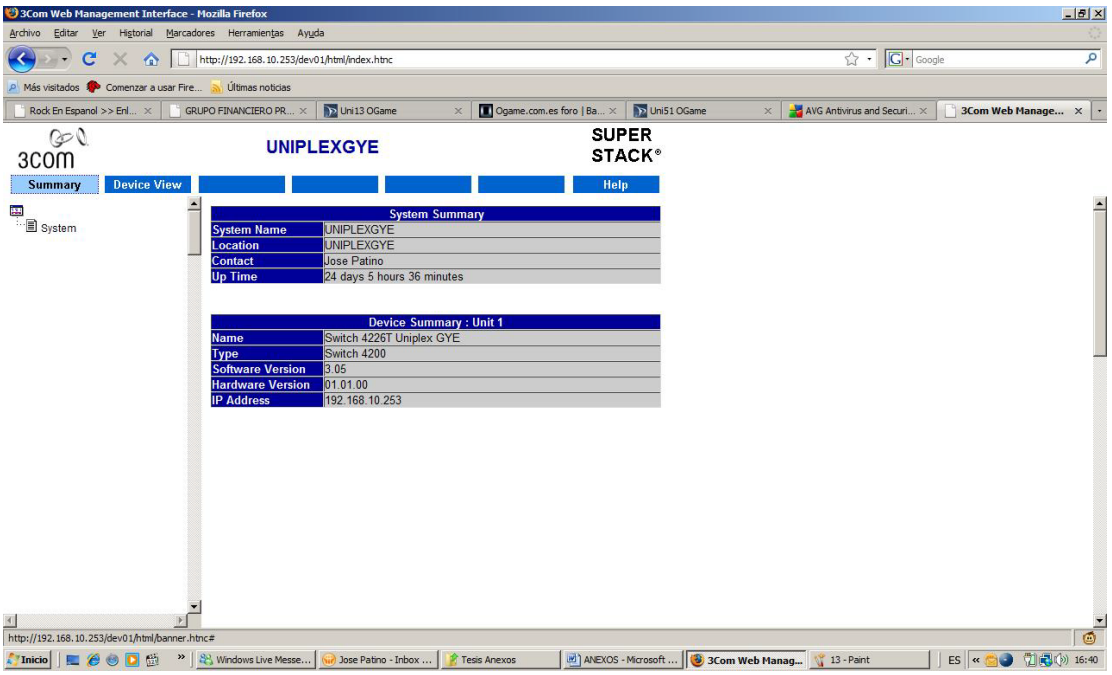
BackUp Switch 3Com

Tanto el manejo del equipo como la realización de los respaldos es via browser.

10. Para el backup del Switch 3Com es mas facil primero se debe ingresar via web a la dirección 192.168.10.253

11. Luego ingresar el user y password
12. Una vez ingresado al equipo nos dirigimos a la parte izquierda, seleccionamos la opción save para realizar el BackUP





13. Para restaurar la configuración se dirige a la misma localidad pero se escoge Restore, bajo ningún concepto apagar el equipo durante el respaldo o restauración ya que eso ocasionaría la corrupción del mismo.

- **Uso de portátiles ante una contingencia**

En caso de suscitarse alguna contingencia que amerite el traslado de la oficina administrativa a un sitio distante, todos los equipos portátiles serán entregados al departamento de sistemas para habilitar una red inalámbrica que servirá temporalmente para brindar atención telefónica a todos los prestadores. Al implementar una red inalámbrica es necesario considerar controles de seguridad debido a que el tráfico que viaja por la red es sensitivo. Para reducir los efectos de fallas en la red es aconsejable que se utilice un software de monitoreo de la red, pues con ello se detectan fallas en los equipos y permiten responder de forma rápida ante una falla.

ANEXO C

ANTIVIRUS

Es necesario configurar de una forma adecuada un antivirus, para garantizar una barrera de seguridad en las estaciones de trabajo, así como en cada uno de los servidores de Uniplex, en base a esta necesidad a continuación se indicará el procedimiento para implementar una adecuada seguridad en base al antivirus que ha adquirido la empresa.

Mcfee Antivirus

Este antivirus se instala en una maquina con características de servidor (puede como no puede serlo lo importante es que maneje sistema operativo de servidor). Una vez instalado se genera un agente que se debe instalar en cada una de las maquinas de la empresa, estas a su vez se autentican al servidor y mandan toda la información ahí (repositorio).

En Uniplex la instalación del AV será administrada por el encargado de la red.
Con respecto a las computadoras que se conectan a la red de Uniplex y pueden recibir virus o algún riesgo de seguridad, estas pueden ser manejadas por el programa administrador Centro del Sistema Mcfee.

Se requiere que las computadoras remotas conectadas a Uniplex cumplan con algunos requerimientos de seguridad, como por ejemplo: en las computadoras remotas se debe ejecutar el Antivirus con las actualizaciones apropiadas antes de que sean conectadas a la red. Para lo cual el momento en el que se instale el aplicativo para que los usuarios accedan

desde el exterior se debe verificar el cumplimiento con la seguridad mínima y realizar una revisión trimestral del mismo.

Riesgos de seguridad

El Antivirus de Mcfee puede detectar, poner en cuarentena, borrar y remover o reparar los efectos de los riesgos de seguridad en las siguientes categorías:

- Spyware: son programas que pueden secretamente monitorizar la actividad del sistema y detectar información como password y otra información confidencial.
  Spyware pueden ser transmitidos de Sitios Web (típicamente en SW de libre distribución), mensajes de email.

- Adware: Estos programas pueden secretamente reunir información personal través del Internet y puede transmitir información de una computadora a otra.
  Adware puede rastrear los hábitos del navegador para determinar los propósitos y de esta manera enviar publicidad de acuerdo a los propósitos determinados. Adware puede trasmitirse de manera similar al caso anterior.

- Dialers: Programas que usa una computadora, sin permiso, marca a fuera a través de Internet a 900 números, típicamente aumenta la carga.

- Hack tools: programas que son usados por un hacker para ganar acceso no autorizado.

- Otros: Los riesgos de seguridad que no conforman ninguna otra categorías de riesgos, pero pueden representar un riesgo de seguridad a su computador y a sus datos.

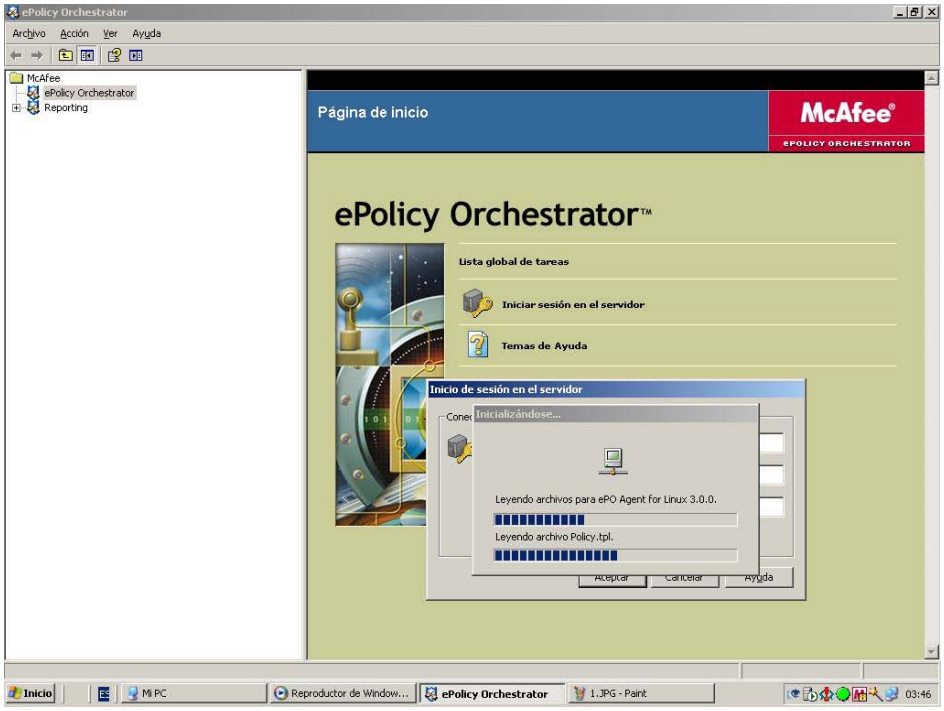
- Acceso Remoto: Programas que permiten el acceso a través de Internet de otra computadora para acceder ala información o atacar o alterar su computador.

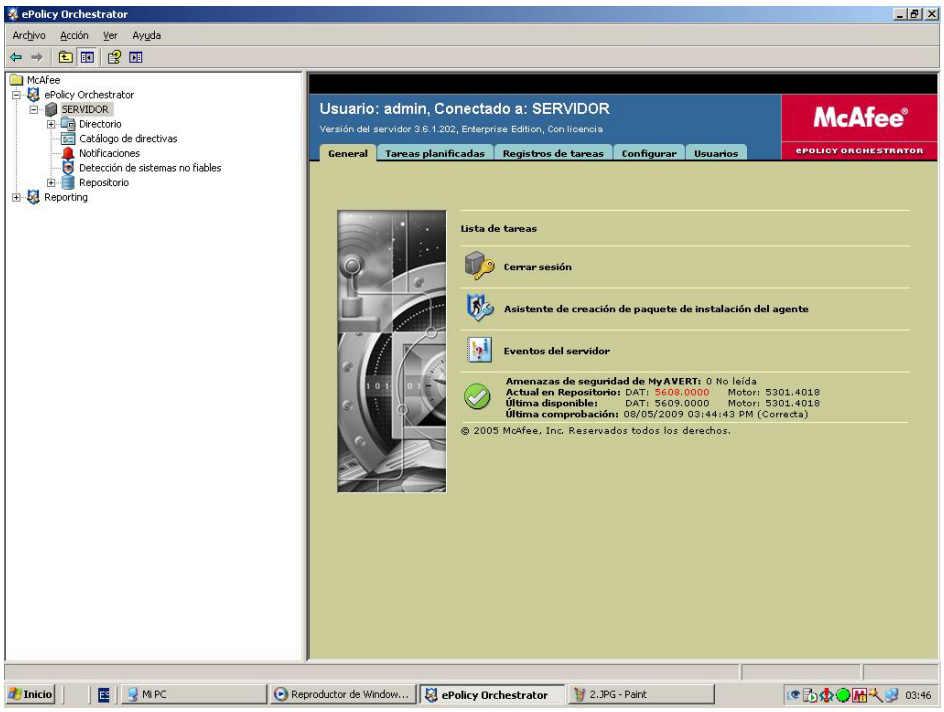
Protección de virus y riesgos de seguridad

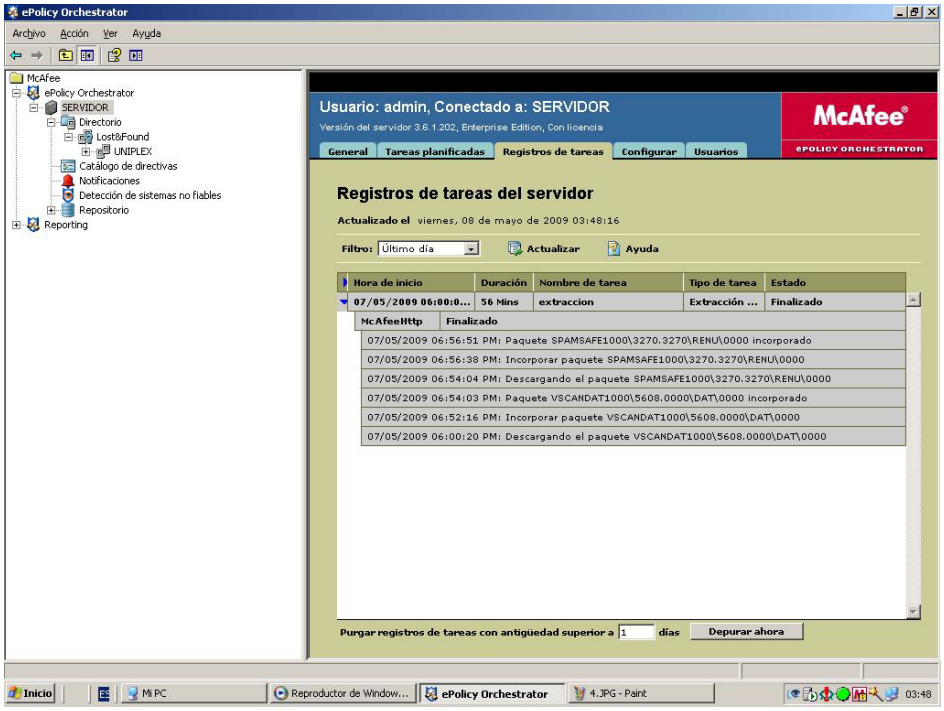
Si un virus o riesgo de seguridad es detectado responde con una primera acción, que es cuando el SW detecta un virus intenta limpiar el virus del archivo infectado. La segunda acción es cuando Mcfee Antivirus no puede limpiar el archivo, registra la falla de intento de limpiar el virus y mueve el archivo infectado a Cuarentena, para que el virus no pueda expandirse.

El antivirus centralizado provee una fácil configuración debido a que las políticas se establecen una sola vez y son replicadas a través de la red a todas las maquinas en las cuales se haya instalado el agente, teniendo un control total y además provee información acerca de cada una de las maquinas en cuestión.

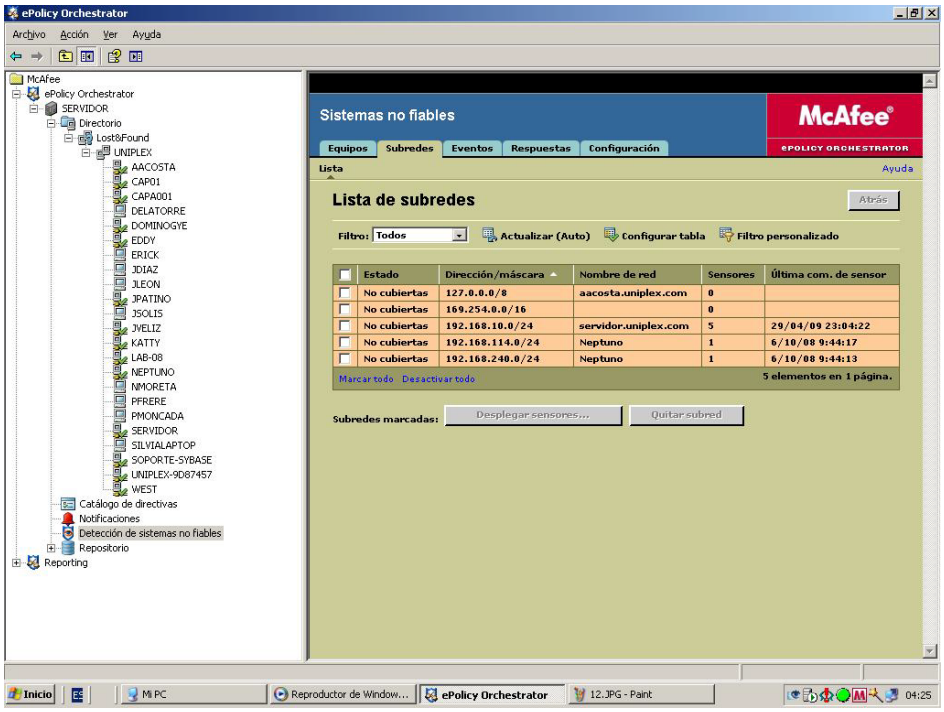
En base a las políticas de seguridad establecidas por Uniplex, el antivirus se configuró de la siguiente manera:

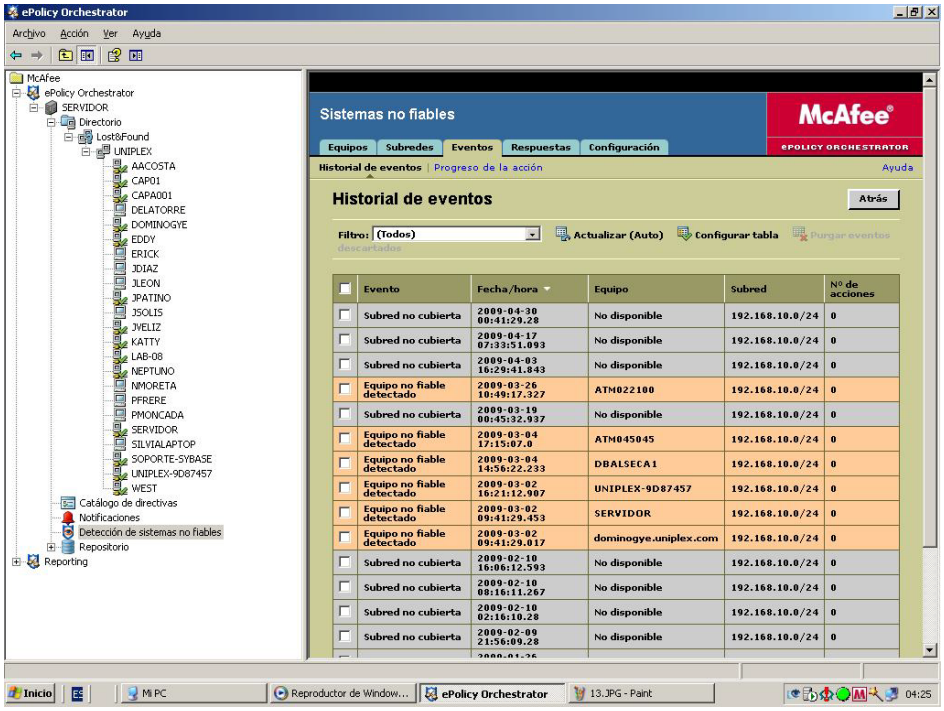

ePolicy Orchestrator
Archivo Acción Ver Ayuda
McAfee
ePolicy Orchestrator
Reporting
Página de inicio
McAfee
ePOLICY ORCHESTRATOR
ePolicy Orchestrator™
Lista global de tareas
Iniciar sesión en el servidor
Temas de Ayuda
Inicio de sesión en el servidor
Inicializándose...
Leyendo archivos para ePO Agent for Linux 3.0.0.
Leyendo archivo Policy.tpl.
Aceptar
Cancelar
Ayuda
Inicio
Mi PC
Reproductor de Window...
ePolicy Orchestrator
1.JPG - Paint
03:46

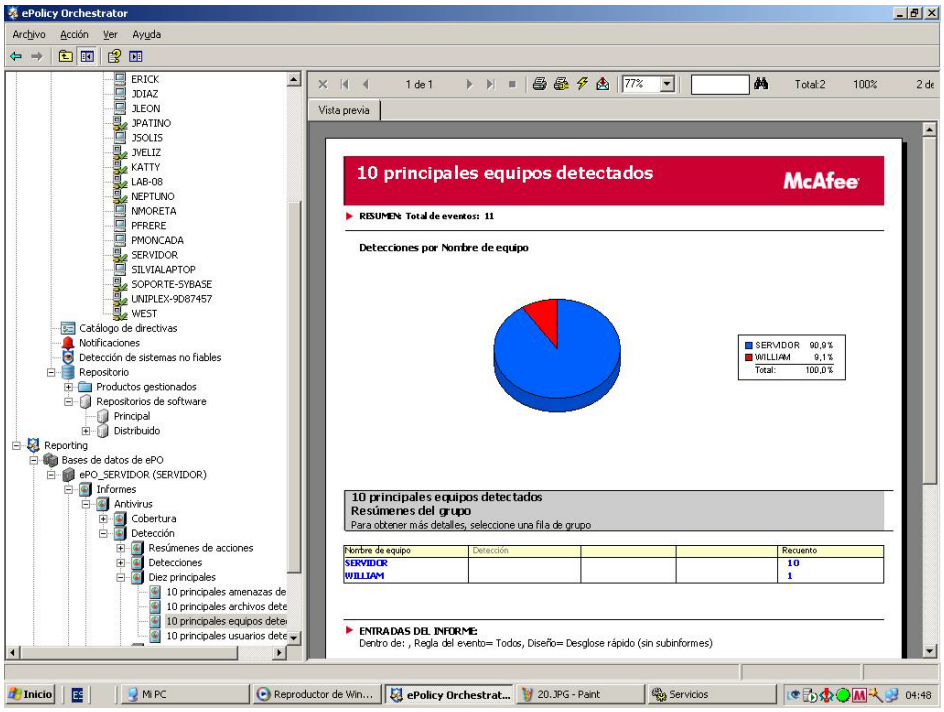

ePolicy Orchestrator
Archivo Acción Ver Ayuda
McAfee
ePolicy Orchestrator
SERVIDOR
Directorio
Catálogo de directivas
Notificaciones
Detección de sistemas no fiables
Repositorio
Reporting
Usuario: admin, Conectado a: SERVIDOR
Versión del servidor 3.6.1.202, Enterprise Edition, Con licencia
McAfee
ePOLICY ORCHESTRATOR
General
Tareas planificadas
Registros de tareas
Configurar
Usuarios
Lista de tareas
Cerrar sesión
Asistente de creación de paquete de instalación del agente
Eventos del servidor
Amenazas de seguridad de MyAVERT: 0 No leída
Actual en Repositorio: DAT: 5608.0000 Motor: 5301.4018
Última disponible: DAT: 5609.0000 Motor: 5301.4018
Última comprobación: 08/05/2009 03:44:43 PM (Correcta)
© 2005 McAfee, Inc. Reservados todos los derechos.
Inicio
Mi PC
Reproductor de Window...
ePolicy Orchestrator
2.JPG - Paint
03:46



Se configuro para tener una visión jerárquica tanto para las políticas como para los reportes:

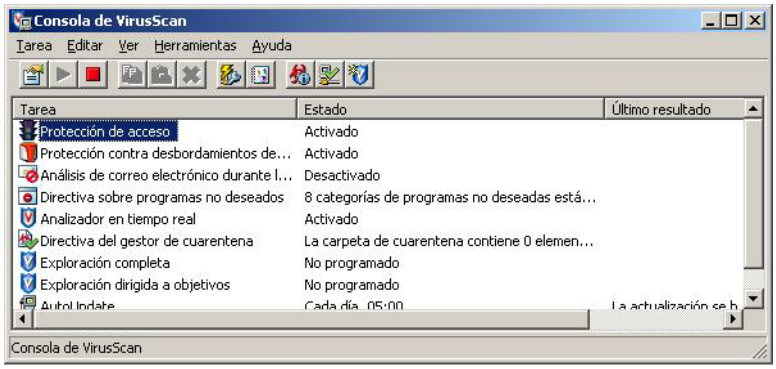


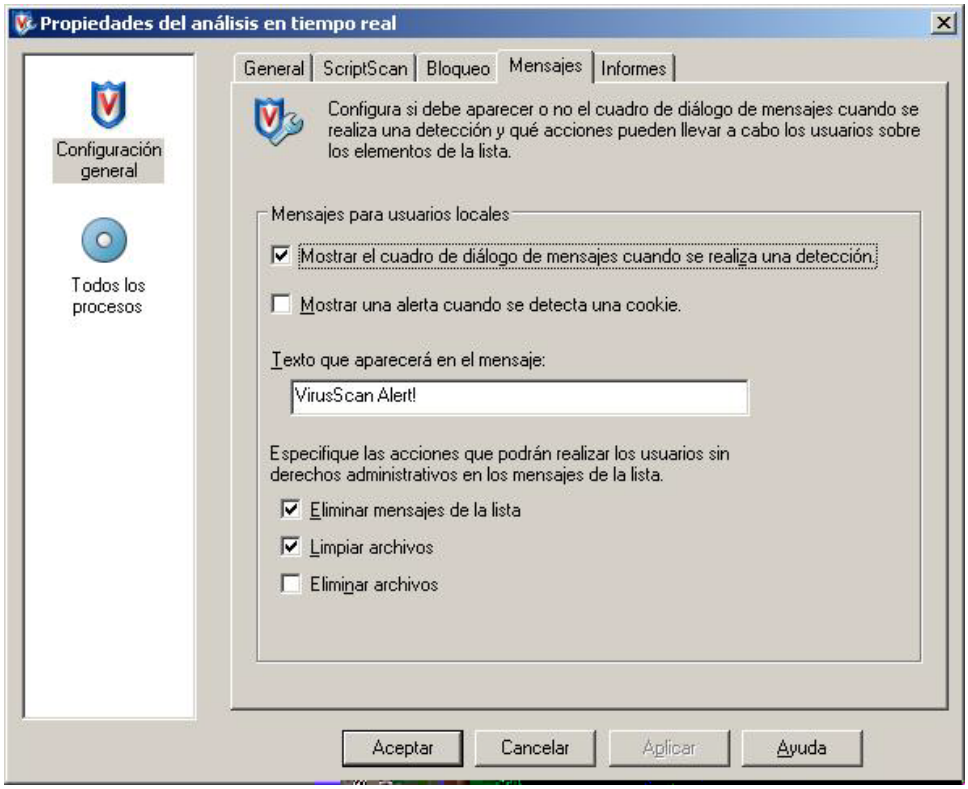




Se escogió Full Scan porque este se caracteriza por un escaneo total tanto de la memoria como del sistema en si, todos los comunes virus y riesgos de seguridad localizados en la

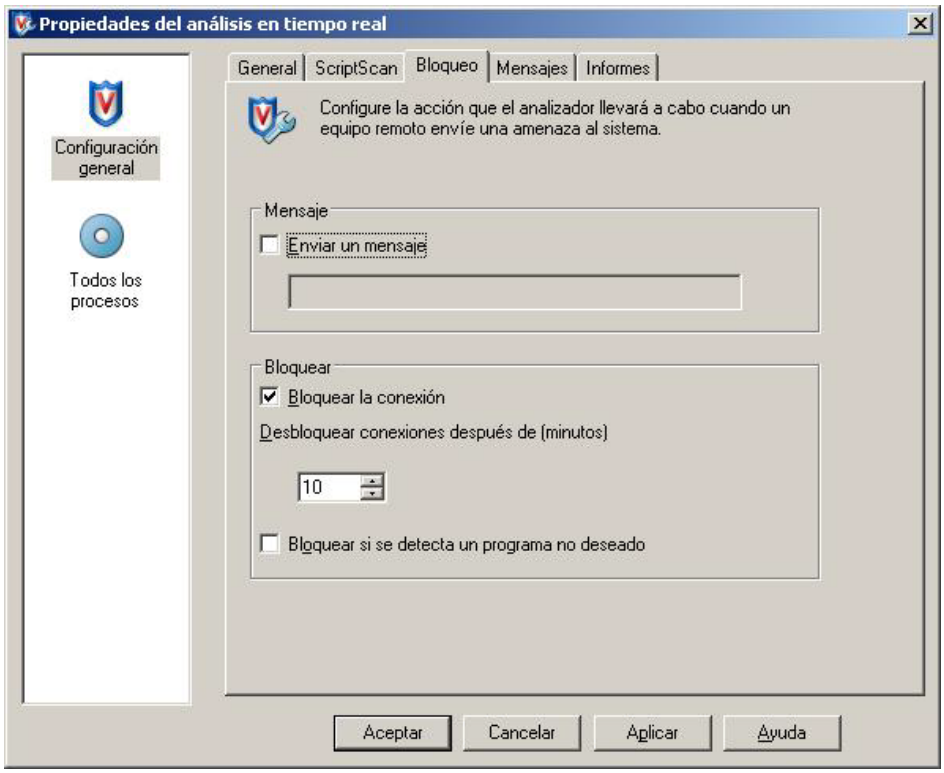
computadora, este se lo tiene calendarizado para realizarlo a la hora del almuerzo, debido a que la mayoría de PC´s se apagan al terminar la jornada laboral.

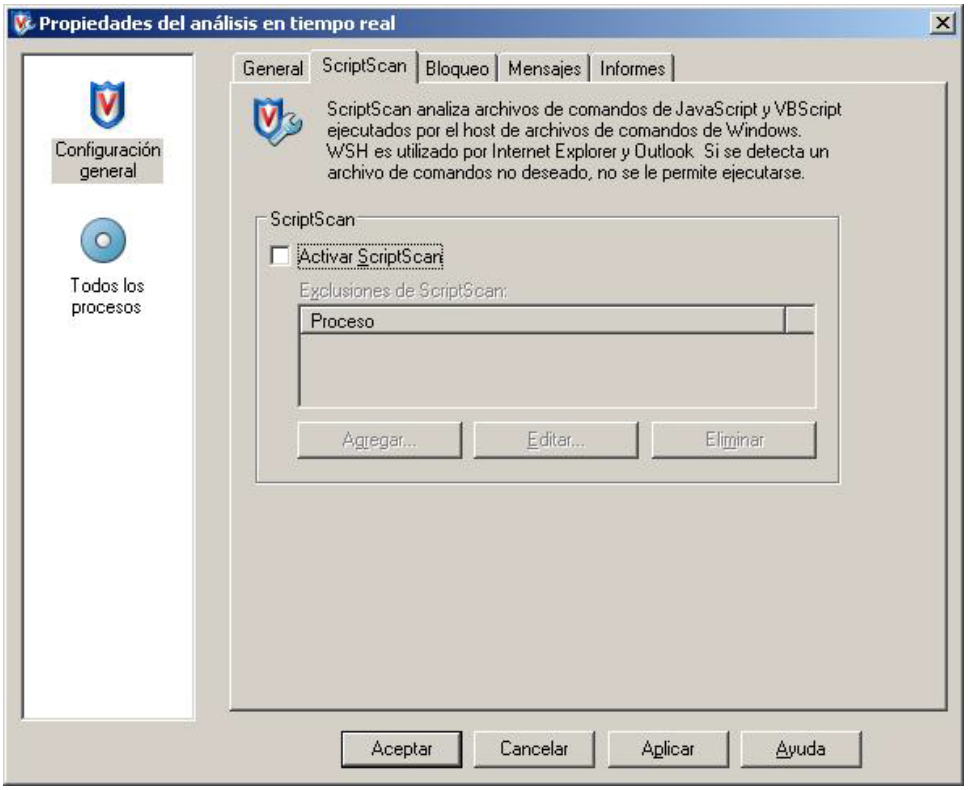


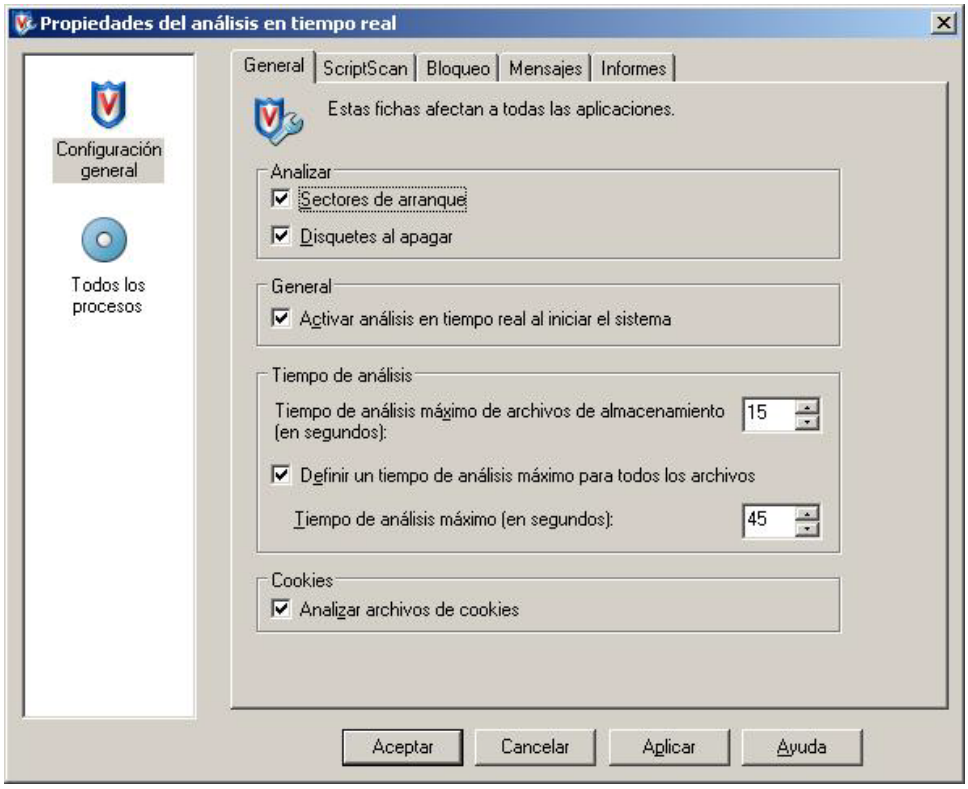


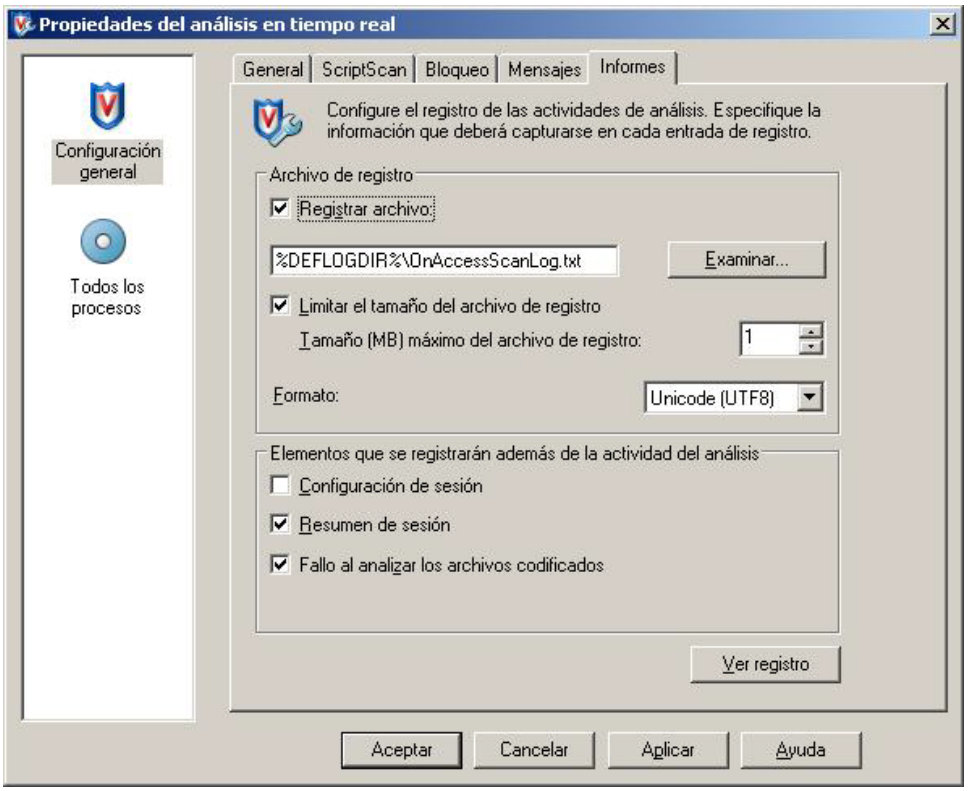
Diariamente se ejecutará el "scanning" para revisar y detectar software viral almacenado en la estación de trabajo a las 13:00, se escogió debido a que es la hora de descanso y no interfiere en las operaciones de los empleados.

Con las siguientes opciones de configuración:



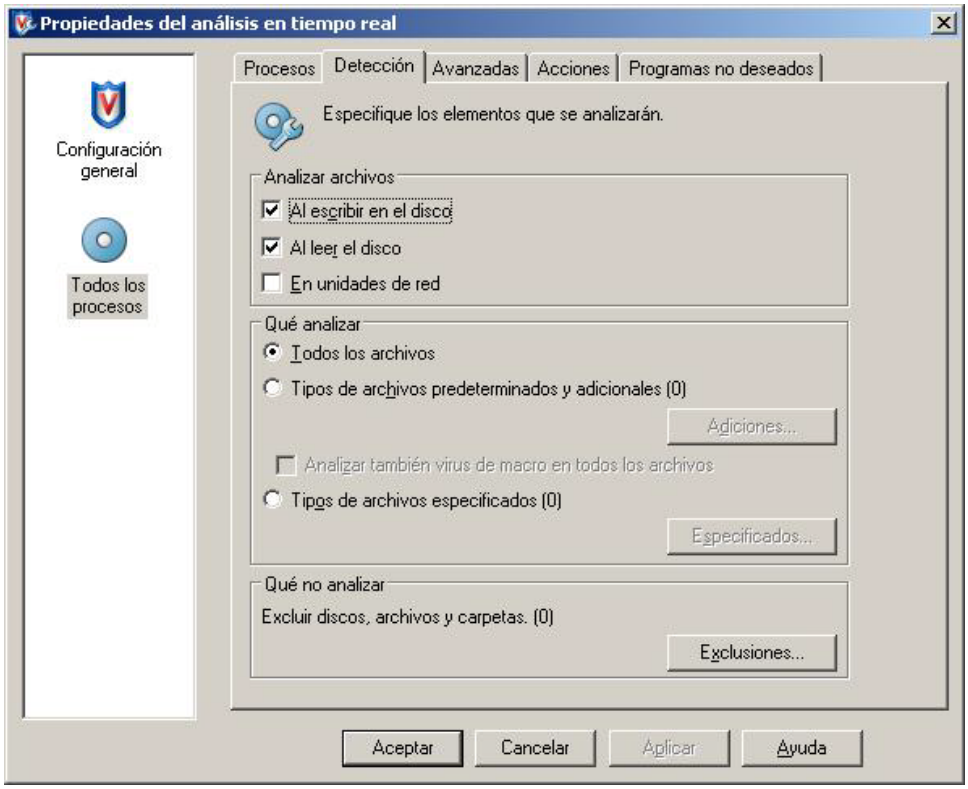


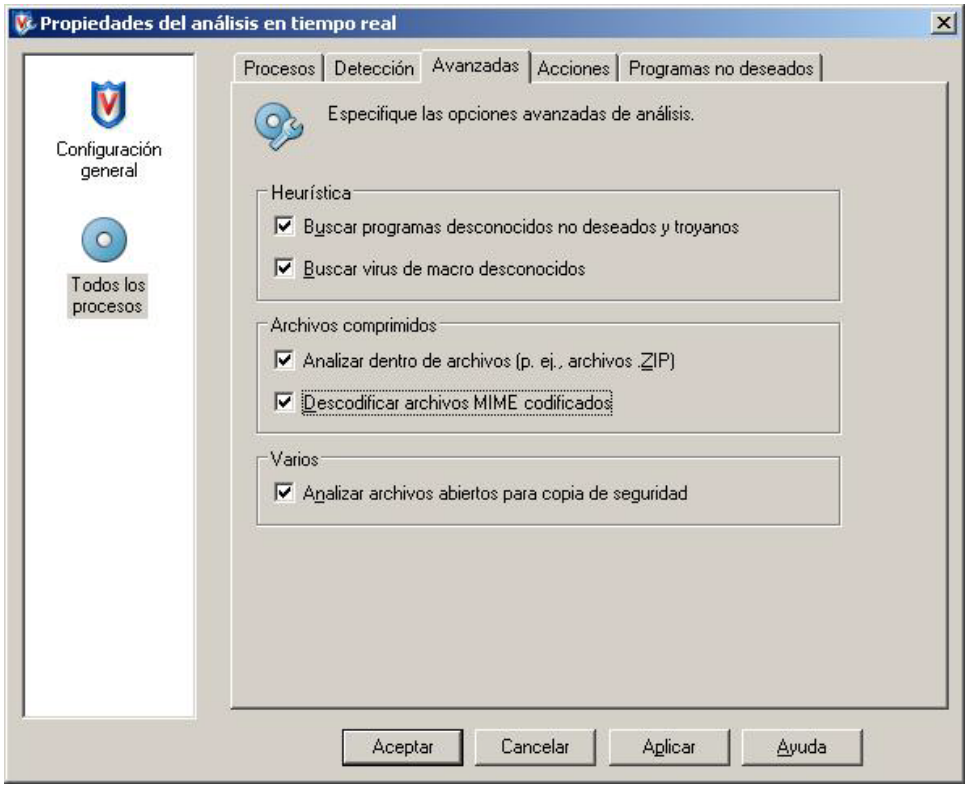

Propiedades del análisis en tiempo real
Configuración general
Todos los procesos
General
ScriptScan
Bloqueo
Mensajes
Informes
Estas fichas afectan a todas las aplicaciones.
Analizar
Sectores de arranque
Disquetes al apagar
General
Activar análisis en tiempo real al iniciar el sistema
Tiempo de análisis
Tiempo de análisis máximo de archivos de almacenamiento (en segundos):
15
Definir un tiempo de análisis máximo para todos los archivos
Tiempo de análisis máximo (en segundos):
45
Cookies
Analizar archivos de cookies
Aceptar
Cancelar
Aplicar
Ayuda

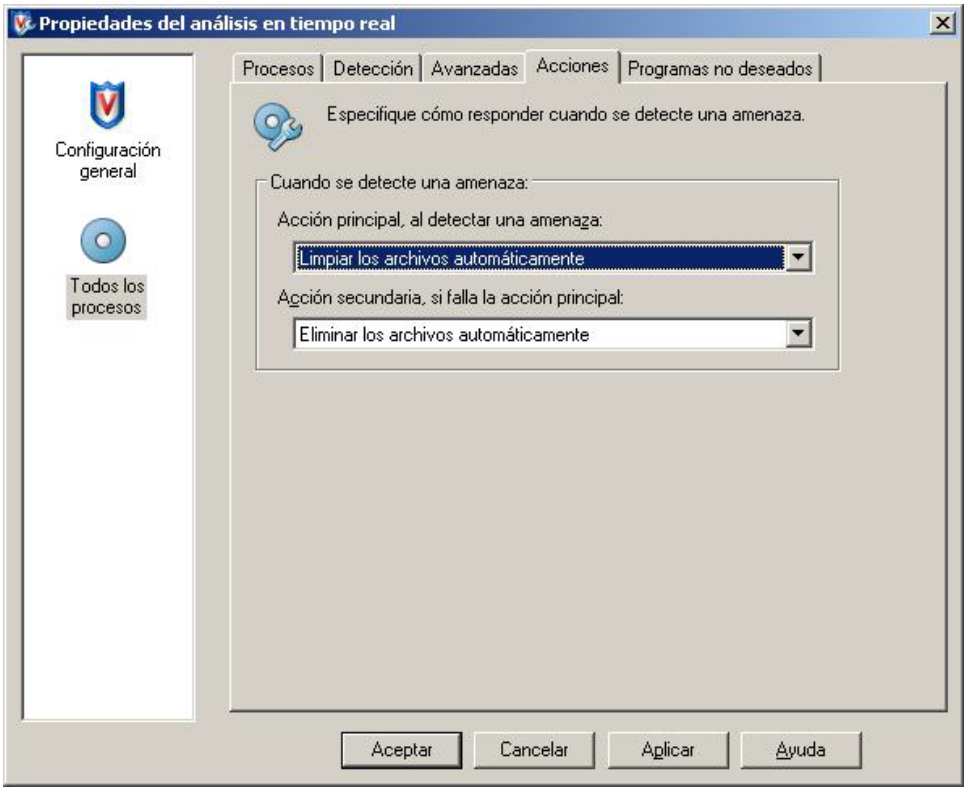

Propiedades del análisis en tiempo real
Configuración general
Todos los procesos
General
ScriptScan
Bloqueo
Mensajes
Informes
Configure el registro de las actividades de análisis. Especifique la información que deberá capturarse en cada entrada de registro.
Archivo de registro
Registrar archivo:
%DEFLOGDIR%\OnAccessScanLog.txt
Examinar...
Limitar el tamaño del archivo de registro
Tamaño (MB) máximo del archivo de registro:
1
Formato:
Unicode (UTF8)
Elementos que se registrarán además de la actividad del análisis
Configuración de sesión
Resumen de sesión
Fallo al analizar los archivos codificados
Ver registro
Aceptar
Cancelar
Aplicar
Ayuda

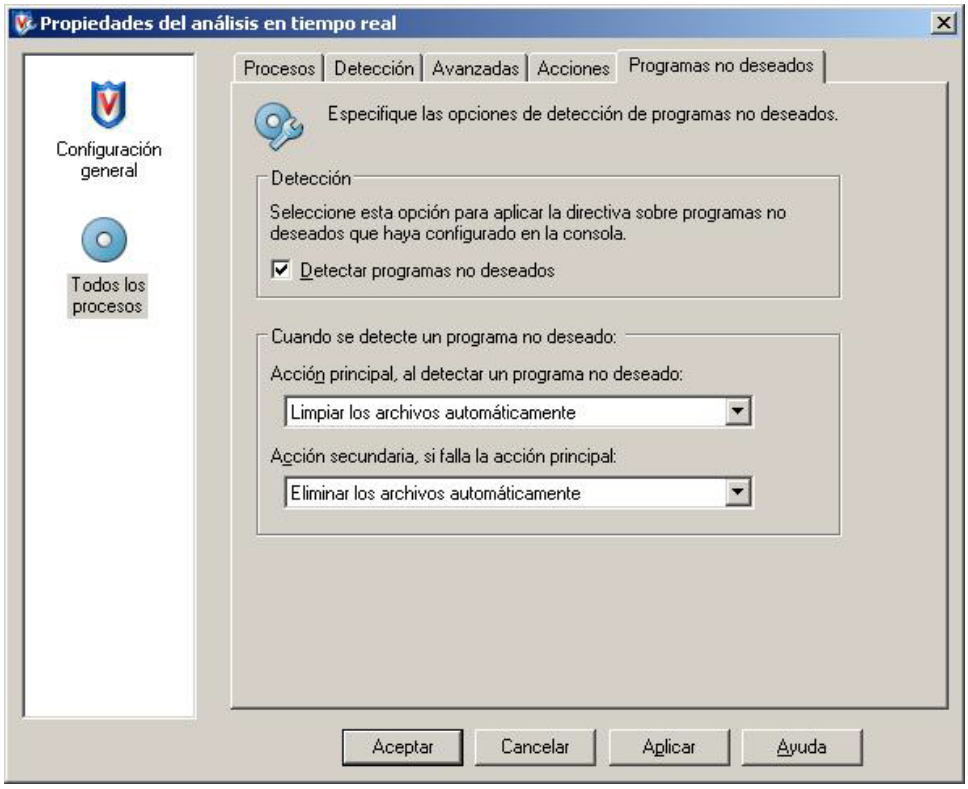
Se habilitó Protección máxima porque es la mejor manera de defenderse con los ataques de los virus, cualquier acción que se realice como copiar, almacenar, mover o abrir un archivo, Protección máxima escanea todo tipo de archivos para asegurar que un virus no atacado.

Con las siguientes opciones dentro de Protección Maxima:




Propiedades del análisis en tiempo real
Configuración general
Todos los procesos
Procesos
Detección
Avanzadas
Acciones
Programas no deseados
Especifique las opciones avanzadas de análisis.
Heurística
Buscar programas desconocidos no deseados y troyanos
Buscar virus de macro desconocidos
Archivos comprimidos
Analizar dentro de archivos (p. ej., archivos ZIP)
Descodificar archivos MIME codificados
Varios
Analizar archivos abiertos para copia de seguridad
Aceptar
Cancelar
Aplicar
Ayuda


Propiedades del análisis en tiempo real
Configuración general
Todos los procesos
Procesos
Detección
Avanzadas
Acciones
Programas no deseados
Especifique cómo responder cuando se detecte una amenaza.
Cuando se detecte una amenaza:
Acción principal, al detectar una amenaza:
Limpiar los archivos automáticamente
Acción secundaria, si falla la acción principal:
Eliminar los archivos automáticamente
Aceptar
Cancelar
Aplicar
Ayuda


Propiedades del análisis en tiempo real
Configuración general
Todos los procesos
Procesos
Detección
Avanzadas
Acciones
Programas no deseados
Especifique las opciones de detección de programas no deseados.
Detección
Seleccione esta opción para aplicar la directiva sobre programas no deseados que haya configurado en la consola.
Detectar programas no deseados
Cuando se detecte un programa no deseado:
Acción principal, al detectar un programa no deseado:
Limpiar los archivos automáticamente
Acción secundaria, si falla la acción principal:
Eliminar los archivos automáticamente
Aceptar
Cancelar
Aplicar
Ayuda

ANEXO D

PROCEDIMIENTOS PARA ENCRIPTAR MEDIANTE PGP

Como un método para implementar un control mayor a la información considerada crítica de cada usuario de Uniplex, utilizamos como una solución la herramienta PGP con la cual podremos encriptar un archivo de tal manera que podamos garantizar que nadie lo pueda leer salvo el destinatario.

El PGP funciona con dos claves o 'keys':

a) **Una pública** que se auto genera y que es la que se tiene que intercambiar con otros usuarios para poder mandar mensajes encriptados.

b) **Una privada** elegida por el usuario, que es la que se tendrá que escribir cuando se desencripte algún archivo.

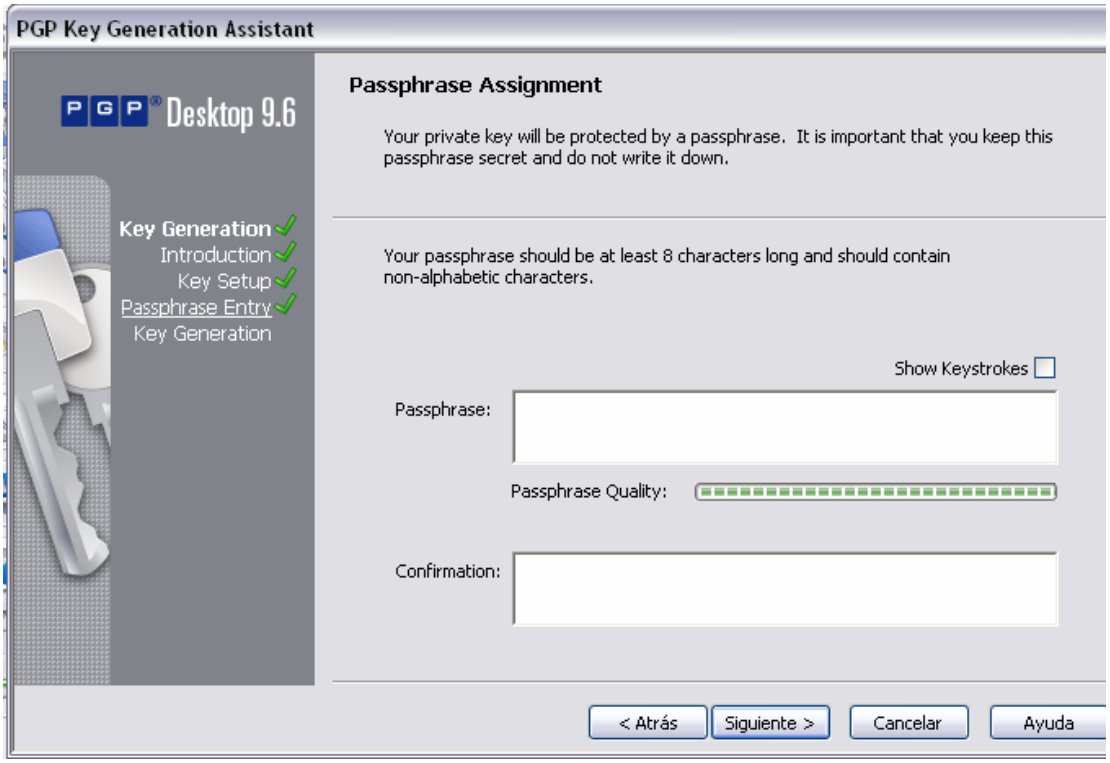
Generación de la clave pública y de la privada.

Para generar la llave pública se sigue los siguientes pasos:

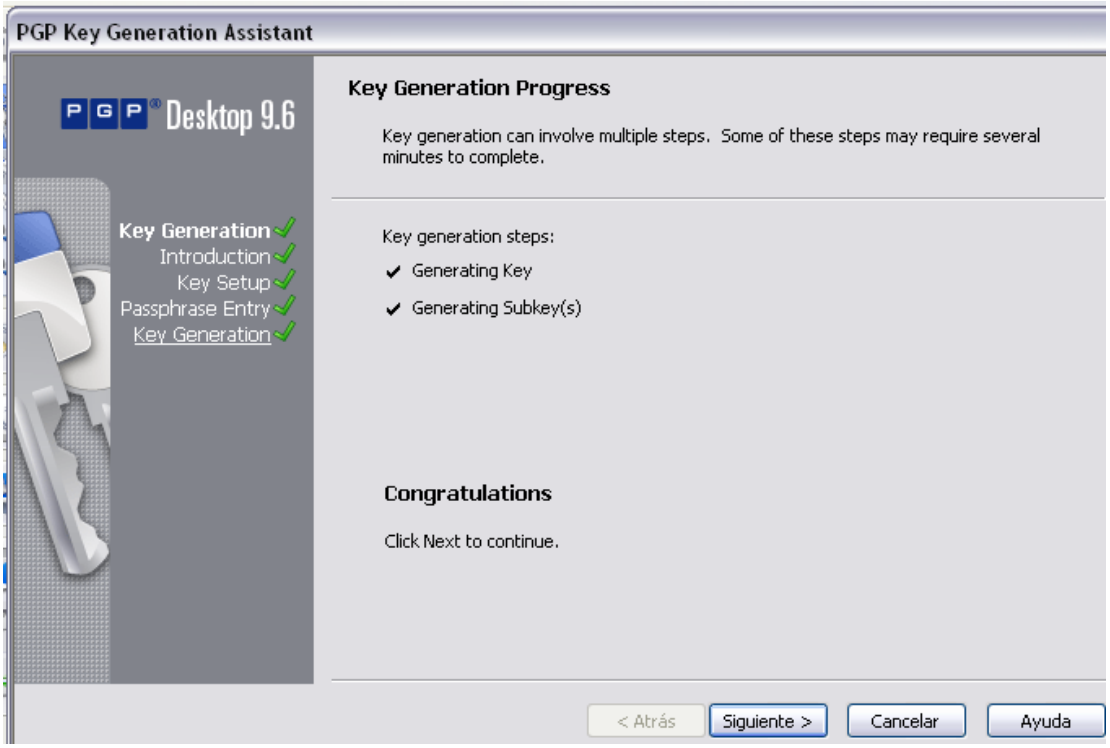
Escoger File y luego New PGP key y aparecerá una pantalla como la que se muestra a continuación:

Cada llave pública debe estar asociada con un nombre y un correo electrónico.

A continuación se debe escribir la frase que será la clave privada. Si la frase de confirmación que está bien, ya se habrá finalizado esta operación.

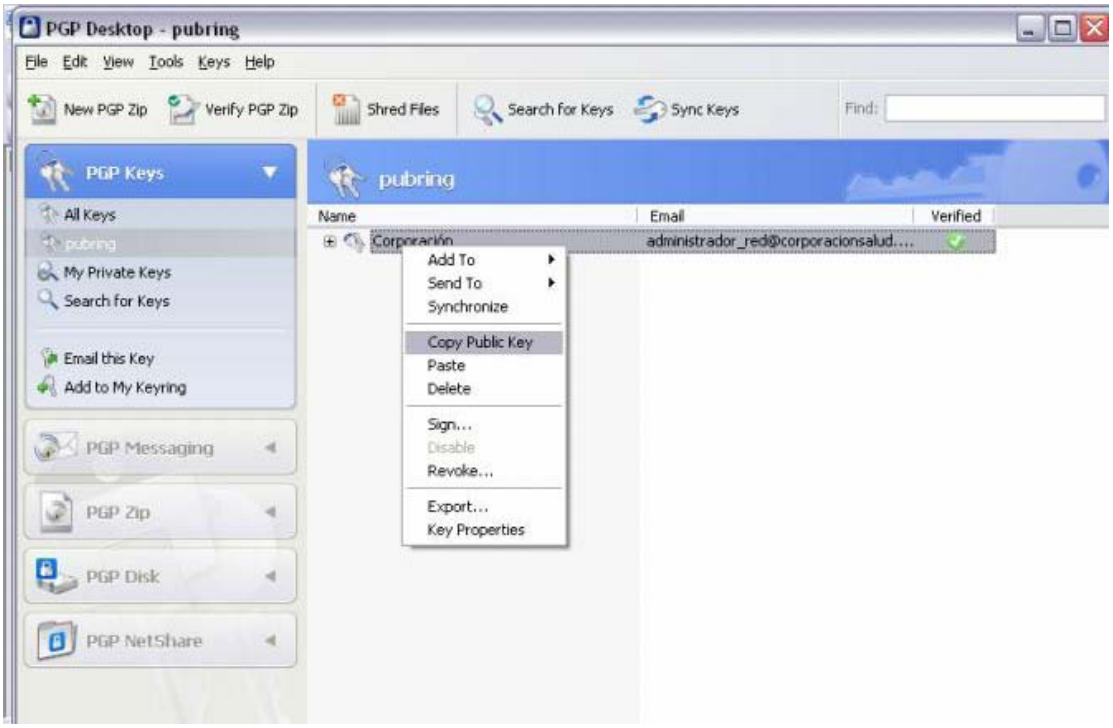


Y finalmente si todo salió bien aparecerá la siguiente pantalla:



Procedimiento para enviar la llave publica a otra persona.

Seleccionar la llave y copiar la llave pública



Esta llave será enviada mediante el correo electrónico, en el cuerpo del mensaje de correo electrónico, poner edit y paste y enviar el mensaje, y se pegará en el cuerpo de mensaje de correo electrónico la llave pública encriptada, para este caso la llave pública es la siguiente:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP Desktop 9.6.3 (Build 3017) - not licensed for commercial use: www.pgp.com
mQENBEbgv0sBCAC9qnT9aUkMHuXKoZyzvysvlFyBygvZLlhdC2evPjYfqiHnpOKM
phqgOlhEWE23XzTmaieP1DYPZjE78jdyIwED3TEL74d3GGaShcABRqRkuEwQ0NM9
ZQm63CYxVPflDNH14MggAZxfHtykJ3Dz3f9eC5FkjajTRsRfNiC9n1GgDSyi1WSf
H9grh3OR/1ohiN5q1/o3FvT6iAN1RmX+mX+Rpx38leuvbUmsoF9Pv9STcmD4bBVd
1ZTNdmd4U//9Ekjpkwh3IwwVwWHadCZ4WYYUbMc0104zMe74xRS+HFtWNAF7+X0F
uNiNbbEtvIXIcMpFJXXNRXTaBsJOsu3ctZXbABEBAAG0F21hcmNvIDxtYXJjb0Bn
bWFpbC5jb20+iQFtBBABAgBXBQJG4L9MMBSAAAAAACAAB3ByZWZlcnJlZC1lbWFp
bC1lbmNvZGluZ0BwZ3AuY29tcGdwbW1tZQcLCQgHAwIKAhkBBRsDAAAAAxYCAQUe
AQAAAAQVCAkKAAoJEEW8RhAX+b0SrZIH/Agufg7w8f0P5fjY73aBIr+otATVavrI
KpDG+2v48Se0Y9x+ACCWhvocwGSfJMZDqpqmzPJw8hezetKwcv6HA/sQCdw1AVax
iKCf2faodfheY82zReR2pWCakvKCpt2itUCbsuoe1Y9oyL55+QQ+mej5xIeVFeY
JP2ap7+mnfH7hYYUMyM5Zpb3wExwJb+y0vUDpTXF4W4WdbfCW4El0tc9gAum1OY2
1yLx4emAxHmhSQ2mXH9JQlSD3+jSAcKHOn4pdjSMUlzJyD3cBh/zrLNuSm6KG6ly
/c7b9A1ZQ193TrzpBBZdogsct/TXWNPFgtUJ6CglcLWOnpZt2u9Qfhu5AQ0ERuC/
TAEIAK9Me3XPMRgki9HrmEn7Csoip+YS4/MLqpMK0x8vvZutKmE0o5/pU+jxGC9j
kQl838jhc89ahEfIGWPk7JuCdhhJmFjTQppBHII7Ia3ox+Sh0Z7C7SWIbVNFLs4B
Kn+Mz1AoM7l+fpWdUdF9Fp1PBl55txww8Dmypb16mCg0P/DaadIEOOywYWHH9CHR
cPpt1+zoXJsiXPvO7poPfV/iQwFAdJxf2T74+GbO0xqIuMFgfpGx5YiOGxI8/6Bn
/RyaYPnGSzQsDjzIpfWgeubcG07rDJFWGTh6/cQgZfqb5hSA/jVBNL6Pojhjpmwn
ZEBJy/LONDBqpnGiSaZVaI75qMUAEQEAAYkCQQQYAQIBKwUCRuC/TQUbDAAAAMBd
IAQZAQgABgUCRuC/TAAKCRB6QgIyhvhZl6mbB/9qDB+iNkAlooNOAdz+42/kdJkZ
M8884pkg4veEU/tIyuRS1mJLQmKuk24hQ6NGrNaFRgebM6cgxKUHIFlk2lXtHjVz
AfKBxGrTver+PRYMvDzHZrUttrTAI25jXVmoftPCWw2aMaACIaw5nI+VgzfZGRLC
dFA/yRahdlHRagNWcYy0xpHse6w+sOWRedhWWqNhYud7/yTfwCjrmnuzgr66CZmX
CCqLXY3YqNW1ZBmrVGGSHI1UEGemiI3mI3IlyH7ajFoMkMk6VX5XVi6maj49dQsi
hncrxbuuMaMiDqhzy1fmYTV+BePSz6c43Lt7D4ndT3rmudi2YsNv4RuCOkqMAAoJ
EEW8RhAX+b0S7qYH/0kxVAI0631VtUUb+BD4pmDxOESDeptmiJgF72YHTE+Lt/cW
3+GPdU2mPO/Ql17zRwJYgzTT2cL9EyK1UzPJI3hdAALVYU6WeqHA9L0vKIKjiTgW
nQG9z7yEKu12rJRa48v9NrZm9u6+DvaHsDtyoNkr8JO2reUicuID5Wmzu/wq2zAT
x7yRgFv943OF03pLkrxh3Q4S065ecp0A2m71g0NibgzmHDqRVfVY5Ko7UuffeSDQ
YYpgbsqbU1wuDivWJN3NpFnSQbdkIrI0kFtPAez4FSrBHPT0OjRLZ+hkWgDZjJN5
pv8x1peufxRZRlczQPSDG8THVxrvztsP9Zr1SeE=
=3lpJ
-----END PGP PUBLIC KEY BLOCK-----
```

Procedimiento para añadir al llavero la llave de otra persona

La llave de la otra persona llegará por un mensaje e-mail.

En el e-mail que se recibirá, seleccionar el texto entre las líneas que dicen 'BEGIN' y 'END' y copiar:

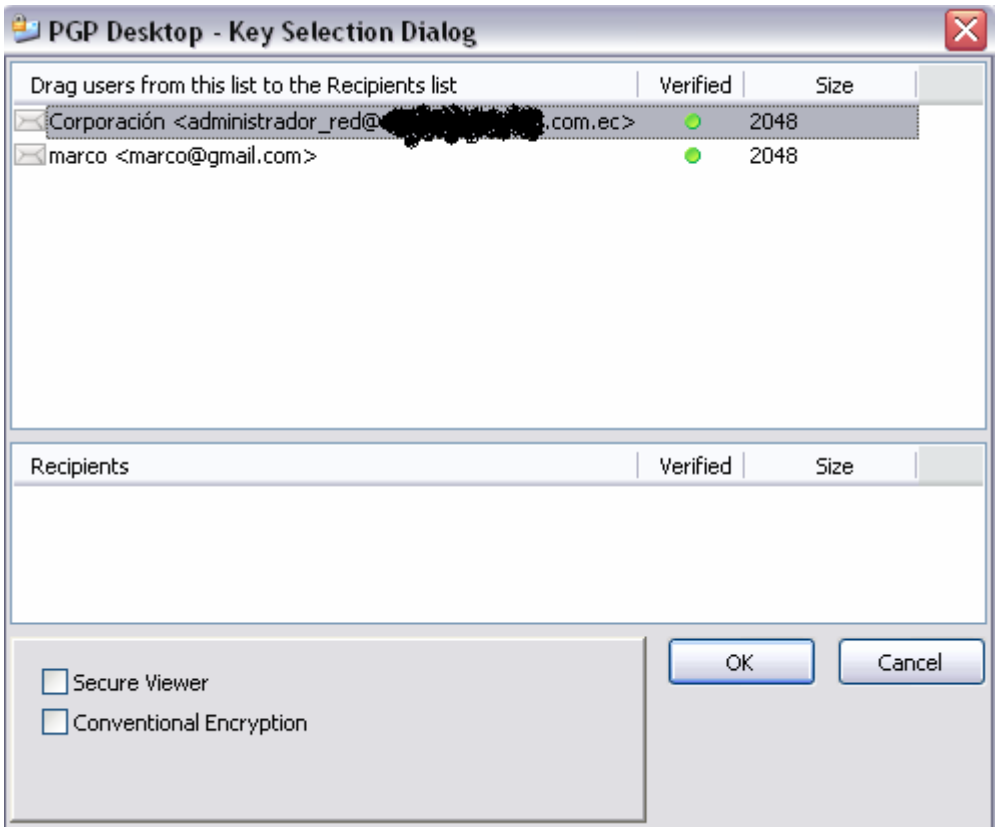
En el icono PGP seleccionar PGP Keys;

Ir a editar (edit): pegar (paste) y aparecerá la llave pública de la persona que te ha enviado por e-mail, finalmente pinchar en 'import'.

Procedimiento para encriptar un mensaje de correo electrónico:

En mensaje a ser encriptado se copia en un block de notas

Un clic sobre el candado ubicado en el la parte inferior al lado derecho y escoger la opción **'Clipboard: encrypt',** aparecerá la siguiente pantalla:



Como se nota aparece el llavero entero pero se deberá escoger la llave pública de la persona a la que se quiere enviar el e-mail, con doble clic para que se pase al rectángulo inferior

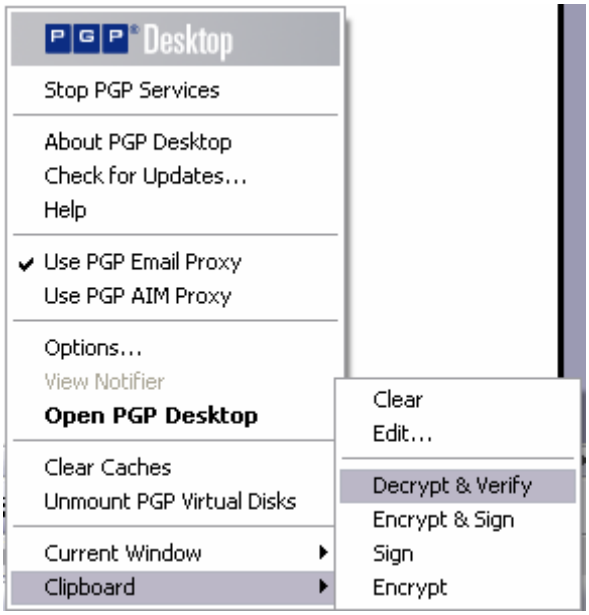
A continuación se abre el programa de e-mail y se pone los mismos parámetros dirección de destinatario, asunto, etc, finalmente se escoge edit, paste y se pegará el mensaje encriptado como el siguiente:

```
-----BEGIN PGP MESSAGE-----

Version: PGP Desktop 9.6.3 (Build 3017) - not licensed for commercial use: www.pgp.com

qANQR1DBwEwD9EwDc9tCO7oBB/9Hq2zHwrB1OjG9pEh2uxZ3YDTBhZnjv0NqldYu

0yvgiv+eDc+kK7U1fpAimIWt+9uFa98S/V/IxQsUzvmS6K0iBIlbCmH+ZEV0Rewa

rTnvRauEvSAQpWRVCpabxnQREUo4lfjCOagTYn29V6pXhCbrNMhheGbyyLgtOb4Y

osPxZjztR35AZFO2vcU6OpV3JuIErNOUYGn1ahxxqFFcLSreYt6xpqQfnFKqIBbD

Jmzc/aqo5G1M2JntkZi3MXzxtr1/tfNmk8FU640QBwEgvJpuDUqqF0pS0NurenfC

mqhKd24ELtmgyfyU3xllByeQMKarmDhdh4EE/wDUo/UlH8oi0osBCMbmfx2Yo2JF

Y3bkTR7WtnJs3CD17fN59m1092tatO62b+YPRCnOpjqupu3a0SkC858rTZ3jUtEl

TIosyt73eY8tS9WHQeVt++n/FUIEH9B9kqL93d58Pb1FGzCcGhGI61l0Ios3YrqU

zlE6rYQvo7kvWJ1+iww9jLD97GKoxqVkZyXS0H13nd1l

=KYn4

-----END PGP MESSAGE-----
```

Procedimiento para desencriptar un mensaje que se recibe por correo electrónico.

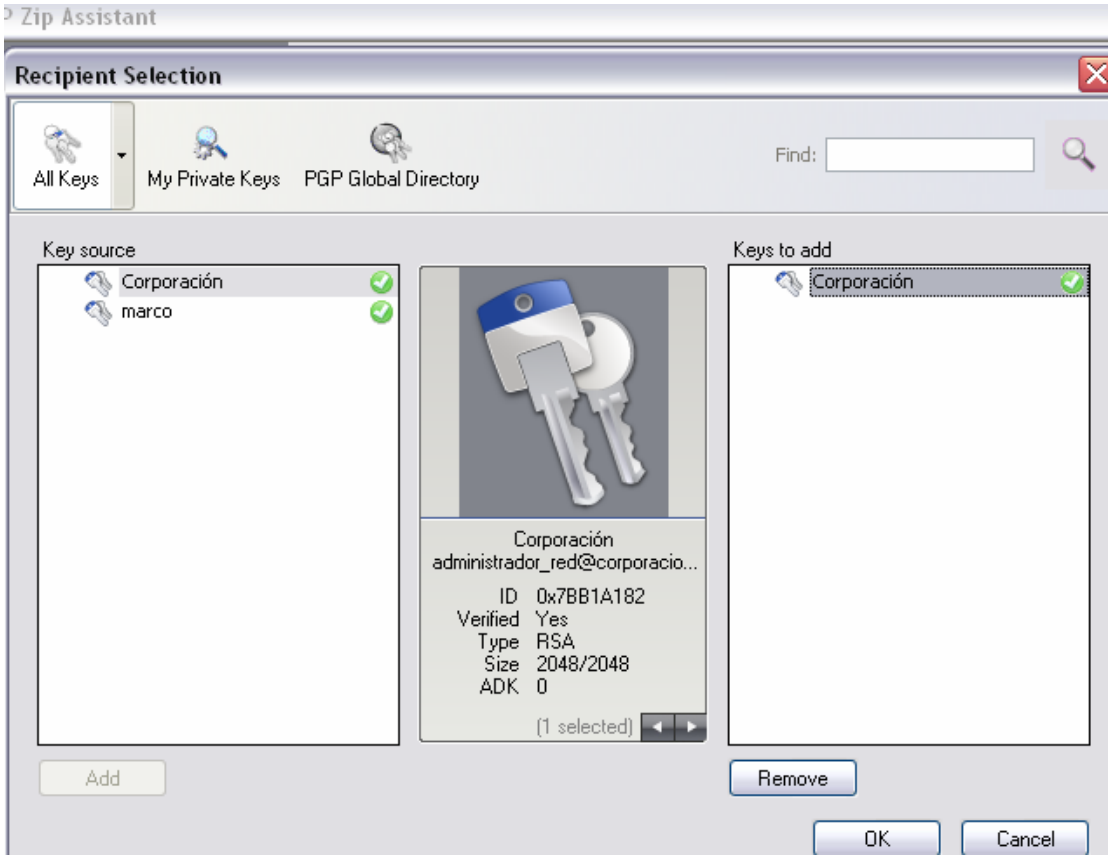
Copiar el bloque sobre el texto de PGP entre BEGIN y END

En el icono PGP escoger: Clipboard: Decrypt and Verify

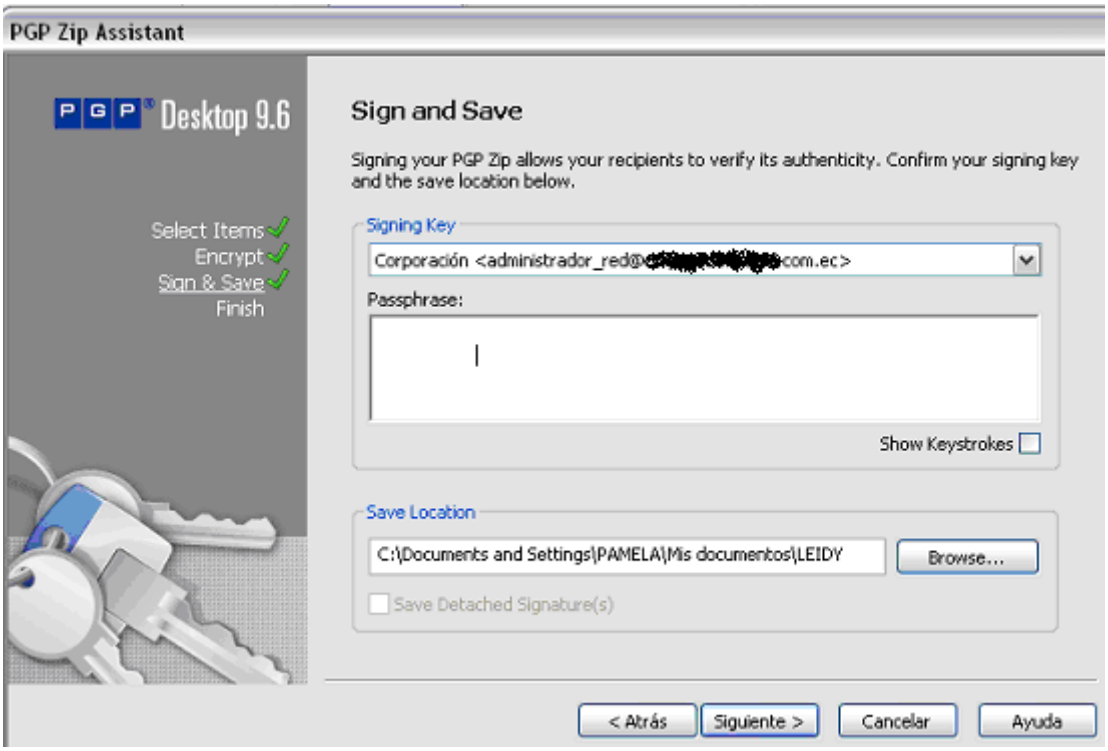


Procedimiento para encriptar un fichero para mandarlo por adjunto (attach).

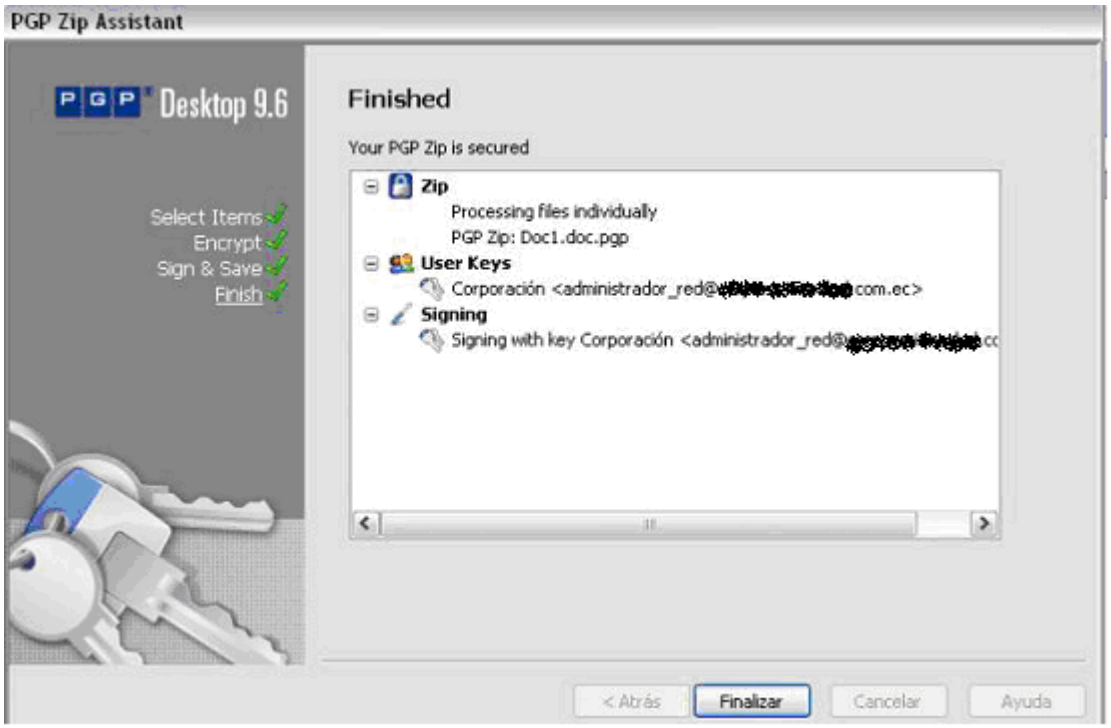
En el explorador de Windows se busca el archivo que se desea encriptar, click derecho sobre el fichero y se escoge la opción encrypt, a continuación se selecciona la llave de la persona a la que se va a enviar la información



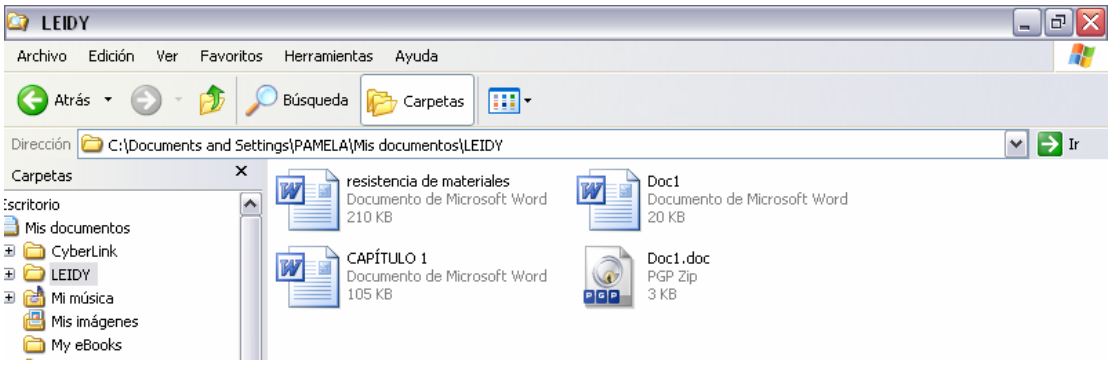
El asistente pedirá insertar la frase de la llave del destinatario:



Una vez ingresada correctamente la clave, aparecerá una pantalla como la que se muestra a continuación:



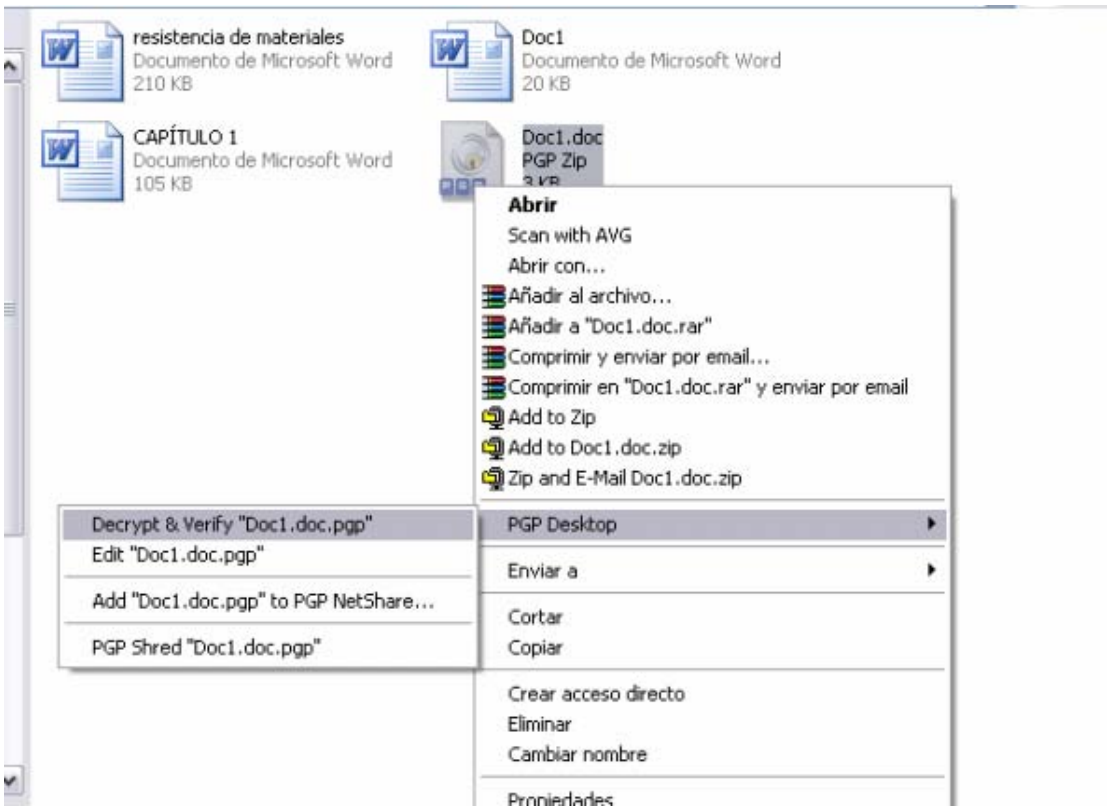
El programa crea un fichero con el mismo nombre que el original (el no encriptado) y que lleva por icono un candado también. Este fichero se crea en el mismo directorio o carpeta en que se encuentra el original.



A partir de aquí se repite el proceso normal de mandar adjuntos (attached files) vía email, como si fuera cualquier otro fichero, pero seleccionando el fichero que lleva el icono del candado.

Procedimiento para desencriptar un fichero adjunto que nos han enviado.

Se graba el archivo encriptado en el disco duro de la máquina local. Click derecho sobre el fichero encriptado en pgp y se elige la opción "PGP: decrypt and verify".



El programa pedirá tu clave privada, si la frase está bien escrito, el programa creará un fichero en el miso directorio y con el mismo nombre de archivo pero desencriptado y llevará el ícono del formato original.

ANEXO E

SEGURIDAD EN EL SERVIDOR DE CORREO ELECTRÓNICO

Seguridad:

La seguridad en Lotus está dada por default en el equipo mediante encriptación propietaria de Domino y la inclusión de certificados digitales.

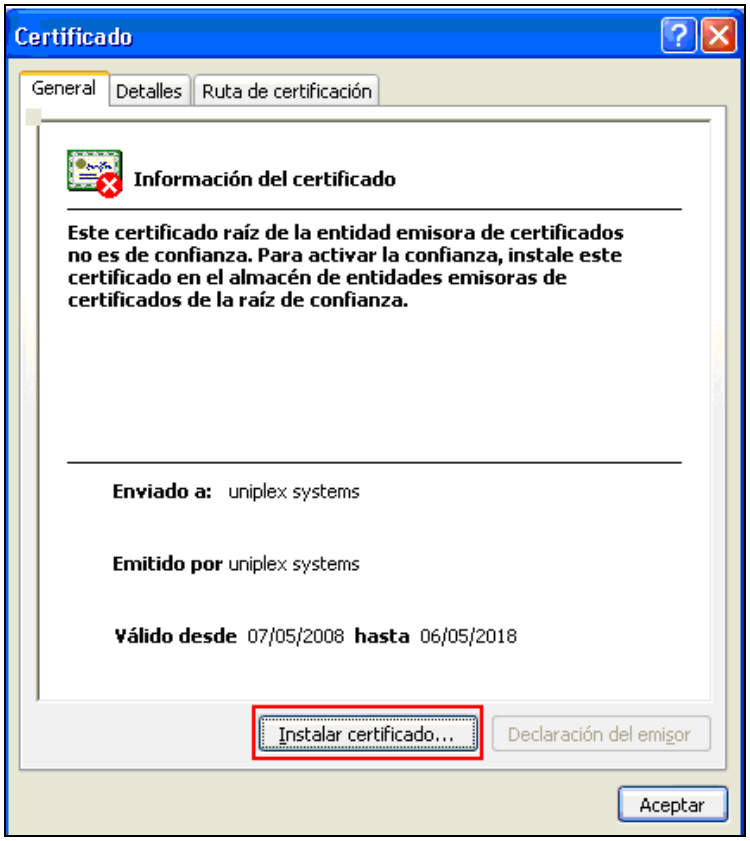
Ejp:

CAMBIO DE CONTRASEÑA DE CORREO VIA WEB

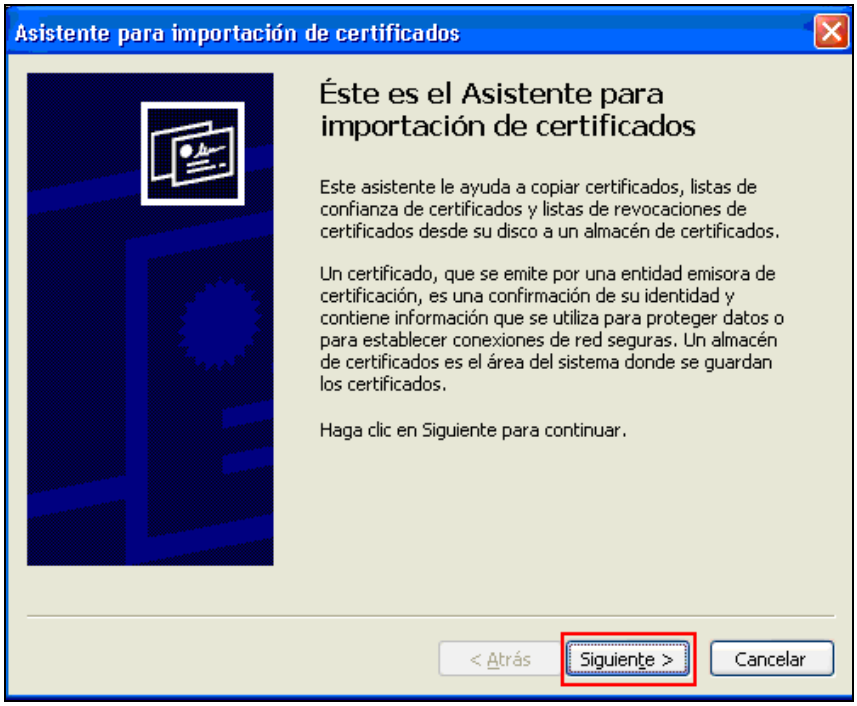
Para cambiar la clave de correo vía web es necesario:

- Instalar el certificado llamado **cert,** para esto dar doble clic sobre el certificado.

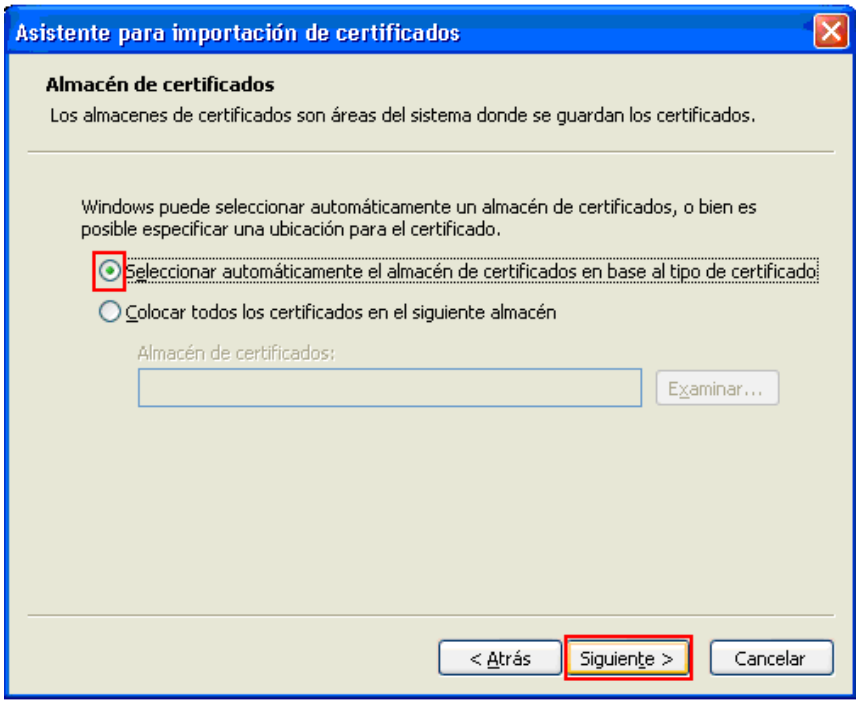
- Dar clic sobre el botón ***Instalar Certificado***



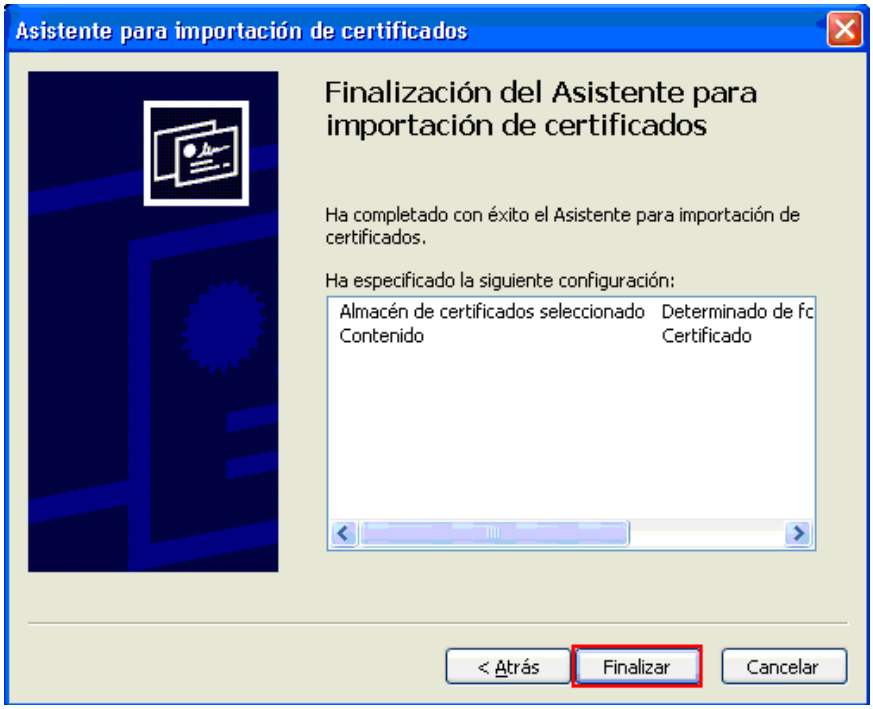
- El asistente para la importación de certificados aparecerá, dar clic sobre el botón ***Siguiente*** para continuar.



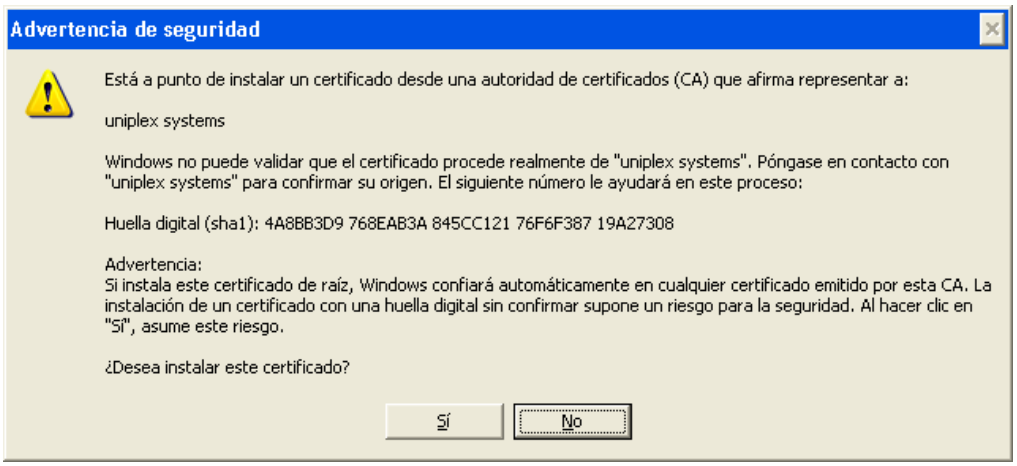
- Verificar que la opción ***Seleccionar automáticamente el almacén de certificados en base al tipo de certificado*** esté seleccionado, dar clic en el botón Siguiente para continuar.



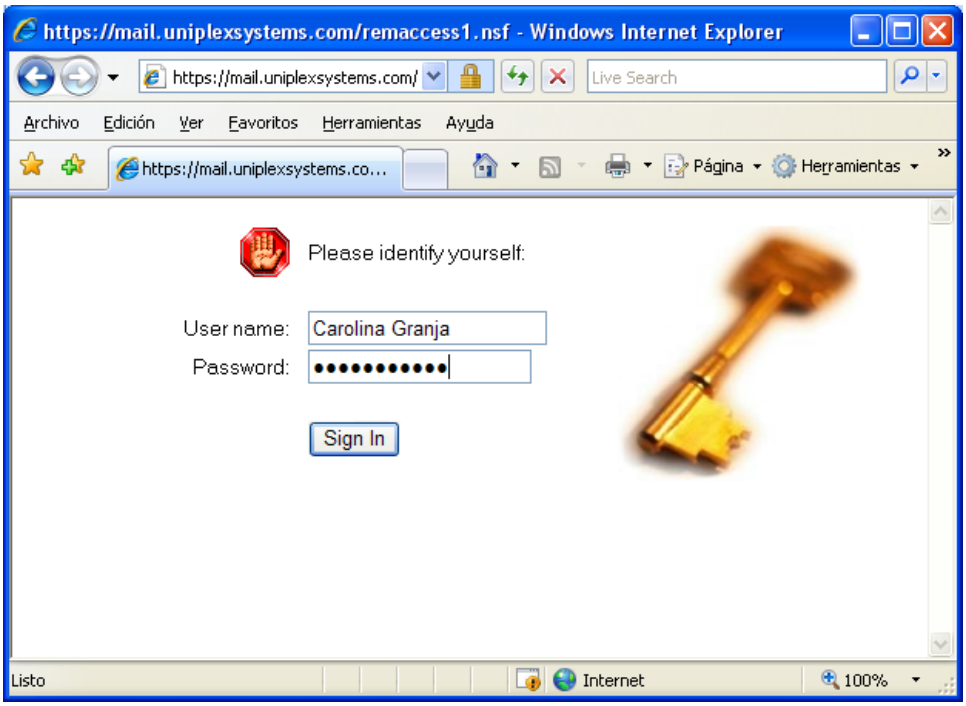
- Dar clic en el botón Finalizar para ferminar el proces de importación de certificados.



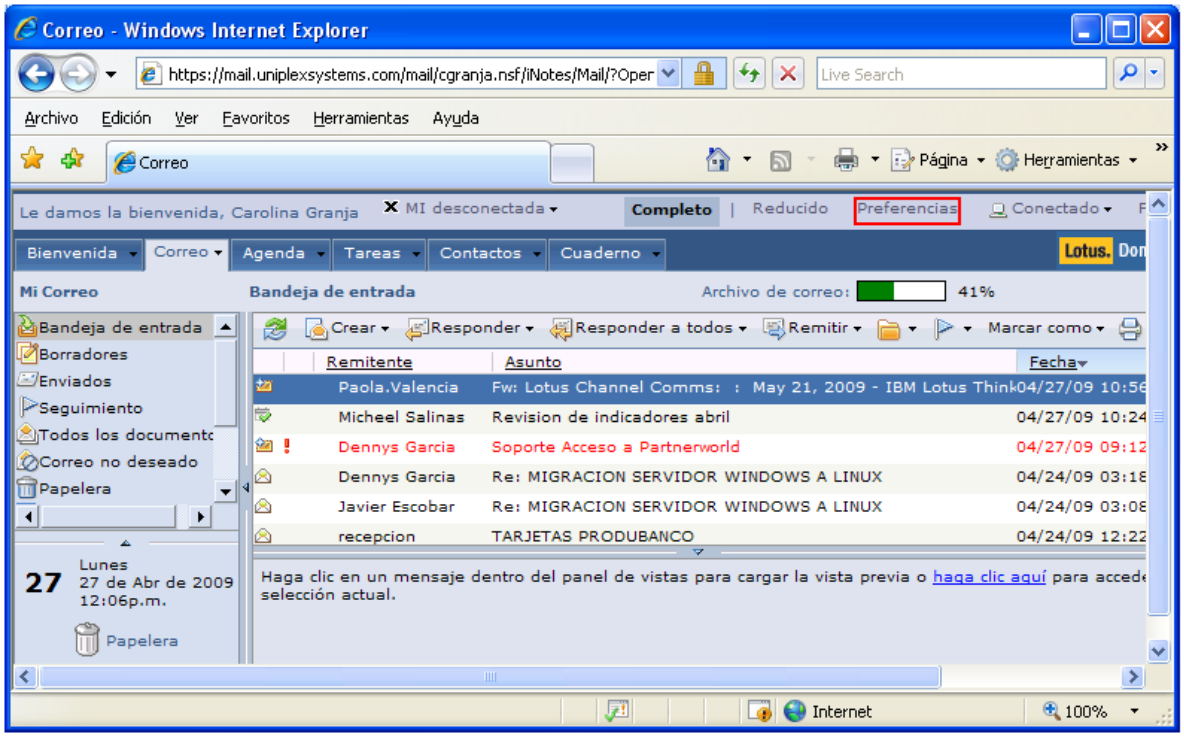
- Dar clic sobre el botón ***Sí*** para instalar el certificado.



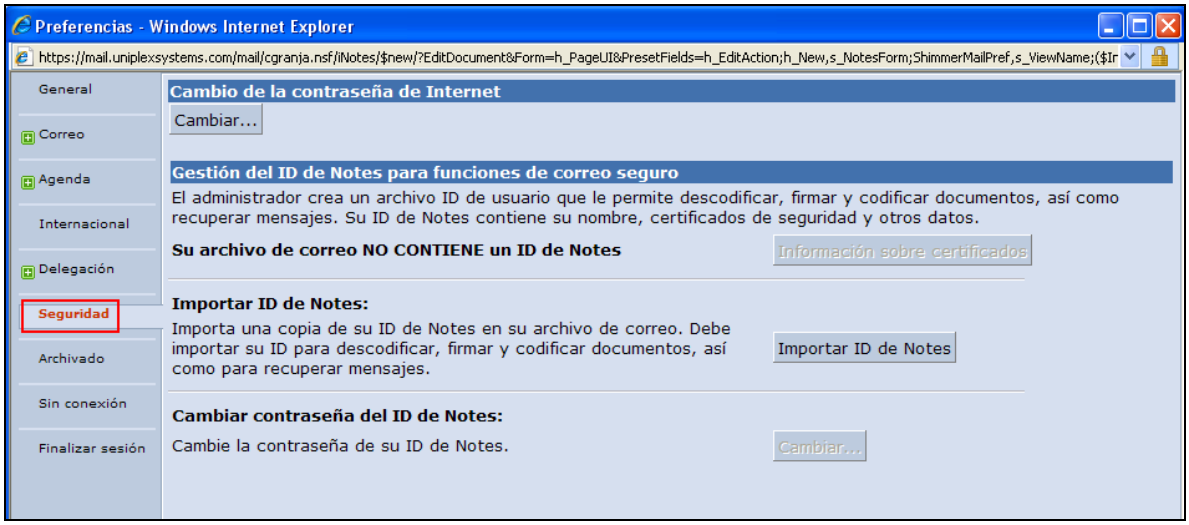
- Abrir un browser e ingresar la dirección: https://mail.uniplexsystems.com/ , ingresar el nombre de usuario y contraseña (la contraseña es la misma del sametime no la del cliente lotus notes).



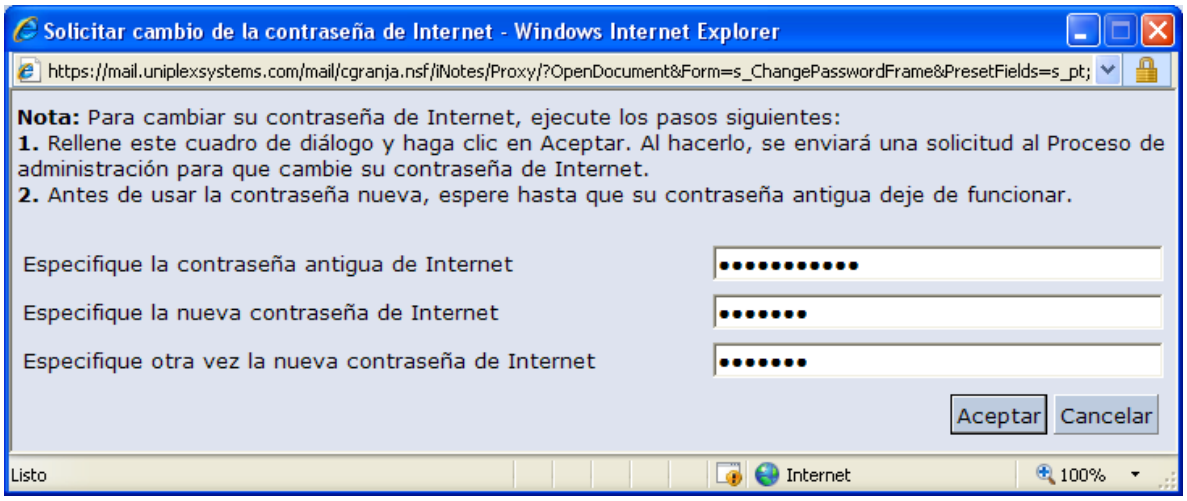
- Hacer clic en el botón ***Preferencias***



- Hacer clic en el menú ***Seguridad***

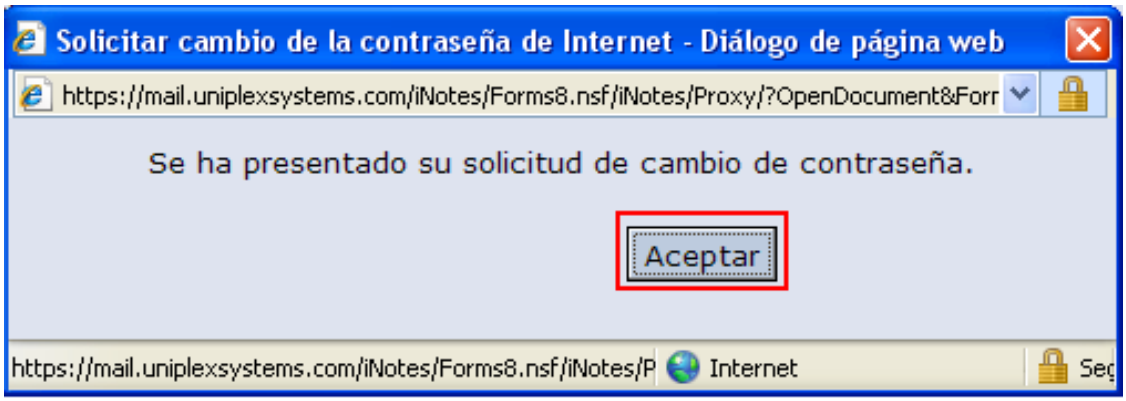


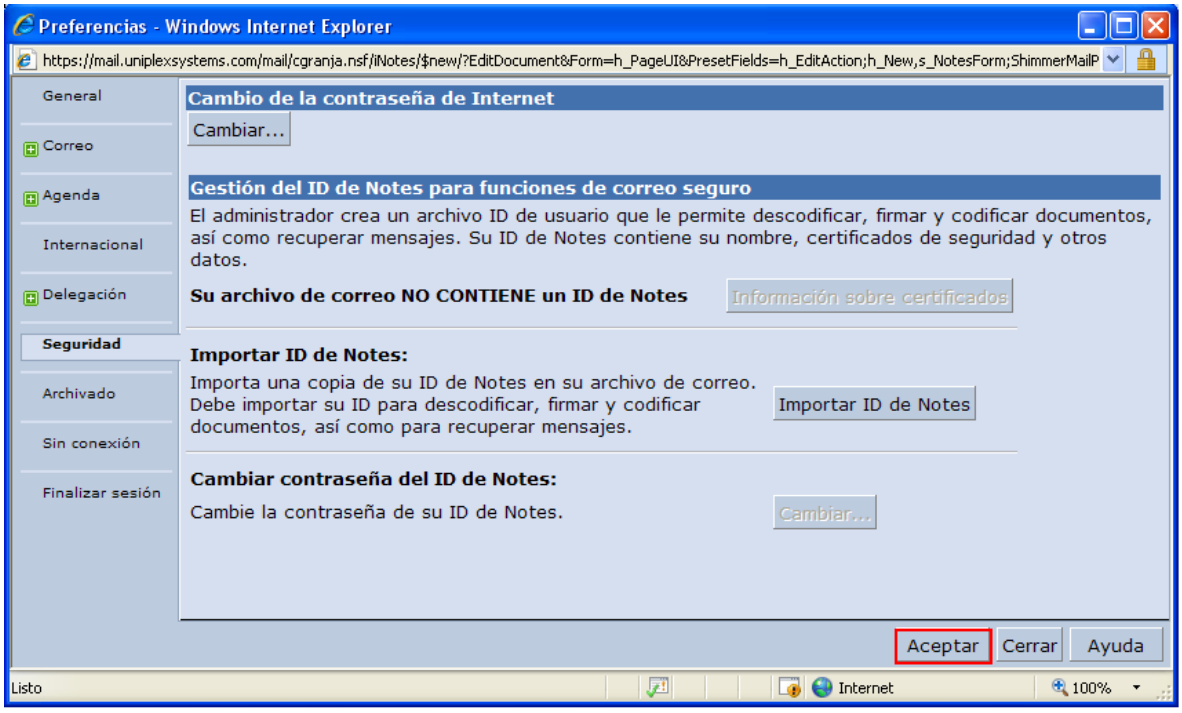
- Hacer clic en el botón ***Cambiar*** y especificar la contraseña antigua y nueva de Internet.



- Dar clic sobre el botón ***Aceptar*** para que la solicitud tome efecto

- Hacer clic en el botón ***Aceptar*** para que se guarden los cambios.

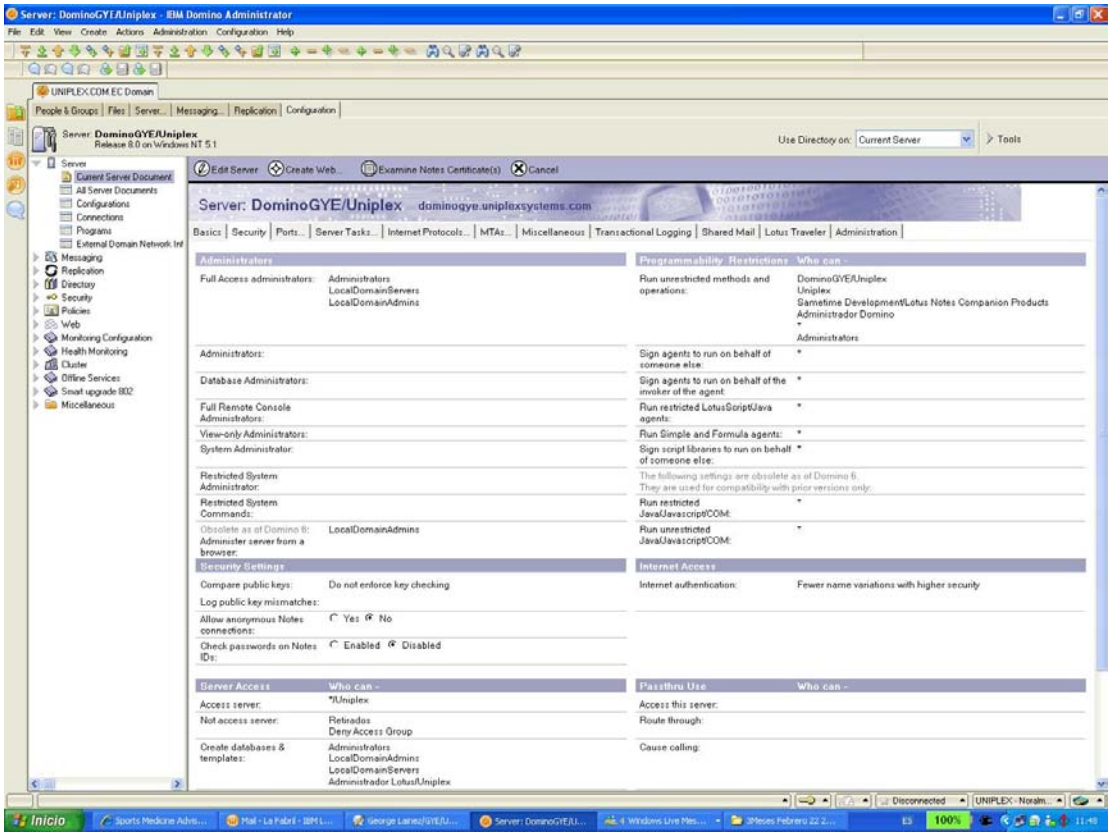


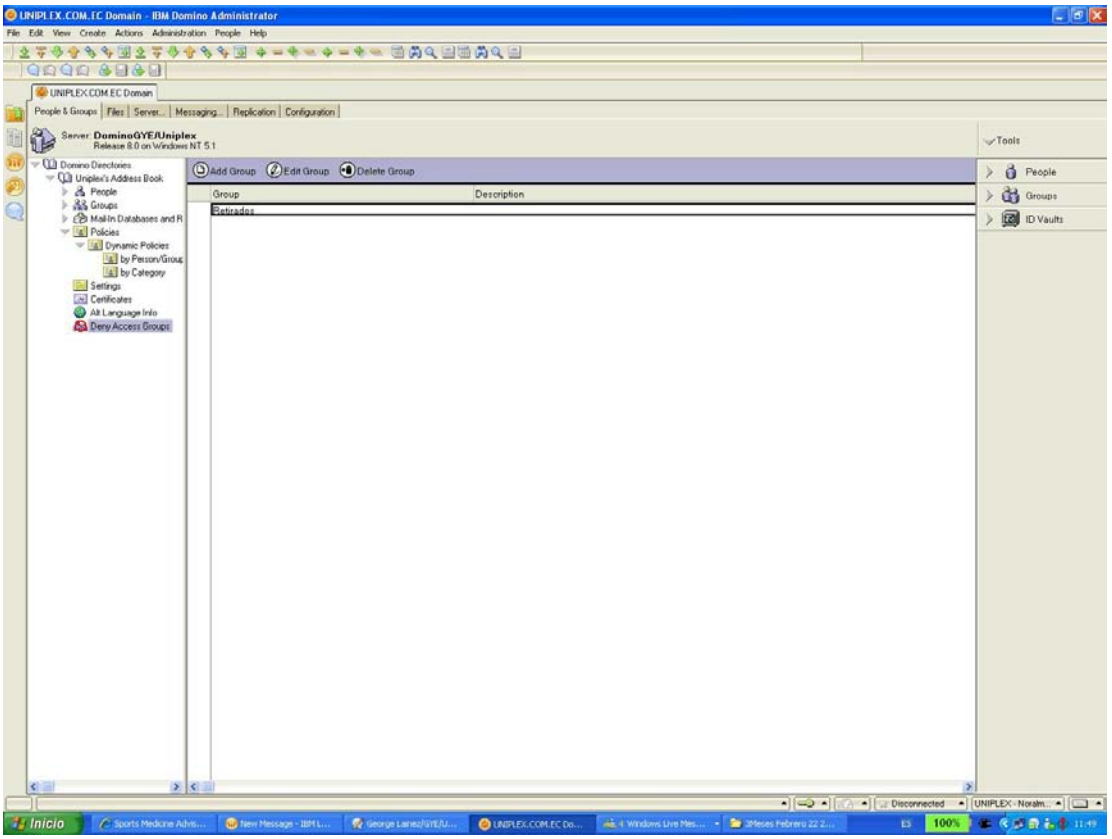


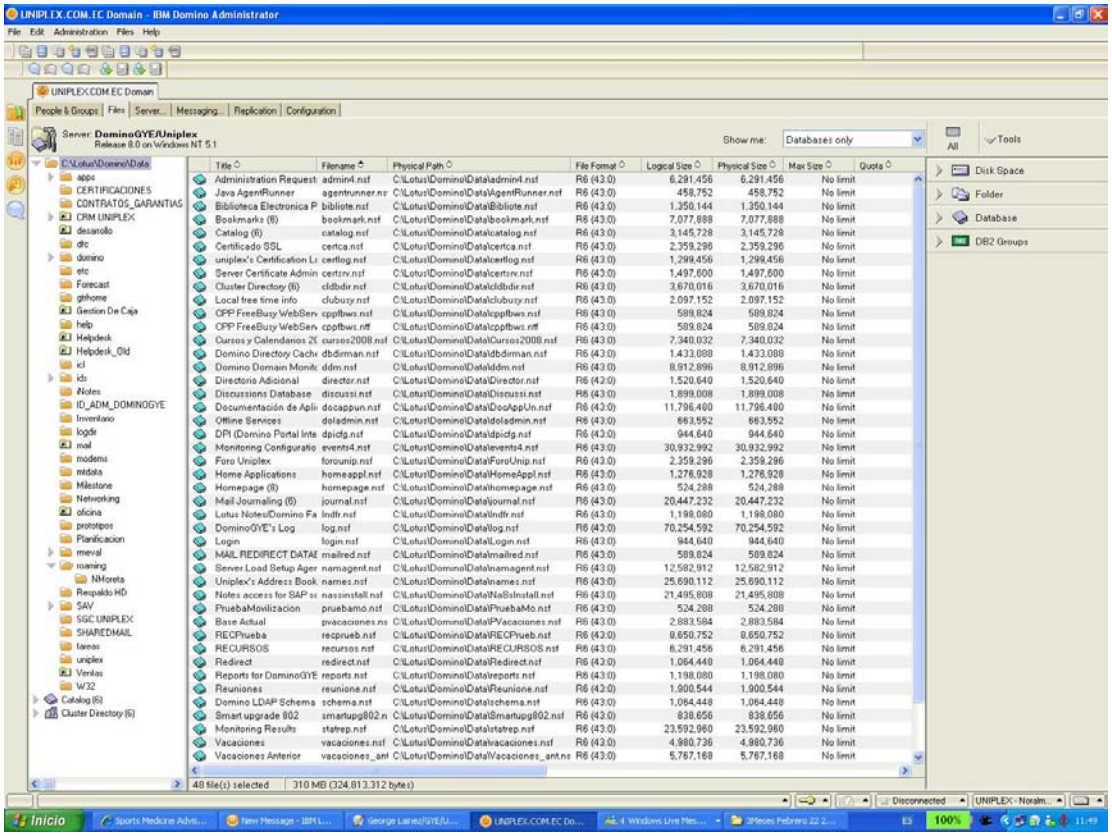
- Siguiendo estos pasos se habrá cambiado la contraseña del correo vía web y la del sametime ya que es la misma contraseña.

Respaldos:

Copia fisica de archivos de la Data del servidor, Ids de usuarios, certificadores y del servidor bases de configuración de Domino (names.nsf, admin4.nsf, certlog.nsf,staprep.nsf)


Server: DominoGYE/Uniplex - IBM Domino Administrator
Server: DominoGYE/Uniplex
dominogye.uniplexsystems.com
Basics | Security | Ports... | Server Tasks... | Internet Protocols... | MTAs... | Miscellaneous | Transactional Logging | Shared Mail | Lotus Traveler | Administration
Administrators
Programmability Restrictions
Security Settings
Internet Access
Server Access
Passthru Use

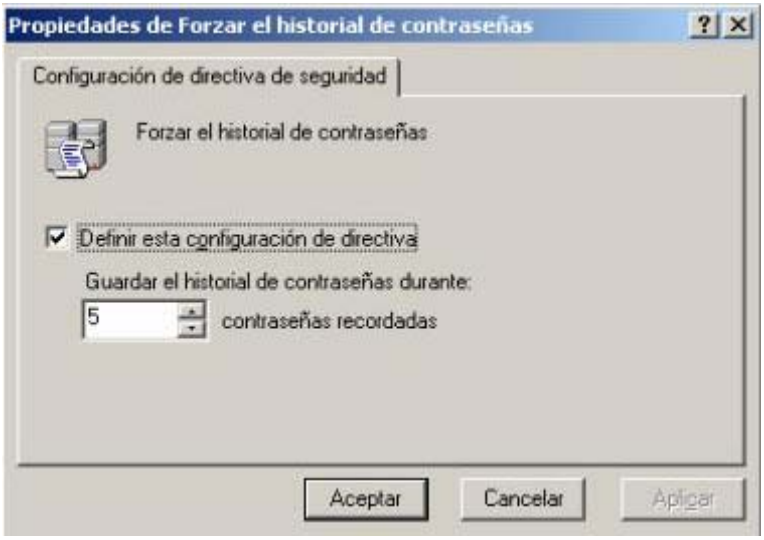

UNIPLEX.COM.EC Domain - IBM Domino Administrator
Server: DominoGYE/Uniplex
Release 8.0 on Windows NT 5.1
Add Group
Edit Group
Delete Group
Group
Description
Retirados
People
Groups
ID Vaults


UNIPLEX.COM.EC Domain - IBM Domino Administrator
File Edit Administration Files Help
People & Groups Files Server... Messaging... Replication Configuration
Server: DominoGYE/Uniplex
Release 8.0 on Windows NT 5.1
Show me: Databases only
All
Tools
Disk Space
Folder
Database
DB2 Groups
48 file(s) selected
310 MB (324,813,312 bytes)
Disconnected
UNIPLEX - Noralm...
Inicio
ES
100%

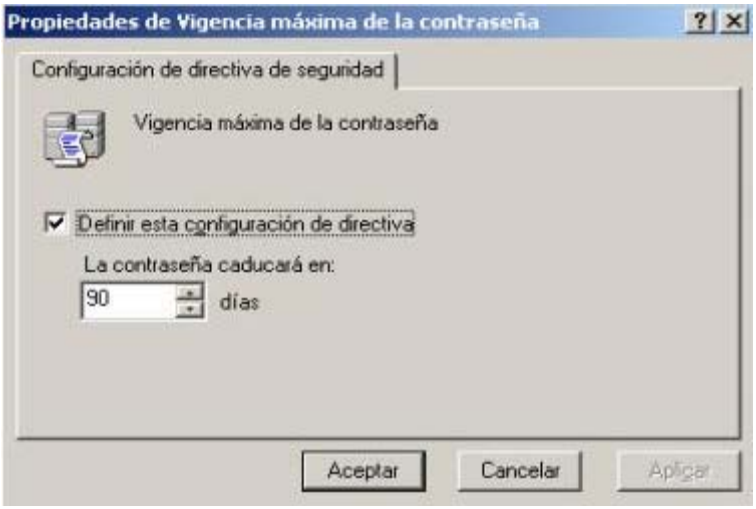
ANEXO F

CONTRASEÑAS

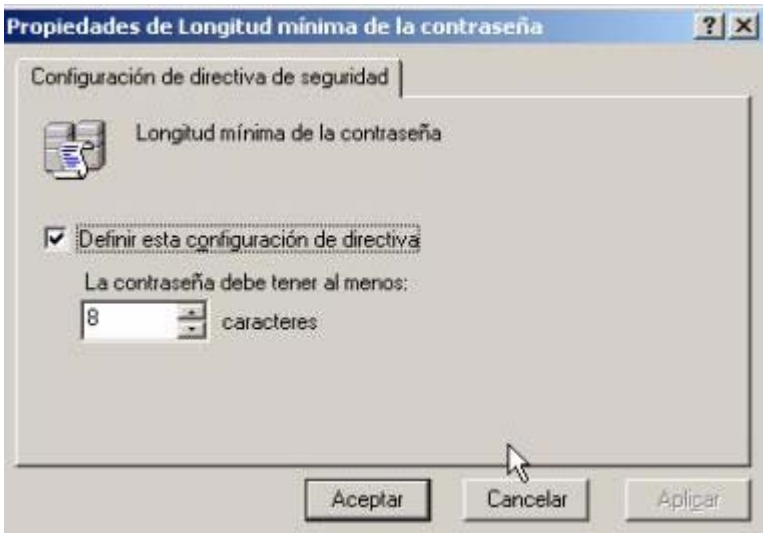
1. **Historial de Contraseña:** Cuando esta política se habilita, el Servidor de Dominio mantiene una lista de las contraseñas recién ingresadas, y no permitirá al usuario utilizar las contraseñas utilizadas anteriormente. La organización debería utilizar el valor de 5 (número de contraseñas guardadas), para forzar al usuario a cambiar su contraseña a otra diferente.



2.- Expiración de la contraseña: Esta política determina cuando la contraseña debe expirar, para que el usuario la cambie y no se corra el riesgo de que pueda ser descubierta, se debería configurar para que expire cada 3 meses.

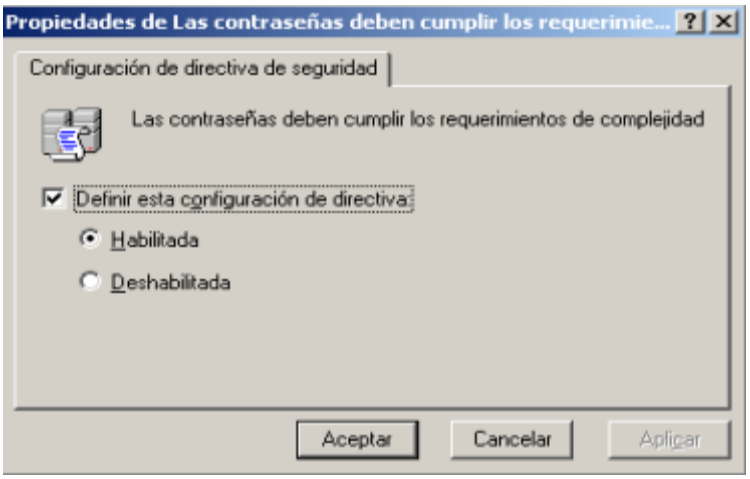


3.- Tamaño mínimo de la contraseña: En esta política se debe especificar el tamaño mínimo que debe tener la contraseña, que debe estar configurado a mínimo 8 caracteres, y se deben configurar reglas para el mismo.



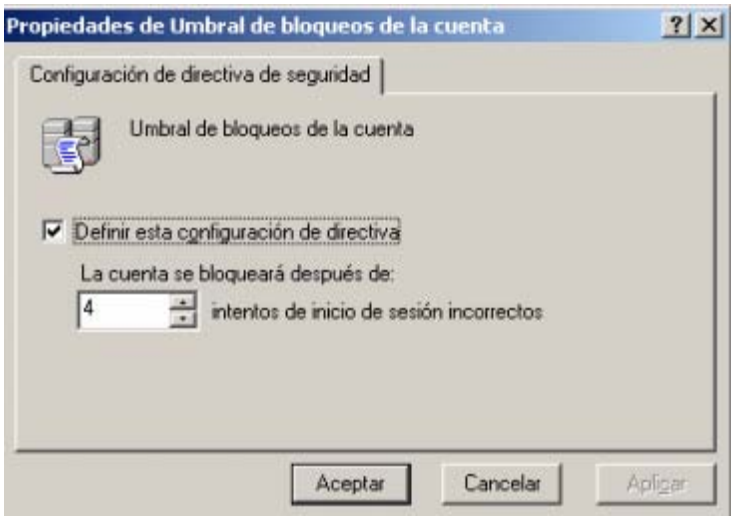
4.- Complejidad de la contraseña: Configurar los requerimientos de complejidad afecta a los nuevos usuarios y los cambios se verán reflejados luego de que la política se aplique. La complejidad que se aplica es la siguiente:

- Debe contener caracteres alfanuméricos (0,..,9; A,…,Z; #,…,%; a,…,z).
- No puede estar basado en la cuenta del usuario.

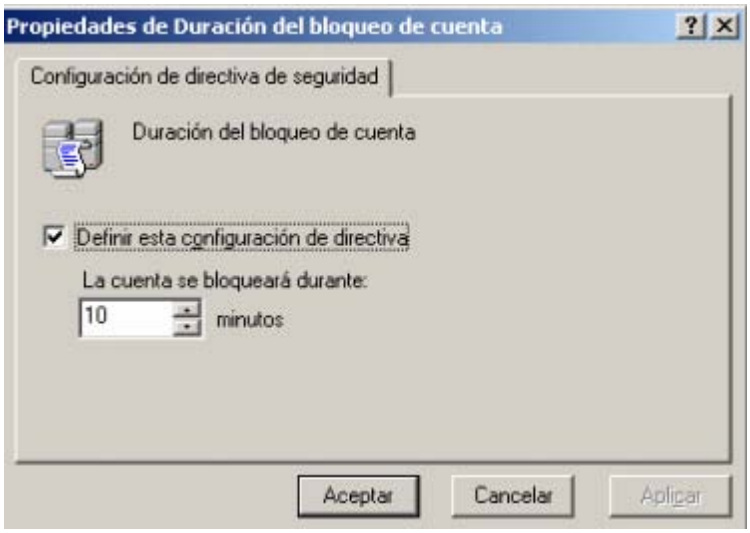


BLOQUEO DE CUENTA

1.- Número de intentos fallidos para el bloqueo: Se configura el número de intentos fallidos antes de bloquear la cuenta del usuario. Debería configurarse en 4 intentos fallidos como máximo.



2.- Duración de bloqueo de la cuenta: Se configura el tiempo en el cual debe estar bloqueada la cuenta, se debería configurar para 5 minutos como mínimo.



ADMINISTRACIÓN DE CUENTAS DE USUARIOS

Si un usuario olvida su contraseña, es necesario que esta sea reseteada y configurada para que cuando trate de ingresar le solicite cambio de la misma.

1.- Reseteo de contraseña de usuarios: Cuando un usuario olvida el contraseña debería solicitar al administrador que resetee el contraseña, el cual se lo debe enviar a su inmediato superior y configurarlo para que cuando lo ingrese le solicite cambio.

2.- Habilitación, Deshabilitación, Eliminación de Usuarios: Cuando un usuario se encuentre de vacaciones, o ausente por un largo período se debe bloquear su cuenta para que no existan problemas de accesos no autorizados.

Cuando un usuario salga de la empresa se debe bloquear inmediatamente. Para lo cual, inmediatamente se produzca un cambio en el personal; la persona encargada de recursos humanos debe enviar una nota al administrador de la red para que elimine los accesos del usuario a los sistemas de la red inmediatamente.

ADMINISTRACIÓN Y CONFIGURACIÓN DE PRIVILEGIOS

El Control de acceso involucra la configuración de derechos y permisos que aplican a ambos los objetos en la computadora local o red y los usuarios potenciales (incluso los individuos, computadoras, y servicios) de esos objetos.

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.
Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

Los privilegios que tienen los usuarios sobre cada máquina es otro punto importante en el control de acceso, para lo cual se debe configurar las máquinas para que todos sean usuarios normales sin privilegios de administrador, en caso de que el negocio requiera instalación de un software adicional al que se configuran las imágenes de las máquinas, se debe requerir una autorización gerencial dirigida al administrador de la red para que pueda ingresar con los privilegios de administrador e instale el programa.

De la misma forma que se configura los accesos en el sistema operativo, se debe también configurar los accesos y privilegios en la aplicación para que no todos los usuarios puedan modificar los servicios y aplicaciones, sino que únicamente las personas autorizadas puedan realizar cambios.

Para configurar determinados privilegios y accesos a sistemas y aplicaciones e instalaciones se debe definir roles, grupos localización física y tiempo en el día.

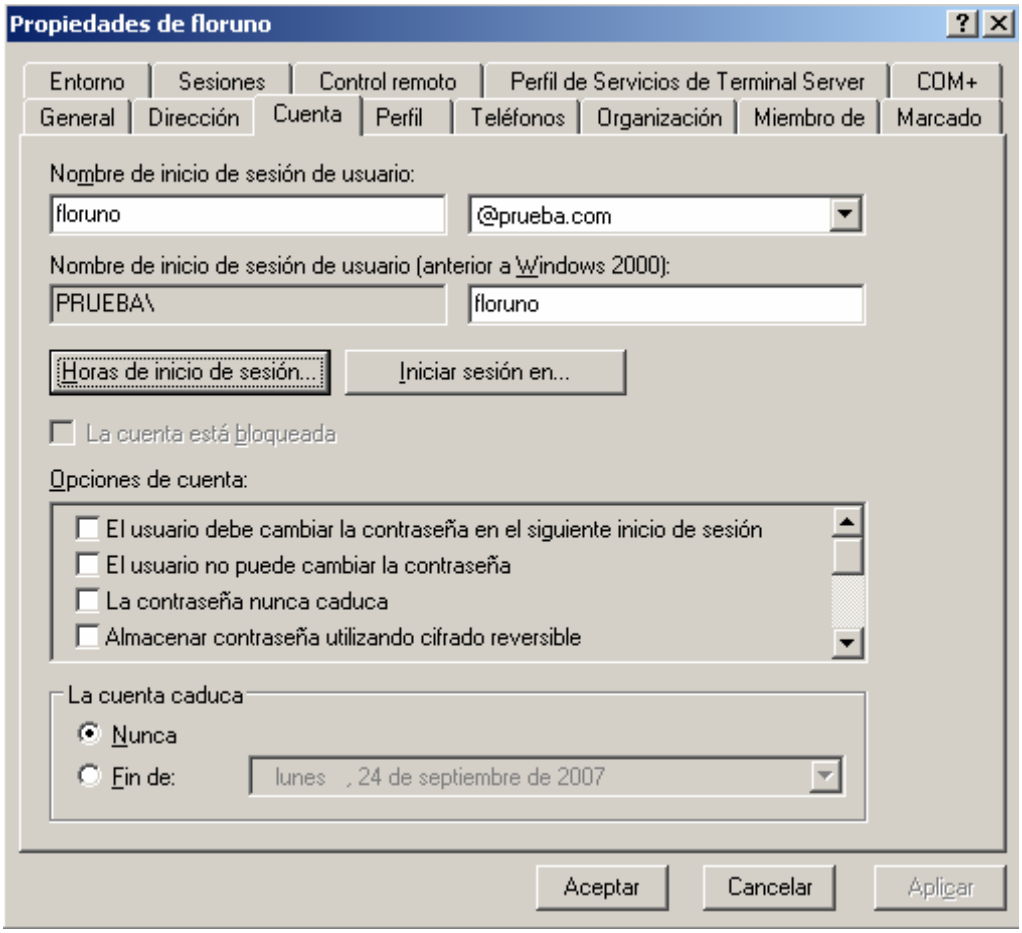
En Uniplex se puede definir diferentes tipos de grupos:

- Administrador
- Invitado
- Usuario estándar
- Usuario especial

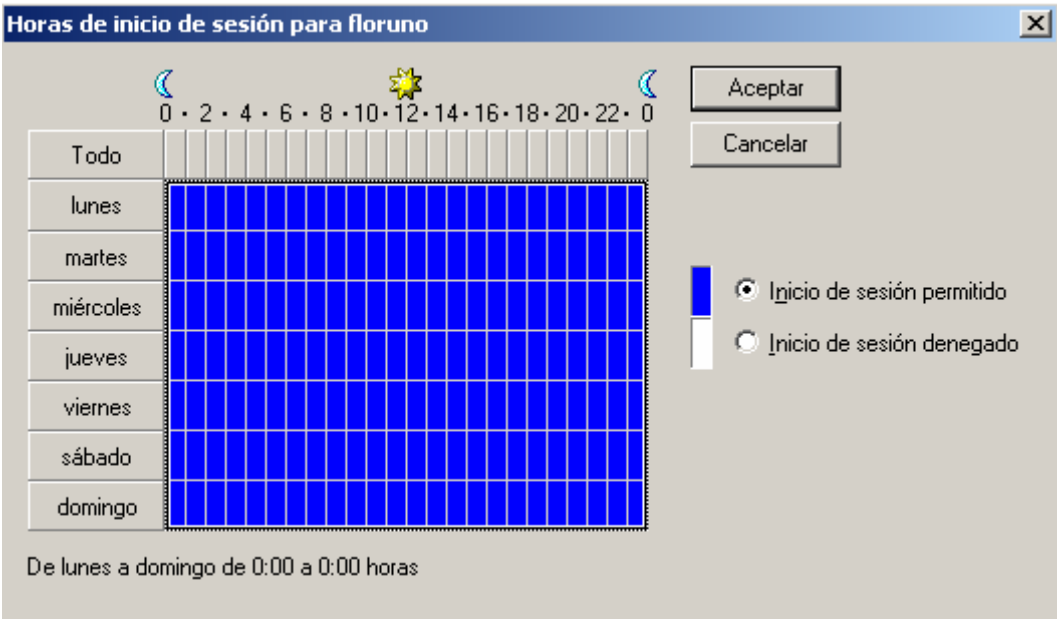
Cuando un nuevo usuario ingresa en la Corporación, el responsable de cada área debe definir los privilegios con los cuales el usuario va a contar, dependiendo de eso el administrador de la red va a configurar los permisos solicitados.

Para configurar usuarios con horarios específicos de acceso al dominio se debe configurar en el perfil del usuario como se determina a continuación:

1.- Seleccionar la opción Hora de Inicio de Sesión:



2.- En el cuadro que aparece se puede seleccionar los horarios para los cuales están limitados el acceso de dicho usuario:



Para todos los grupos, excepto el de Administrador los usuarios tienen restringidos la instalación, modificación eliminación de cualquier programa, no pueden utilizar Messenger a menos que el gerente apruebe la instalación y utilización del mismo.

La información de los usuarios solo se puede almacenar en la carpeta Mis documentos

ANEXO G

IMPLEMENTACIÓN DE SEGURIDAD EN EL SERVIDOR LOTUS

El servidor de IAS es aquel que cuenta con el aplicativo de Lotus Desarrollo al cual acceden los usuarios tanto internos como externos a realizar consultas, modificaciones de información necesaria para mantener actualizado los servicios que presta la unidad.
Debido a que el acceso a este aplicativo es mediante el internet, es necesario configurar una seguridad que permita que la información que viaja a través del internet se encuentre cifrada para que de esta manera se minimicen los riesgos.

Aprovechando las facilidades que presta el SO Windows 2003 se propone como solución la implementación de SSL, el cual permite que la información viaje encriptada a través de Internet, haciendo el uso de certificados digitales internos en la empresa, para de esta forma no afectar tanto a la economía de la organización y a los proveedores externos para que no tengan problemas a la hora de implementar esta solución.

Los pasos necesarios para realizar esta configuración son los siguientes:

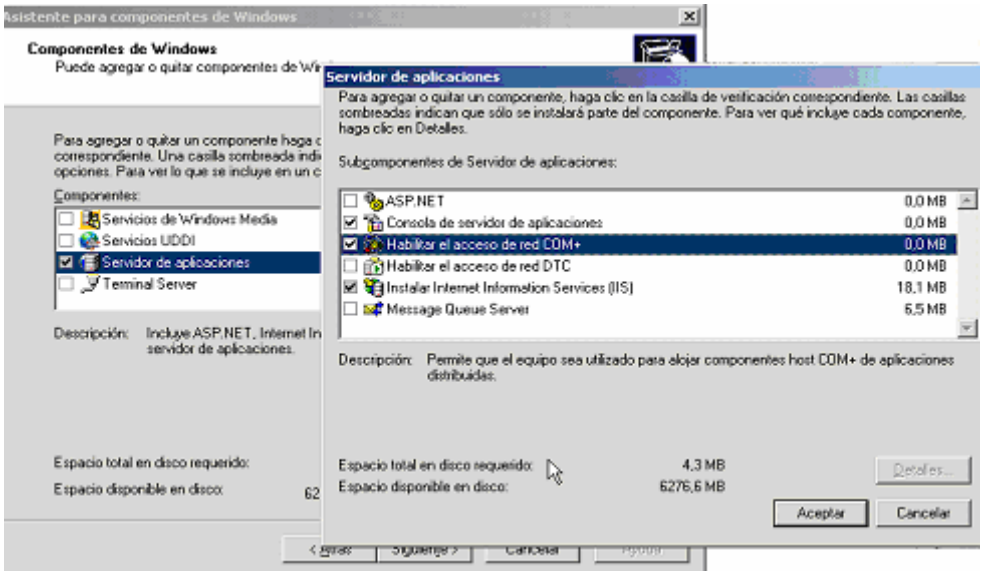
1.- implementación de una entidad certificadora:

La jerarquía que se va a utilizar es de una única entidad certificadora interna de la corporación pues el número de usuarios que acceden al aplicativo es menor que 100 usuarios, no es necesario realizar una implementación mayor, si bien se tiene un único punto de falla pues si deja de funcionar el servidor, deja de brindarse el servicio. No se considera

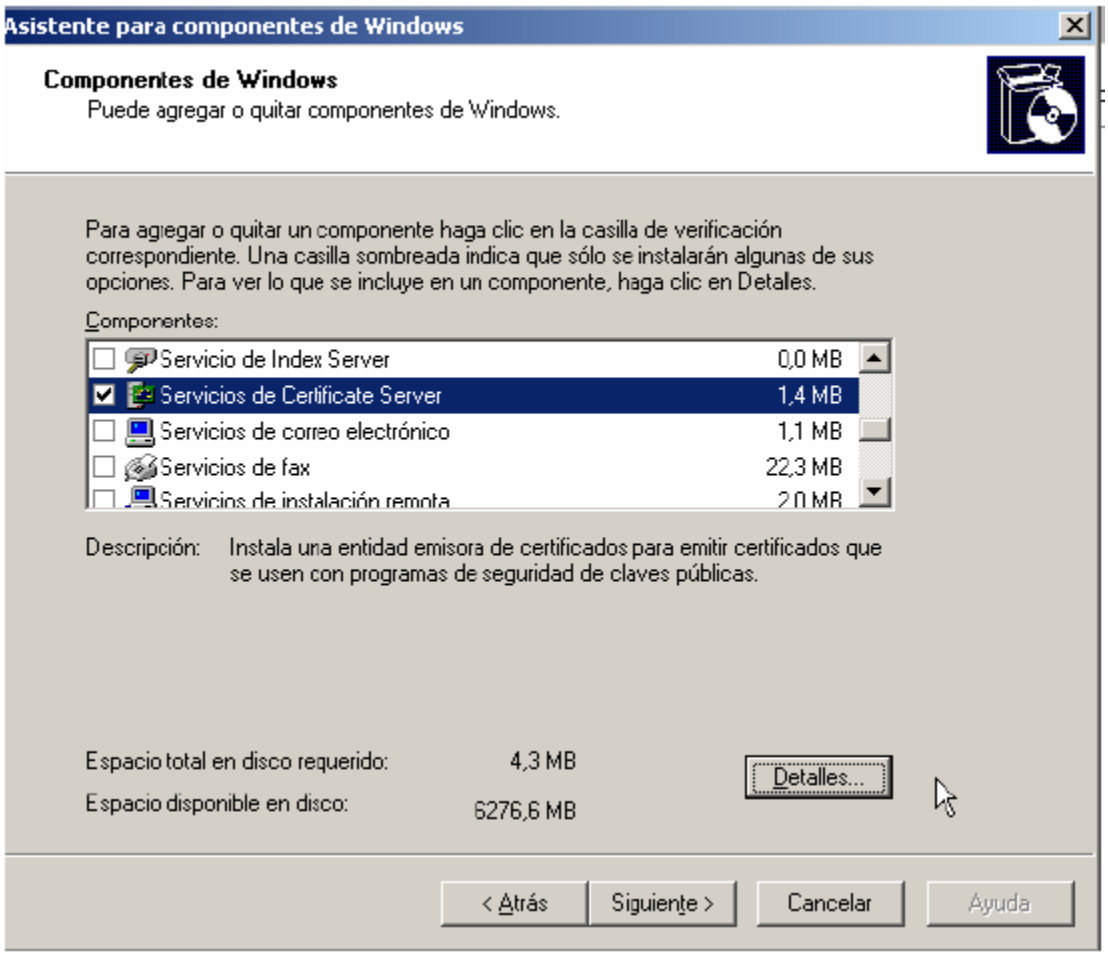
un punto de falla crítico pues actualmente se tiene implementado el servicio RAID –5+1, es decir un backup del disco del servidor en caso de que este falle.

Para configurar una entidad certificadora en el servidor, y de esta manera emitir un certificado para autenticar al servidor y encriptar la información que viaja desde y hacia el servidor es necesario.

1.1.- Instalar el servicio IIS en el servidor

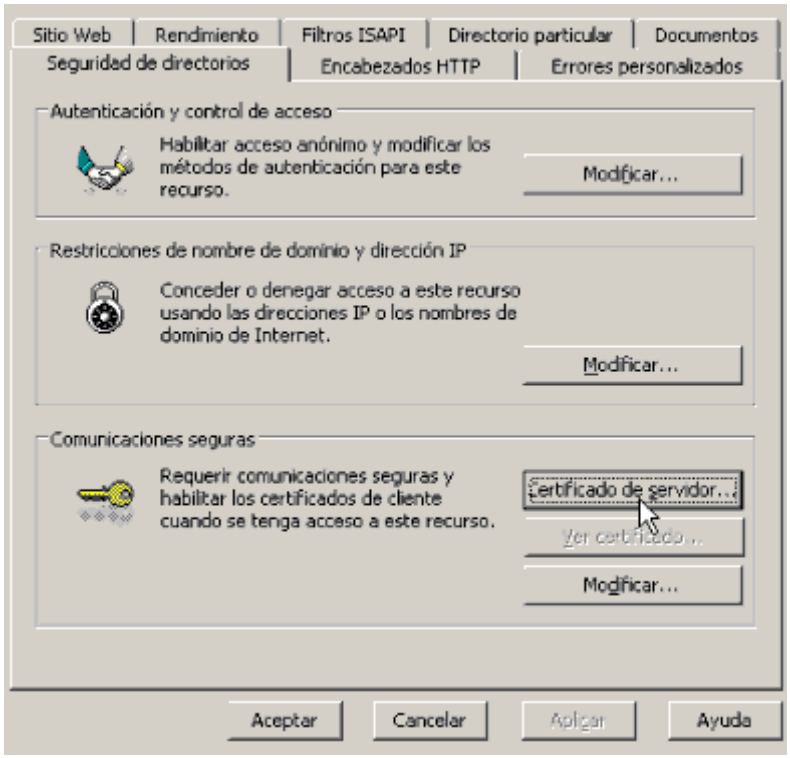


1.2.- Instalar la entidad emisora de certificados digitales



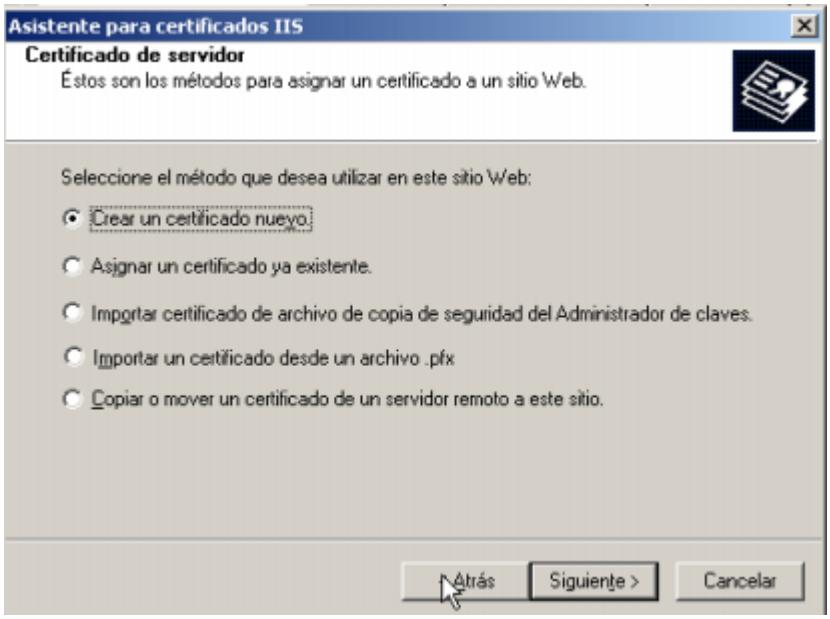
2.- Luego de tener configurado una entidad certificadora es necesario crear el certificado que va a permitir realizar la implementación del protocolo SSL en el aplicativo web. Para lo cual se debe realizar los siguientes pasos:

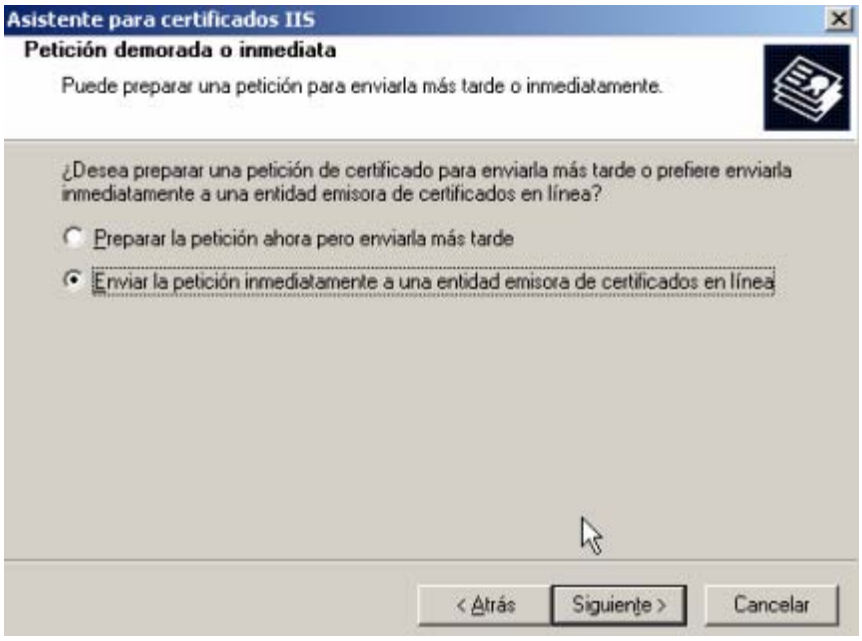
2.1 En la consola del IIS se selecciona el aplicativo sobre el cual se desea configurar el certificado, y se selecciona la pestaña seguridad de directorios, en la parte que se especifica comunicaciones seguras se selecciona Certificado de Servidor:



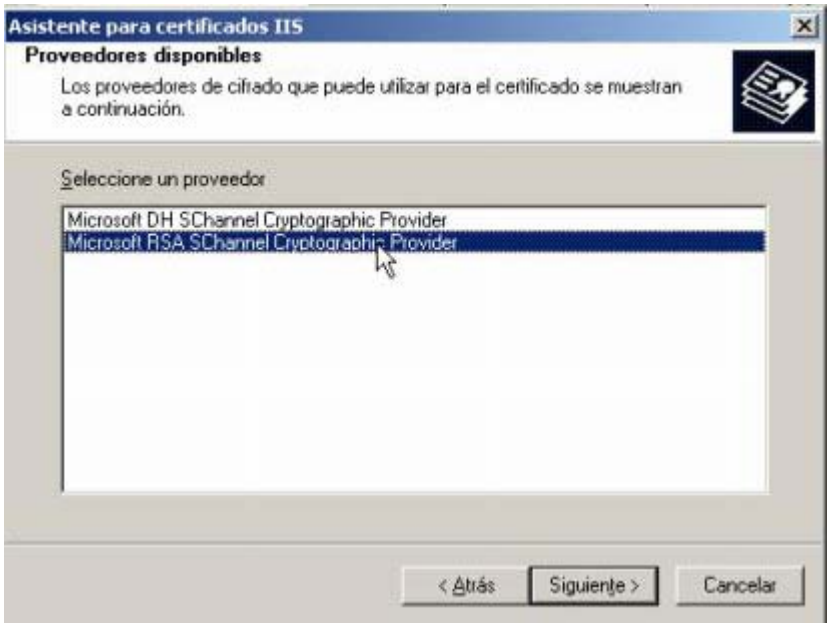
2.2.- En el asistente que aparece se solicita el certificado para el aplicativo, se adjunta los pasos:

Se debe seleccionar crear un nuevo certificado para el aplicativo y solicitarlo a la entidad emisora:

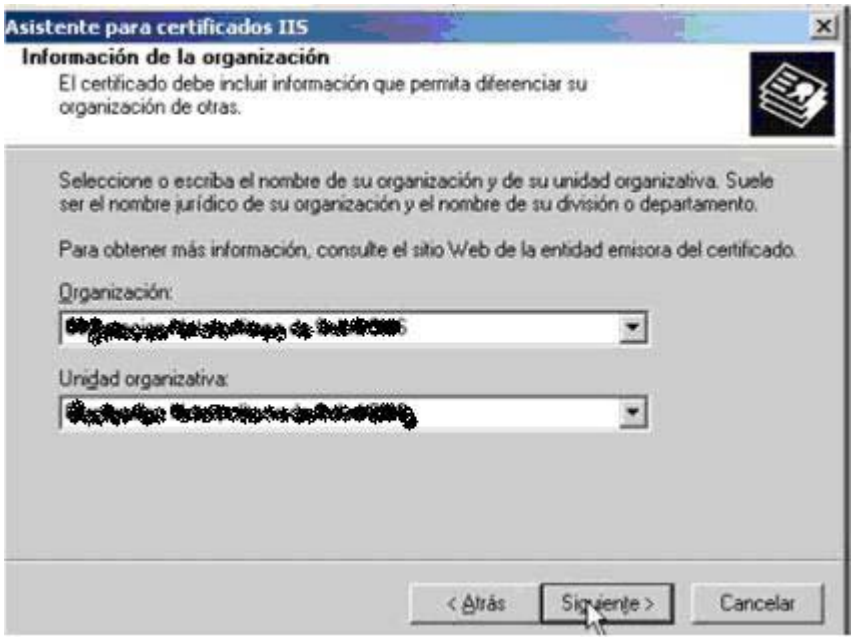




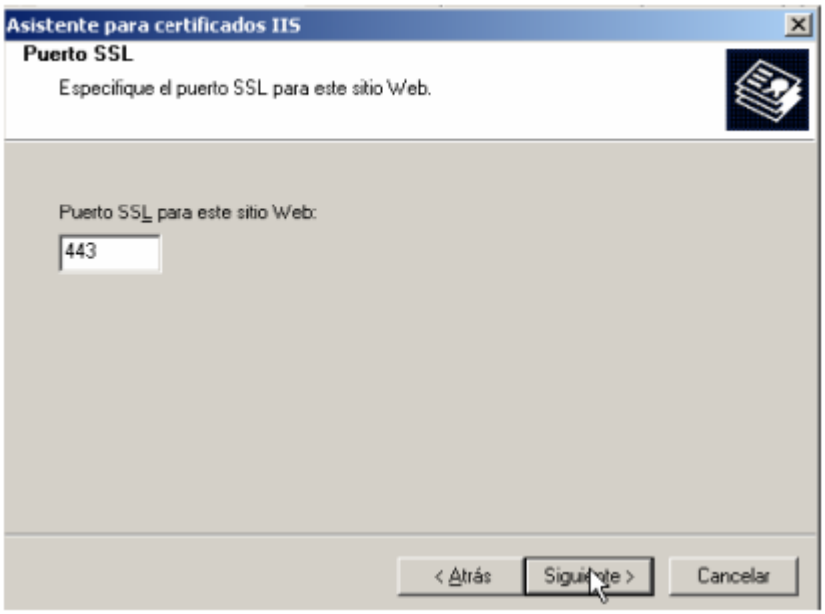
Es necesario indicar el nombre del certificado, así como la longitud de la clave para el cifrado, para una mejor seguridad seleccionamos una longitud de 1024 bits y controles criptográficos:



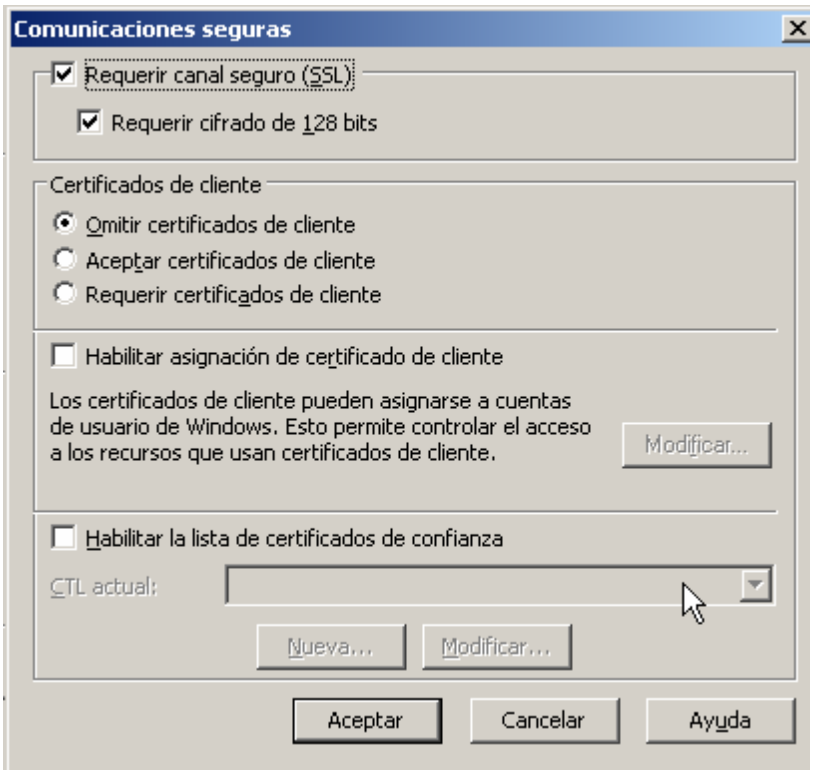
Se configura la información de la organización, así como el lugar de emisión del certificado:



Finalmente se configura el puerto para el Servidor Web con SSL, luego se selecciona el servidor del certificado:

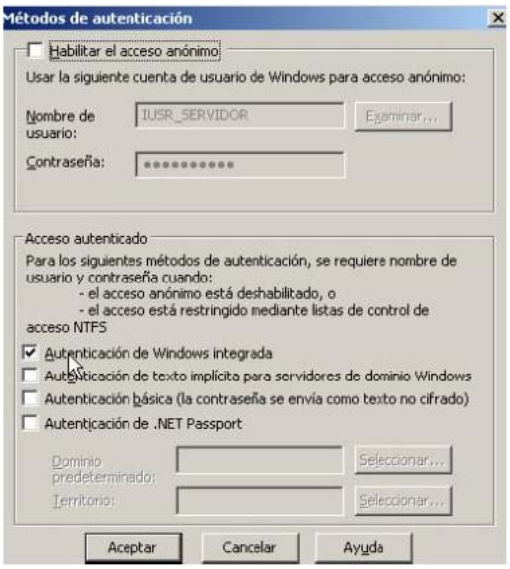


3.- Una vez configurado el certificado, se configura el aplicativo para que trabaje con un canal seguro como es SSL, con un cifrado de 128 bits, esto se selecciona en propiedades, en la pestaña Seguridad de directorios:



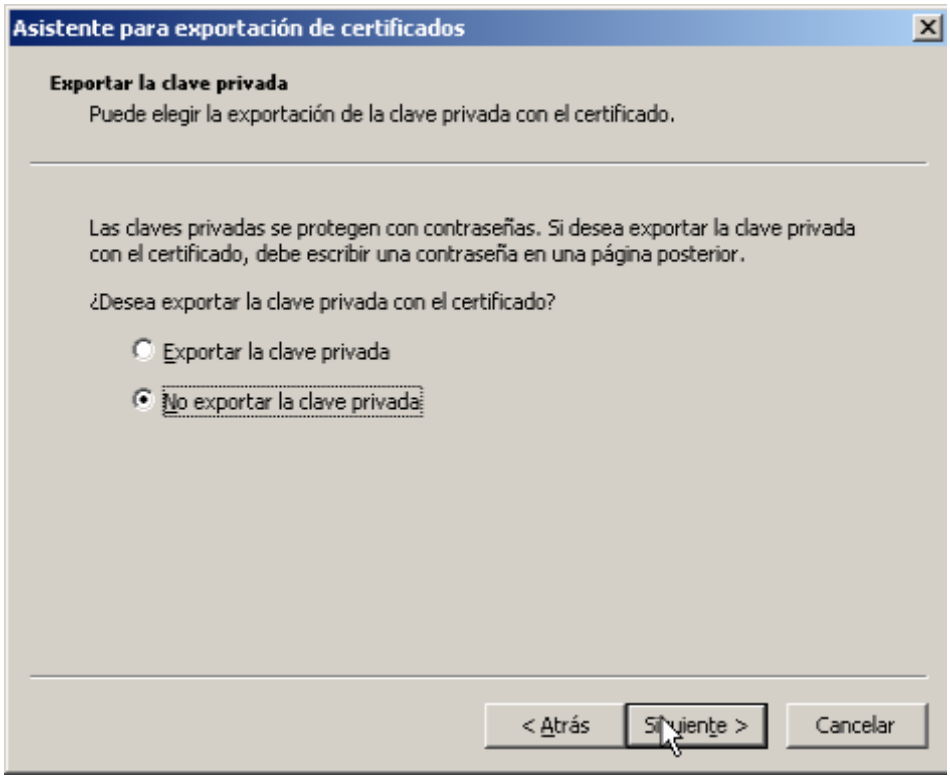
4.- Para implementar un control de acceso al aplicativo, se configuró lo siguiente:

4.1 En el Aplicativo al cual se le desea dar un nivel de control de acceso, se selecciona en propiedades la pestaña Seguridad de Directorio, en Autenticación y Control de Acceso y se configura lo siguiente:

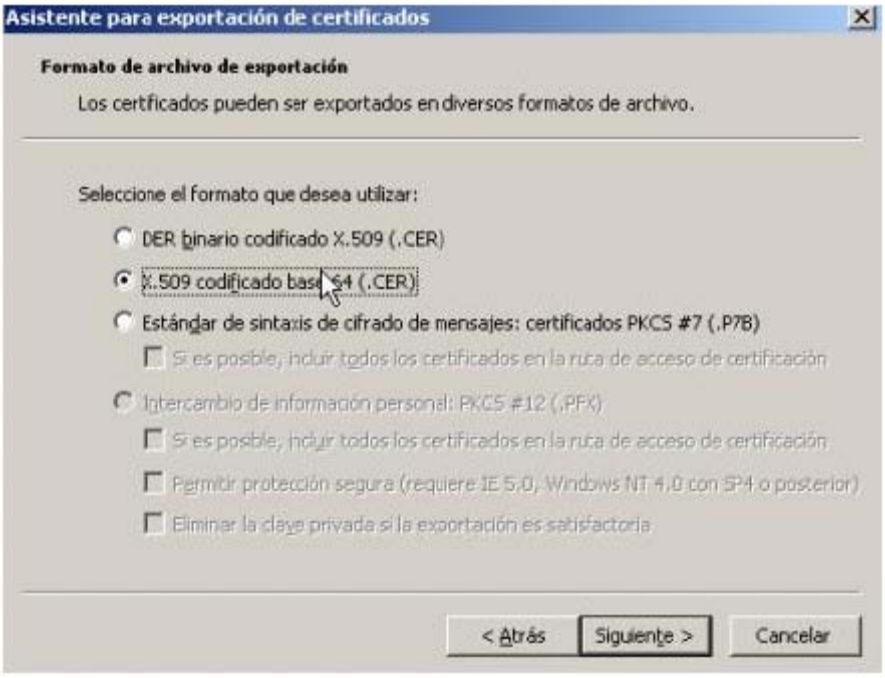


Para poder configurar este control de acceso, es necesario que se encuentren creados perfiles para los usuarios que van a acceder al servicio.

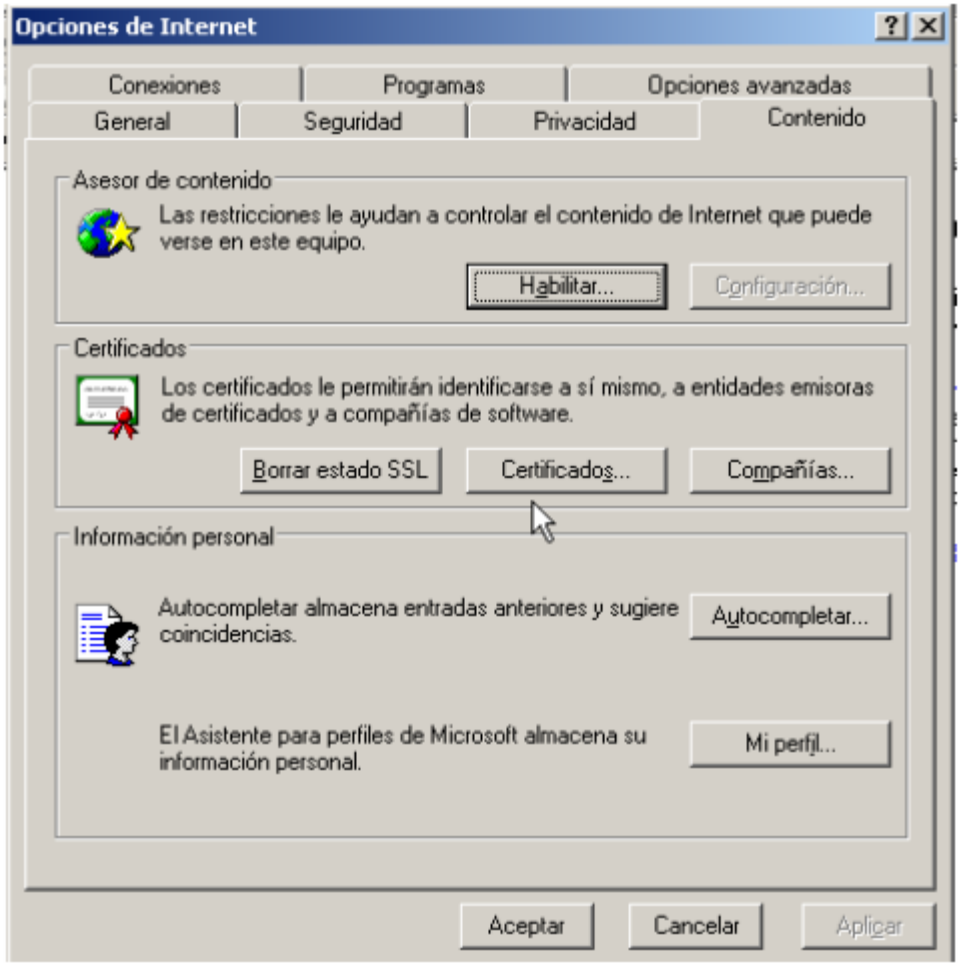
5.- Como paso final, es necesario importar el certificado para que el archivo se pueda configurar en los Exploradores de cada cliente, para lo cual es necesario seleccionar el certificado en la pestaña detalles y copiarlo en un archivo, luego se escoge la forma de exportar:



Se especifica el archivo de configuración y el nombre del Certificado que se va a copiar en los exploradores de los clientes:



6.- El último paso para poder realizar la comunicación segura entre el aplicativo del servidor y el cliente, se debe importar el certificado, de la siguiente manera en el explorador, como por ejemplo en el IE en Opciones de internet en la pestaña Contenido:

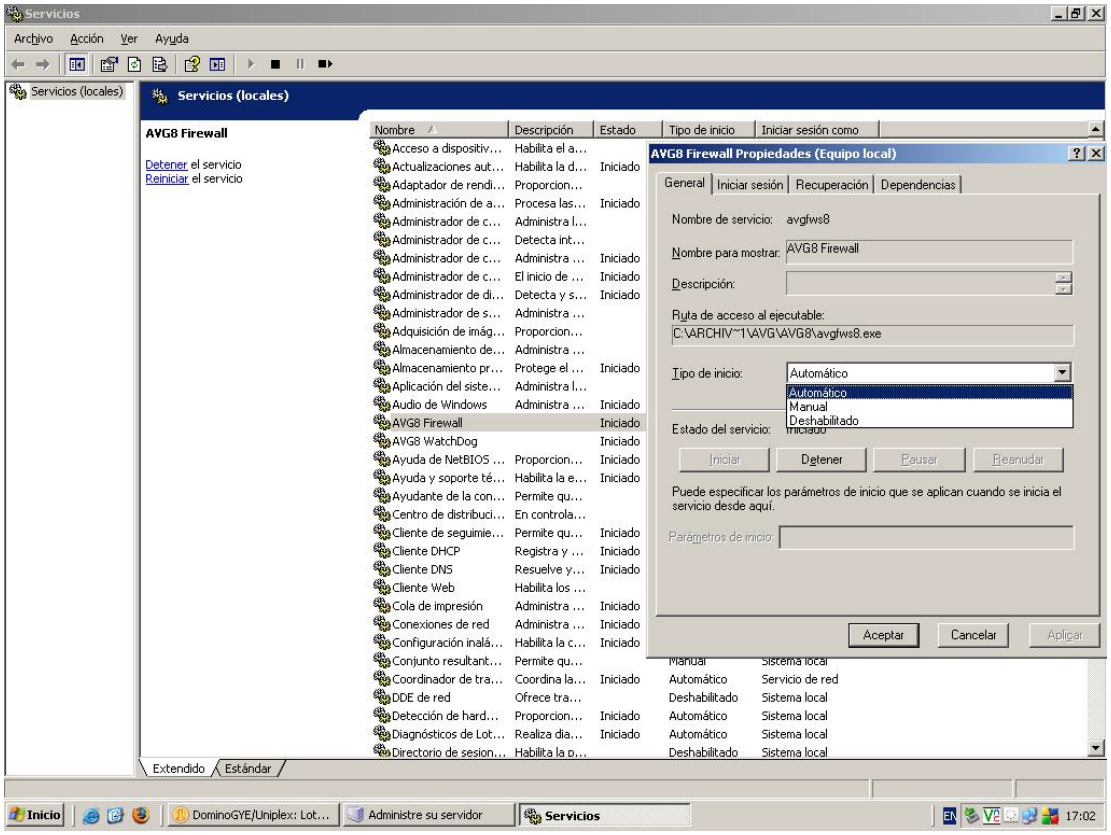


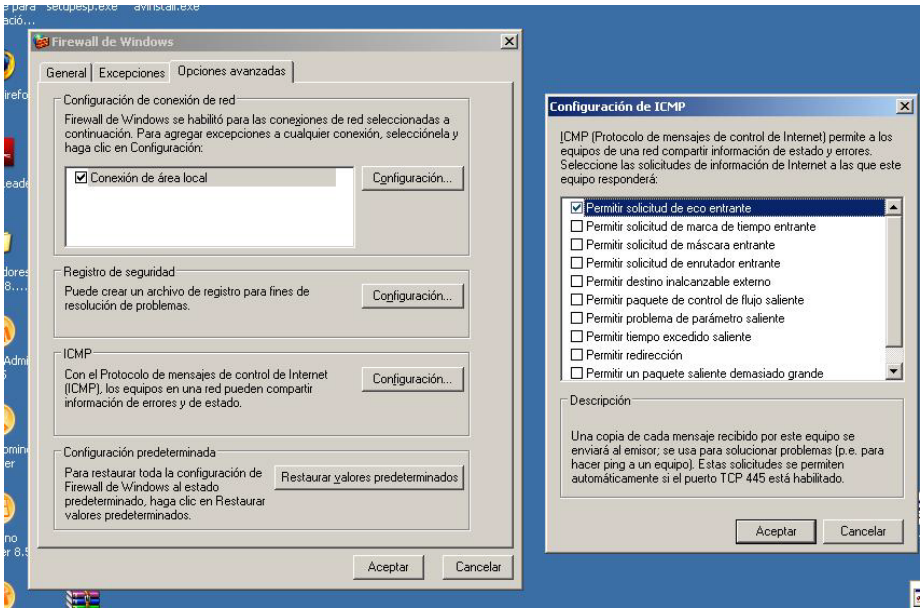
ANEXO H

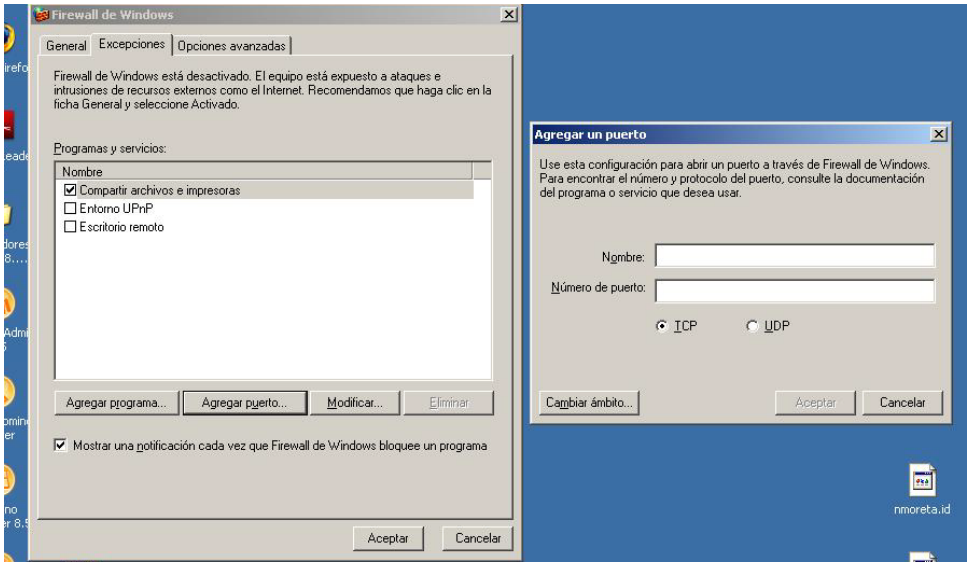
DESHABILITAR SERVICIOS Y PUERTOS INNECESARIOS

Para que un servidor sea más robusto, se debe deshabilitar cualquier servicio o puerto innecesario. Pues esto puede ser una vulnerabilidad crítica que puede ser explotada por usuarios no autorizados para cambiar información importante.

Bloquear Puertos




Firewall de Windows
General
Excepciones
Opciones avanzadas
Configuración de conexión de red
Firewall de Windows se habilitó para las conexiones de red seleccionadas a continuación. Para agregar excepciones a cualquier conexión, selecciónela y haga clic en Configuración:
Conexión de área local
Configuración...
Registro de seguridad
Puede crear un archivo de registro para fines de resolución de problemas.
Configuración...
ICMP
Con el Protocolo de mensajes de control de Internet (ICMP), los equipos en una red pueden compartir información de errores y de estado.
Configuración...
Configuración predeterminada
Para restaurar toda la configuración de Firewall de Windows al estado predeterminado, haga clic en Restaurar valores predeterminados.
Restaurar valores predeterminados
Aceptar
Cancelar
Configuración de ICMP
ICMP (Protocolo de mensajes de control de Internet) permite a los equipos de una red compartir información de estado y errores. Seleccione las solicitudes de información de Internet a las que este equipo responderá:
Permitir solicitud de eco entrante
Permitir solicitud de marca de tiempo entrante
Permitir solicitud de máscara entrante
Permitir solicitud de enrutador entrante
Permitir destino inalcanzable externo
Permitir paquete de control de flujo saliente
Permitir problema de parámetro saliente
Permitir tiempo excedido saliente
Permitir redirección
Permitir un paquete saliente demasiado grande
Descripción
Una copia de cada mensaje recibido por este equipo se enviará al emisor; se usa para solucionar problemas (p.e. para hacer ping a un equipo). Estas solicitudes se permiten automáticamente si el puerto TCP 445 está habilitado.
Aceptar
Cancelar


Firewall de Windows
General
Excepciones
Opciones avanzadas
Firewall de Windows está desactivado. El equipo está expuesto a ataques e intrusiones de recursos externos como el Internet. Recomendamos que haga clic en la ficha General y seleccione Activado.
Programas y servicios:
Nombre
Compartir archivos e impresoras
Entorno UPnP
Escritorio remoto
Agregar programa...
Agregar puerto...
Modificar...
Eliminar
Mostrar una notificación cada vez que Firewall de Windows bloquee un programa
Aceptar
Cancelar
Agregar un puerto
Use esta configuración para abrir un puerto a través de Firewall de Windows. Para encontrar el número y protocolo del puerto, consulte la documentación del programa o servicio que desea usar.
Nombre:
Número de puerto:
TCP
UDP
Cambiar ámbito...
Aceptar
Cancelar
nmoreta.id

Pero antes de proceder a bloquear puertos y aplicaciones hay que conocer cuales son los que están transcurriendo actualmente en la maquina sean estos servidores o Pc´s

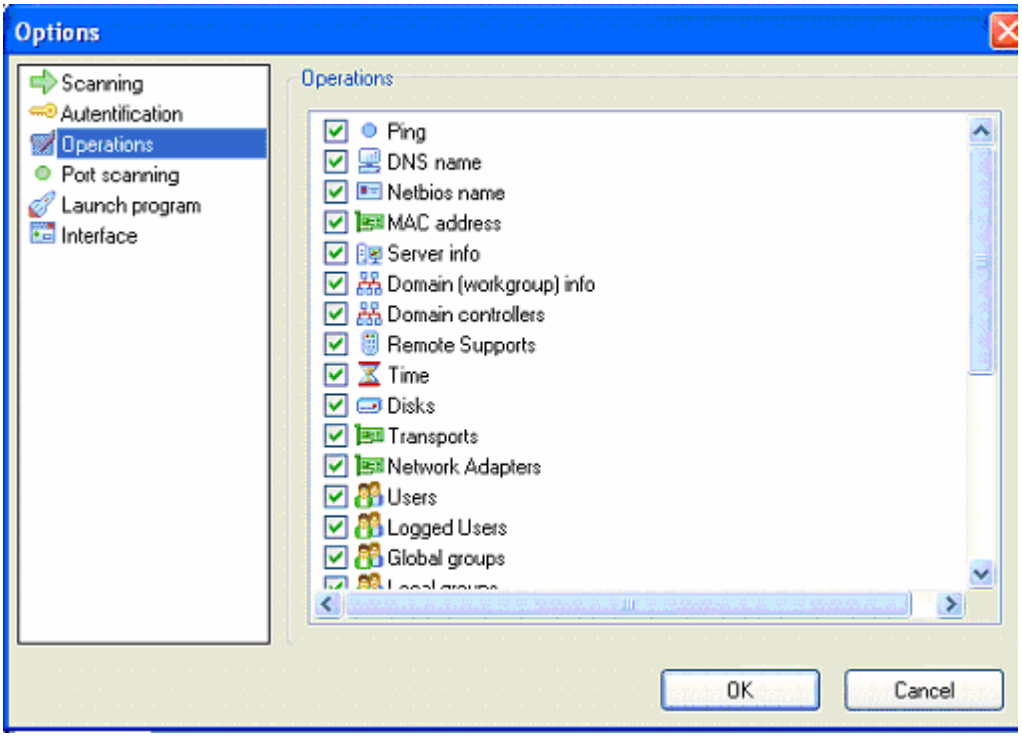
LANSPY

Esta herramienta permite la administración de la red, utilizando el protocolo SNMP que es necesario se encuentre levantado en todos los equipos de la red, tanto computadores como equipos de conectividad con esto podemos tener una mayor administración de la red.
Esta herramienta ofrece los siguientes beneficios:

- Realizar un ping de comprobación de conectividad de equipos
- Determinar la dirección Mac de los equipos
- Determinar recursos compartidos en la red
- Determinar la dirección IP interna y externa de cada dispositivo de la red
- Escuchar los puertos TCP abiertos y servicio de SNMP levantado
- Determinar usuarios actualmente registrados en la red.

Esta es una herramienta muy útil que permite además de realizar el monitoreo de la red, escasear los puertos que se encuentran abiertos en cada dispositivo de la red, e indica los servicios que están utilizando dichos puertos. Lo único que es necesario es definir el rango que se desea monitorear, con lo cual la herramienta empieza a escasear por todas las direcciones que ingresan dentro de ese rango, identifica aquellas que se encuentran apagadas, así como aquellas que se encuentran activas y los servicios de cada una.

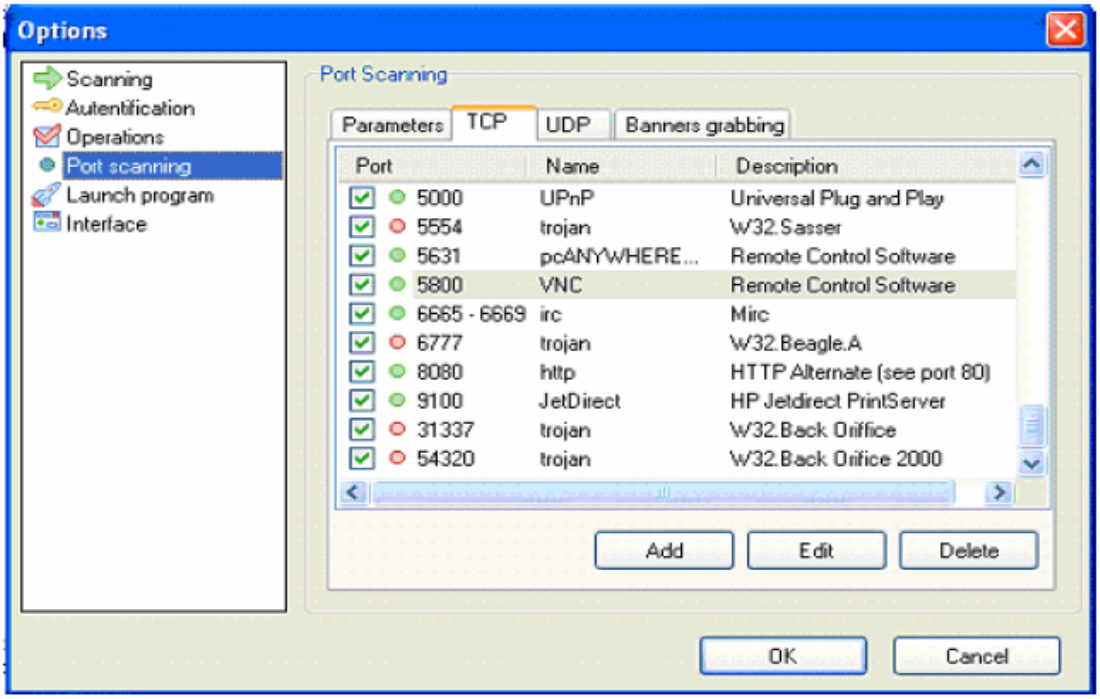
En la siguiente pantalla se muestra las operaciones que se pueden realizar con LANSPY:



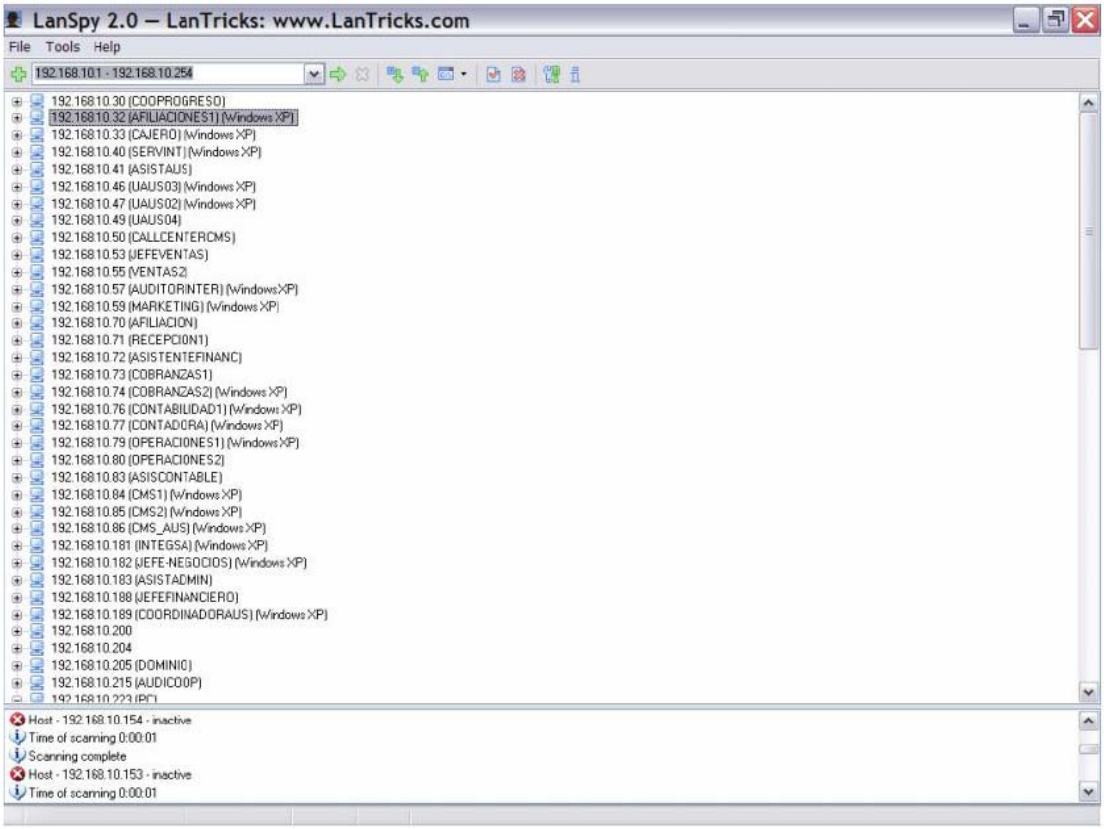
- Ping
- Domain name
- NetBios names
- MAC address
- Server information
- Domain (workgroup) information
- Domain controllers
- Remote control
- Time
- Disks
- Transports

- Users
- Logged users
- Global groups
- Local groups
- Security options
- Shared resources
- Sessions
- Open files
- Services
- Processes
- Registry
- Event log
- TCP port scanner
- UDP port scanner

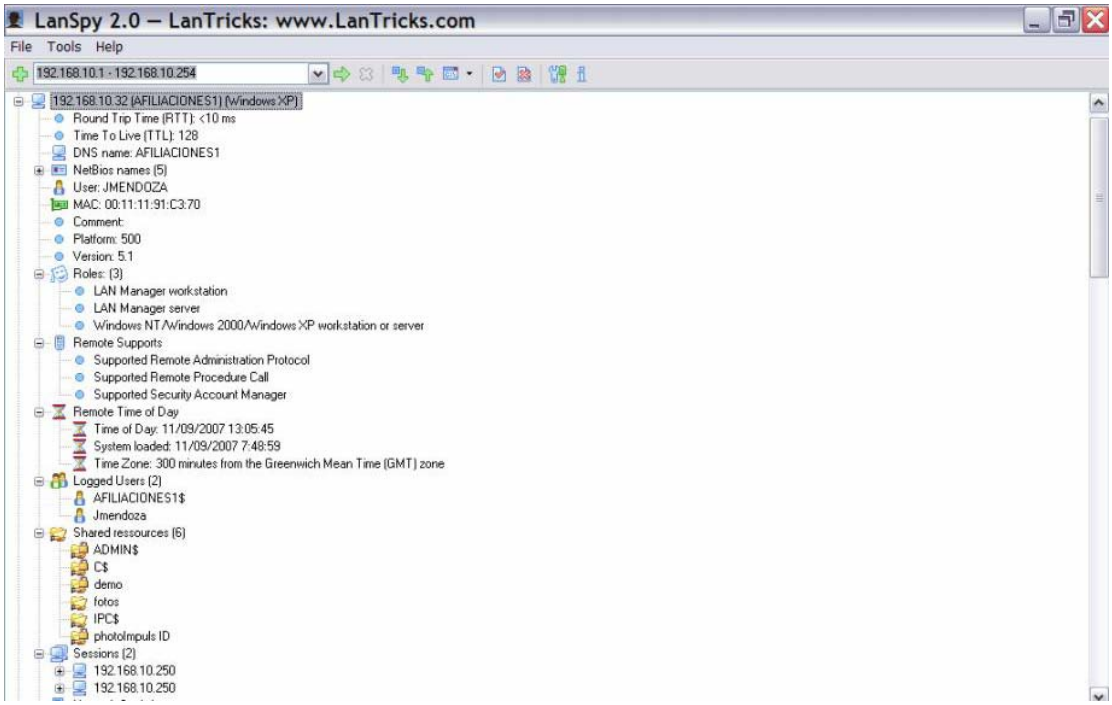
Para el escaneo de puertos, se encuentra una lista con los puertos, su respectivo nombre y su uso, como se muestra:



A continuación se presenta un ejemplo del resultado del escaneo de la red de la CMS utilizando LANSPY:



Si seleccionamos alguna máquina para ver la información, se puede obtener los siguientes datos:



LAN HELPER

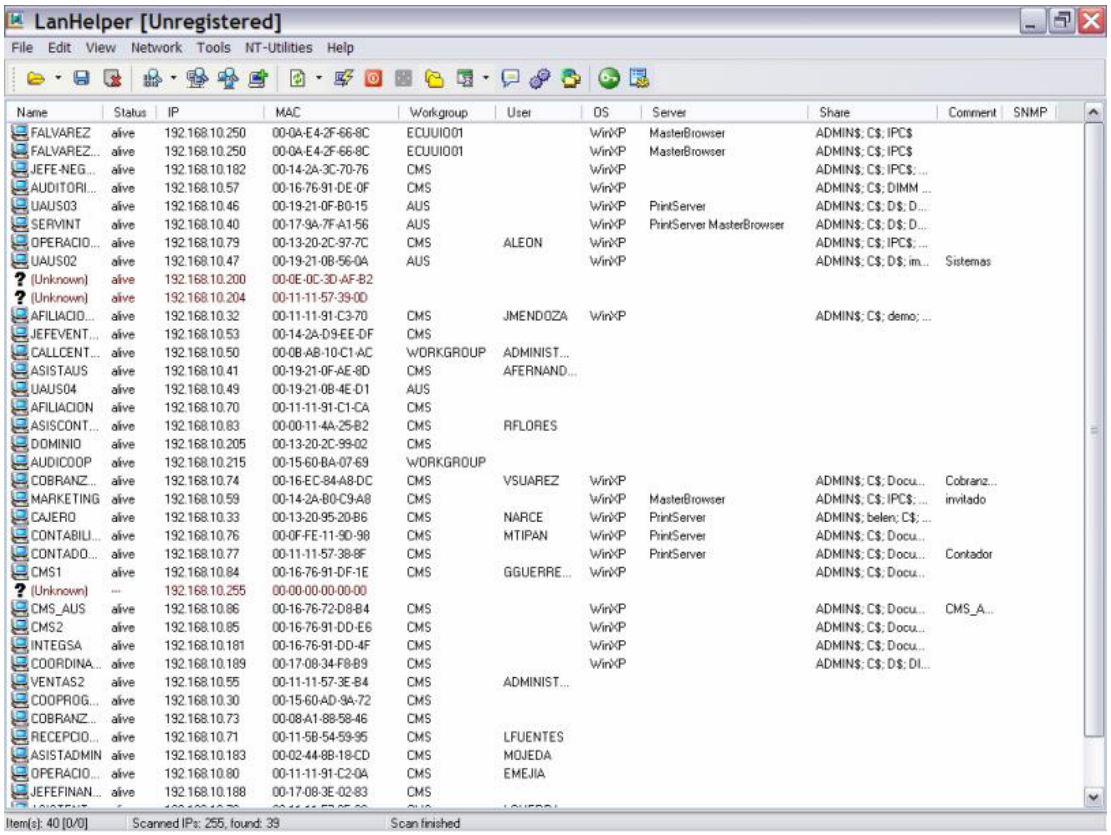
1.- Permite descubrir todas las computadoras disponibles en la red, mediante un rango de direcciones IP, multiples grupos y dominios. Además de coleccionar datos de la máquina como dirección IP, dirección MAC, SNMP, NetBIOS, etc.

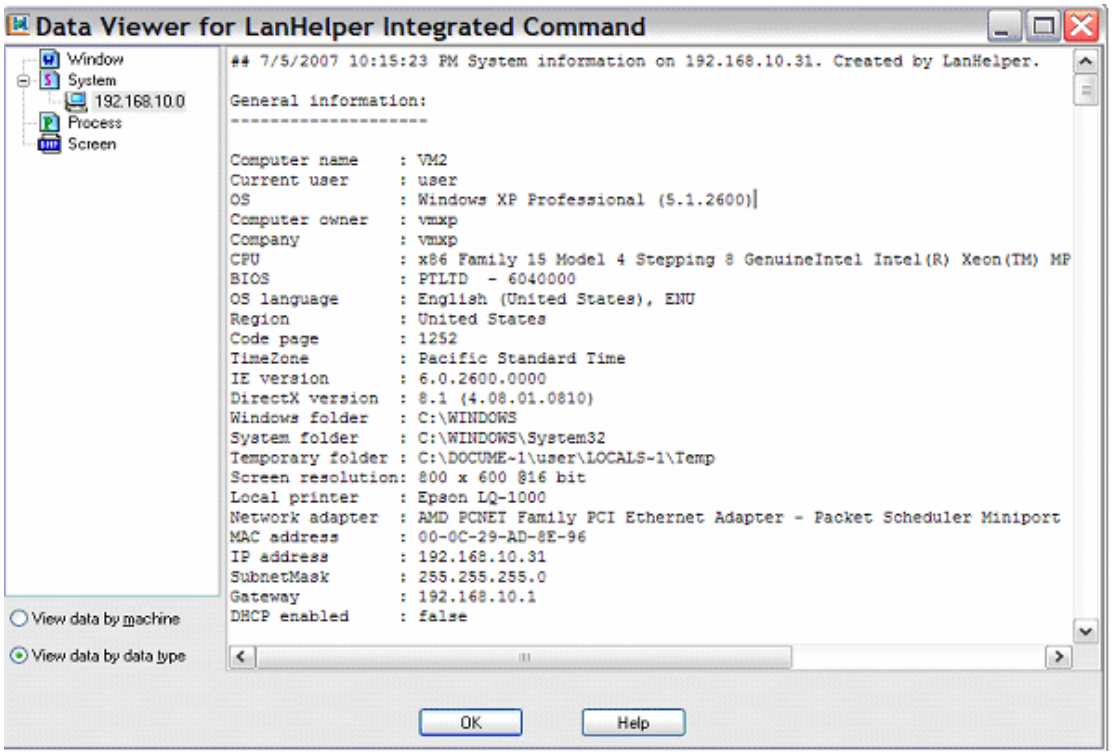
2.- Verifican que computadores se encuentran encendidos, y detecta si las direcciones IP han sido modificadas

3.- Monitorea la disponibilidad de servidores y estaciones de trabajo, cuando una falla ocurre, el aplicativo lo detecta y envía una alerta al administrador de red además de bootear inmediatamente las computadoras que se encuentran fallando.

4.- Permite la administración de los servicios, reiniciar, detener servicios, instalar y desinstalar servicios, de las diferentes computadoras fácilmente.

5.- identifica el identificador de la interfaz de red.





7/5/2007 10:15:23 PM System information on 192.168.10.31. Created by LanHelper.
General information:

Computer name : VM2
Current user : user
OS : Windows XP Professional (5.1.2600)
Computer owner : vmxp
Company : vmxp
CPU : x86 Family 15 Model 4 Stepping 8 GenuineIntel Intel(R) Xeon(TM) MP CPU 3.16GHz
BIOS : PTLTD - 6040000
OS language : English (United States), ENU
Region : United States
Code page : 1252
TimeZone : Pacific Standard Time
IE version : 6.0.2600.0000
DirectX version : 8.1 (4.08.01.0810)
Windows folder : C:\WINDOWS
System folder : C:\WINDOWS\System32
Temporary folder : C:\DOCUME~1\user\LOCALS~1\Temp
Screen resolution: 800 x 600 @16 bit
Local printer : Epson LQ-1000
Network adapter : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
MAC address : 00-0C-29-AD-8E-96
IP address : 192.168.10.31
SubnetMask : 255.255.255.0
Gateway : 192.168.10.1

DHCP enabled : false
Total physical memory : 261,616 KB
Available physical memory: 170,656 KB
Total page file : 633,368 KB
Available page file : 565,016 KB
Disk size on C:(NTFS) : 8,578 MB
Disk free space on C: : 6,403 MB
Disk size on D:(CDFS) : 512 MB
Disk free space on D: : 0 MB
Installed programs:

LanHelper v1.71
VMware Tools {3.1.0000}
WebFldrs XP {9.50.5318}
Installed computer devices:

Batteries -- Microsoft AC Adapter
Computer -- ACPI Uniprocessor PC
Disk drives -- VMware Virtual IDE Hard Drive
Display adapters -- VMware SVGA II
DVD/CD-ROM drives -- NECVMWar VMware IDE CDR10
Floppy disk controllers -- Standard floppy disk controller
Floppy disk drives -- Floppy disk drive
IDE ATA/ATAPI controllers -- Intel(r) 82371AB/EB PCI Bus Master IDE Controller
IDE ATA/ATAPI controllers -- Primary IDE Channel
IDE ATA/ATAPI controllers -- Secondary IDE Channel
Keyboards -- Standard 101/102-Key or Microsoft Natural PS/2 Keyboard
Mice and other pointing devices -- VMware Pointing Device
Network adapters -- AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport
Network adapters -- Direct Parallel
Network adapters -- VMware Accelerated AMD PCNet Adapter
Network adapters -- WAN Miniport (IP)
Network adapters -- WAN Miniport (IP) - Packet Scheduler Miniport
Network adapters -- WAN Miniport (L2TP)
Network adapters -- WAN Miniport (PPPOE)
Network adapters -- WAN Miniport (PPTP)
Ports (COM & LPT) -- Communications Port (COM1)
Ports (COM & LPT) -- Communications Port (COM2)
Ports (COM & LPT) -- Printer Port (LPT1)
Processors -- Intel(R) Xeon(TM) MP CPU 3.16GHz
SCSI and RAID controllers -- VMware SCSI Controller
Sound, video and game controllers -- Audio Codecs
Sound, video and game controllers -- Creative AudioPCI (ES1371,ES1373) (WDM)
Sound, video and game controllers -- Game Port for Creative
Sound, video and game controllers -- Legacy Audio Drivers
Sound, video and game controllers -- Legacy Video Capture Devices
Sound, video and game controllers -- Media Control Devices
Sound, video and game controllers -- Microsoft Kernel System Audio Device
Sound, video and game controllers -- Microsoft WINMM WDM Audio Compatibility Driver
Sound, video and game controllers -- Video Codecs
Storage volumes -- Generic volume

System devices -- ACPI Fixed Feature Button
System devices -- Direct memory access controller
System devices -- EISA programmable interrupt controller
System devices -- Generic Bus
System devices -- Intel 82371AB/EB PCI to ISA bridge (ISA mode)
System devices -- Intel 82443BX Pentium(r) II Processor to AGP Controller
System devices -- Intel 82443BX Pentium(r) II Processor to PCI Bridge
System devices -- ISAPNP Read Data Port
System devices -- Logical Disk Manager
System devices -- Microcode Update Device
System devices -- Microsoft ACPI-Compliant System
System devices -- Microsoft Composite Battery
System devices -- Motherboard resources
System devices -- PCI bus
System devices -- PCI standard PCI-to-PCI bridge
System devices -- Plug and Play Software Device Enumerator
System devices -- Printer Port Logical Interface
System devices -- System CMOS/real time clock
System devices -- System speaker
System devices -- System timer
System devices -- Terminal Server Device Redirector
System devices -- Terminal Server Keyboard Driver
System devices -- Terminal Server Mouse Driver
System devices -- Volume Manager
Universal Serial Bus controllers -- Intel(r) 82371AB/EB PCI to USB Universal Host Controller
Universal Serial Bus controllers -- USB Root Hub
The programs start up with Windows:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\
"VMware Tools" = "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
"VMware User Process" = "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
"kernelfaultcheck" = "C:\WINDOWS\system32\dumprep 0 -k"
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\
"MSMSGS" = ""C:\Program Files\Messenger\msmsgs.exe" /background"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\
Shell = "Explorer.exe"
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\
Userinit = "C:\WINDOWS\system32\userinit.exe,"
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager\
BootExecute = "autocheck autochk * u t o c h k *"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\Notify\
"crypt32chain" = "crypt32.dll"
"cryptnet" = "cryptnet.dll"
"cscdll" = "cscdll.dll"
"ScCertProp" = "wlnotify.dll"
"Schedule" = "wlnotify.dll"
"sclgntfy" = "sclgntfy.dll"
"SensLogn" = "WlNotify.dll"
"termsrv" = "wlnotify.dll"
"wlballoon" = "wlnotify.dll"

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\
"Browser Customizations" = "RunDLL32 IEDKCS32.DLL,BrandIE4 SIGNUP"
"Microsoft Windows Media Player 6.4" = "rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\mplayer2.inf,PerUserStub.NT"
"themes setup" = "C:\WINDOWS\system32\regsvr32.exe /s /n /i:/userinstall
C:\WINDOWS\system32\themeui.dll"
"microsoft outlook express 6" = ""C:\Program Files\outlook express\setup50.exe" /app:oe
/caller:winnt /user /install"
"NetMeeting 3.01" = "rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\msnetmtg.inf,NetMtg.Install.PerUser.NT"
"Windows Messenger 4.0" = "rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\msmsgs.inf,BLC.Install.PerUser"
"Microsoft Windows Media Player 8" = "rundll32.exe advpack.dll,LaunchINFSection
C:\WINDOWS\INF\wmp.inf,PerUserStub"
"address book 6" = ""C:\Program Files\outlook express\setup50.exe" /app:wab /caller:winnt /user
/install"
"Windows Desktop Update" = "regsvr32.exe /s /n /i:U shell32.dll"
"internet explorer 6" = "C:\WINDOWS\system32\ie4uinit.exe"
"Internet Explorer Access" = "rundll32 iesetup.dll,IEAccessUserInst"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SharedTaskS
cheduler\
"browseui preloader" = "C:\WINDOWS\system32\browseui.dll"
"component categories cache daemon" = "C:\WINDOWS\system32\browseui.dll"
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellServiceObjectDel
ayLoad\
"postbootreminder" = "C:\WINDOWS\system32\shell32.dll"
"cdburn" = "C:\WINDOWS\system32\shell32.dll"
"webcheck" = "C:\WINDOWS\system32\webcheck.dll"
"SysTray" = "C:\WINDOWS\System32\stobject.dll"
All services on this machine:

Service: Alerter -- Alerter
Path : C:\WINDOWS\System32\svchost.exe -k LocalService (%SystemRoot%\system32\alrsvc.dll)
Manual, Stopped
Service: ALG -- Application Layer Gateway Service
Path : C:\WINDOWS\System32\alg.exe
Manual, Stopped
Service: AppMgmt -- Application Management
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs (%SystemRoot%\System32\appmgmts.dll)
Manual, Stopped
Service: AudioSrv -- Windows Audio
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\audiosrv.dll)
Automatic, Running
Service: BITS -- Background Intelligent Transfer Service
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (C:\WINDOWS\System32\qmgr.dll)
Manual, Stopped
Service: Browser -- Computer Browser
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\browser.dll)
Automatic, Running
Service: cisvc -- Indexing Service
Path : C:\WINDOWS\System32\cisvc.exe

Manual, Stopped
Service: ClipSrv -- ClipBook
Path : C:\WINDOWS\system32\clipsrv.exe
Manual, Stopped
Service: COMSysApp -- COM+ System Application
Path : C:\WINDOWS\System32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
Manual, Stopped
Service: CryptSvc -- Cryptographic Services
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs (%SystemRoot%\System32\cryptsvc.dll)
Automatic, Running
Service: Dhcp -- DHCP Client
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\dhcpcsvc.dll)
Automatic, Running
Service: dmadmin -- Logical Disk Manager Administrative Service
Path : C:\WINDOWS\System32\dmadmin.exe /com
Manual, Stopped
Service: dmserver -- Logical Disk Manager
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\dmserver.dll)
Automatic, Running
Service: Dnscache -- DNS Client
Path : C:\WINDOWS\System32\svchost.exe -k NetworkService (%SystemRoot%\System32\dnsrslvr.dll)
Automatic, Running
Service: ERSvc -- Error Reporting Service
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\ersvc.dll)
Automatic, Running
Service: Eventlog -- Event Log
Path : C:\WINDOWS\system32\services.exe
Automatic, Running
Service: EventSystem -- COM+ Event System
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (C:\WINDOWS\System32\es.dll)
Manual, Running
Service: FastUserSwitchingCompatibility -- Fast User Switching Compatibility
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\shsvcs.dll)
Manual, Running
Service: helpsvc -- Help and Support
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%WINDIR%\PCHealth\HelpCtr\Binaries\pchsvc.dll)
Automatic, Running
Service: HidServ -- Human Interface Device Access
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\hidserv.dll)
Disabled, Stopped
Service: ImapiService -- IMAPI CD-Burning COM Service
Path : C:\WINDOWS\System32\imapi.exe
Manual, Stopped
Service: lanmanserver -- Server
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\srvsvc.dll)
Automatic, Running
Service: lanmanworkstation -- Workstation
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\wkssvc.dll)

Automatic, Running
Service: LmHosts -- TCP/IP NetBIOS Helper
Path : C:\WINDOWS\System32\svchost.exe -k LocalService (%SystemRoot%\System32\lmhsvc.dll)
Automatic, Running
Service: Messenger -- Messenger
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\msgsvc.dll)
Automatic, Running
Service: mnmsrvc -- NetMeeting Remote Desktop Sharing
Path : C:\WINDOWS\System32\mnmsrvc.exe
Manual, Stopped
Service: MSDTC -- Distributed Transaction Coordinator
Path : C:\WINDOWS\System32\msdtc.exe
Manual, Stopped
Service: MSIServer -- Windows Installer
Path : C:\WINDOWS\System32\msiexec.exe /V
Manual, Stopped
Service: NetDDE -- Network DDE
Path : C:\WINDOWS\system32\netdde.exe
Manual, Stopped
Service: NetDDEdsdm -- Network DDE DSDM
Path : C:\WINDOWS\system32\netdde.exe
Manual, Stopped
Service: Netlogon -- Net Logon
Path : C:\WINDOWS\System32\lsass.exe
Manual, Stopped
Service: Netman -- Network Connections
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\netman.dll)
Manual, Running
Service: Nla -- Network Location Awareness (NLA)
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\mswsock.dll)
Manual, Running
Service: NtLmSsp -- NT LM Security Support Provider
Path : C:\WINDOWS\System32\lsass.exe
Manual, Stopped
Service: NtmsSvc -- Removable Storage
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs (%SystemRoot%\system32\ntmssvc.dll)
Manual, Stopped
Service: PlugPlay -- Plug and Play
Path : C:\WINDOWS\system32\services.exe
Automatic, Running
Service: PolicyAgent -- IPSEC Services
Path : C:\WINDOWS\System32\lsass.exe
Automatic, Running
Service: ProtectedStorage -- Protected Storage
Path : C:\WINDOWS\system32\lsass.exe
Automatic, Running
Service: RasAuto -- Remote Access Auto Connection Manager
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\rasauto.dll)
Manual, Stopped
Service: RasMan -- Remote Access Connection Manager
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\rasmans.dll)

Manual, Stopped
Service: RDSessMgr -- Remote Desktop Help Session Manager
Path : C:\WINDOWS\system32\sessmgr.exe
Manual, Stopped
Service: RemoteAccess -- Routing and Remote Access
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\mprdim.dll)
Disabled, Stopped
Service: RemoteRegistry -- Remote Registry
Path : C:\WINDOWS\system32\svchost.exe -k LocalService (%SystemRoot%\system32\regsvc.dll)
Automatic, Running
Service: RpcLocator -- Remote Procedure Call (RPC) Locator
Path : C:\WINDOWS\System32\locator.exe
Manual, Stopped
Service: RpcSs -- Remote Procedure Call (RPC)
Path : C:\WINDOWS\system32\svchost -k rpcss (%SystemRoot%\system32\rpcss.dll)
Automatic, Running
Service: RSVP -- QoS RSVP
Path : C:\WINDOWS\System32\rsvp.exe
Manual, Stopped
Service: SamSs -- Security Accounts Manager
Path : C:\WINDOWS\system32\lsass.exe
Automatic, Running
Service: SCardDrv -- Smart Card Helper
Path : C:\WINDOWS\System32\SCardSvr.exe
Manual, Stopped
Service: SCardSvr -- Smart Card
Path : C:\WINDOWS\System32\SCardSvr.exe
Manual, Stopped
Service: Schedule -- Task Scheduler
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\system32\schedsvc.dll)
Automatic, Running
Service: seclogon -- Secondary Logon
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\seclogon.dll)
Automatic, Running
Service: SENS -- System Event Notification
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs (%SystemRoot%\system32\sens.dll)
Automatic, Running
Service: SharedAccess -- Internet Connection Firewall (ICF) / Internet Connection Sharing (ICS)
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\ipnathlp.dll)
Manual, Stopped
Service: ShellHWDetection -- Shell Hardware Detection
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\shsvcs.dll)
Automatic, Running
Service: Spooler -- Print Spooler
Path : C:\WINDOWS\system32\spoolsv.exe
Automatic, Running
Service: srservice -- System Restore Service
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (C:\WINDOWS\System32\srsvc.dll)
Automatic, Running
Service: SSDPSRV -- SSDP Discovery Service
Path : C:\WINDOWS\System32\svchost.exe -k LocalService (%SystemRoot%\System32\ssdpsrv.dll)

Manual, Running
Service: stisvc -- Windows Image Acquisition (WIA)
Path : C:\WINDOWS\System32\svchost.exe -k imgsvc (%SystemRoot%\system32\wiaservc.dll)
Manual, Stopped
Service: SwPrv -- MS Software Shadow Copy Provider
Path : C:\WINDOWS\System32\dllhost.exe /Processid:{3996C149-0A2A-4E22-B0DC-5B489772950E}
Manual, Stopped
Service: SysmonLog -- Performance Logs and Alerts
Path : C:\WINDOWS\system32\smlogsvc.exe
Manual, Stopped
Service: TapiSrv -- Telephony
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\tapisrv.dll)
Manual, Stopped
Service: TermService -- Terminal Services
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\termsrv.dll)
Manual, Running
Service: Themes -- Themes
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\shsvcs.dll)
Automatic, Running
Service: TlntSvr -- Telnet
Path : C:\WINDOWS\System32\tlntsvr.exe
Manual, Stopped
Service: TrkWks -- Distributed Link Tracking Client
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs (%SystemRoot%\system32\trkwks.dll)
Automatic, Running
Service: uploadmgr -- Upload Manager
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%WINDIR%\PCHealth\HelpCtr\Binaries\pchsvc.dll)
Automatic, Running
Service: upnphost -- Universal Plug and Play Device Host
Path : C:\WINDOWS\System32\svchost.exe -k LocalService (%SystemRoot%\System32\upnphost.dll)
Manual, Stopped
Service: UPS -- Uninterruptible Power Supply
Path : C:\WINDOWS\System32\ups.exe
Manual, Stopped
Service: VMTools -- VMware Tools Service
Path : C:\Program Files\VMware\VMware Tools\VMwareService.exe
Automatic, Running
Service: VSS -- Volume Shadow Copy
Path : C:\WINDOWS\System32\vssvc.exe
Manual, Stopped
Service: W32Time -- Windows Time
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (C:\WINDOWS\System32\w32time.dll)
Automatic, Running
Service: WebClient -- WebClient
Path : C:\WINDOWS\System32\svchost.exe -k LocalService (%SystemRoot%\System32\webclnt.dll)
Automatic, Running
Service: winmgmt -- Windows Management Instrumentation
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs

(%SystemRoot%\system32\wbem\WMIsvc.dll)
Automatic, Running
Service: WmdmPmSp -- Portable Media Serial Number
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (C:\WINDOWS\System32\mspmspsv.dll)
Automatic, Running
Service: Wmi -- Windows Management Instrumentation Driver Extensions
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\advapi32.dll)
Manual, Stopped
Service: WmiApSrv -- WMI Performance Adapter
Path : C:\WINDOWS\System32\wbem\wmiapsrv.exe
Manual, Stopped
Service: wuauserv -- Automatic Updates
Path : C:\WINDOWS\system32\svchost.exe -k netsvcs (C:\WINDOWS\System32\wuauserv.dll)
Automatic, Running
Service: WZCSVC -- Wireless Zero Configuration
Path : C:\WINDOWS\System32\svchost.exe -k netsvcs (%SystemRoot%\System32\wzcsvc.dll)
Automatic, Running

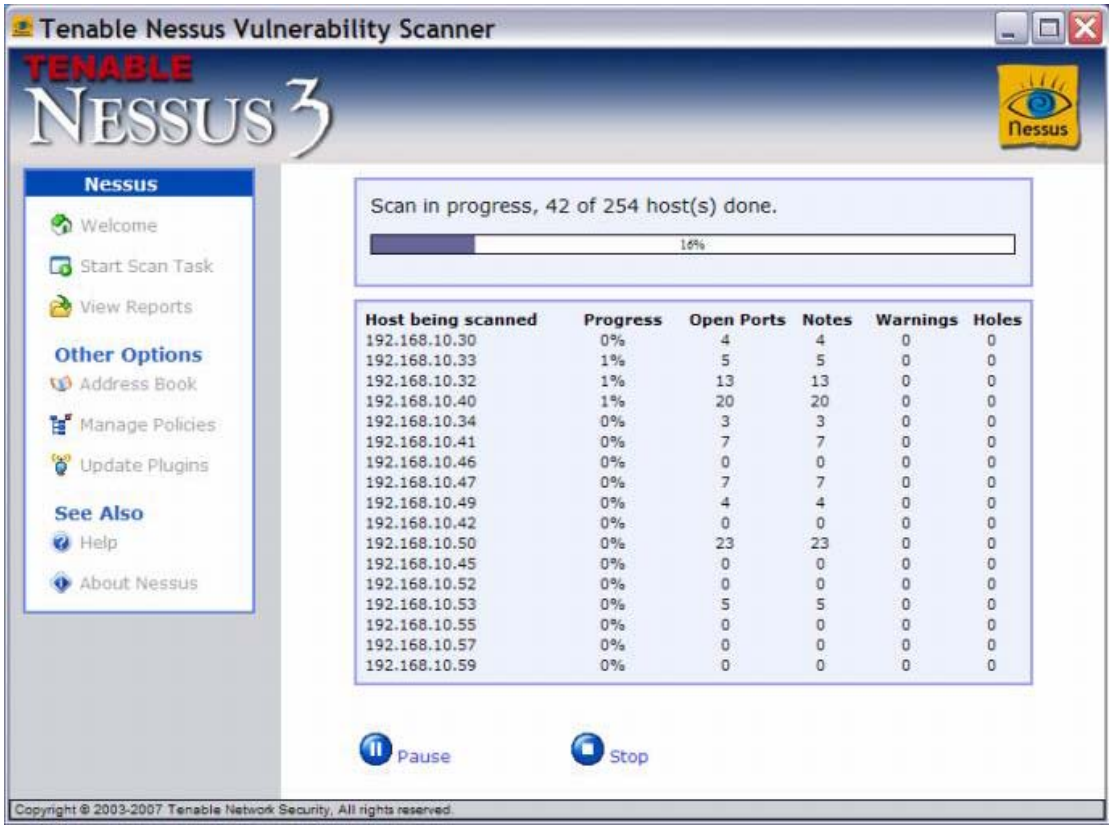
NESSUS

Nessus es una utilería que permite realizar auditorías y revisiones de vulnerabilidades en redes (www.nessus.org). Nessus es una herramienta que nos ayudará a revisar vulnerabilidades en nuestro sistema, de acuerdo a los plugin que tengamos instalados o actualizado.

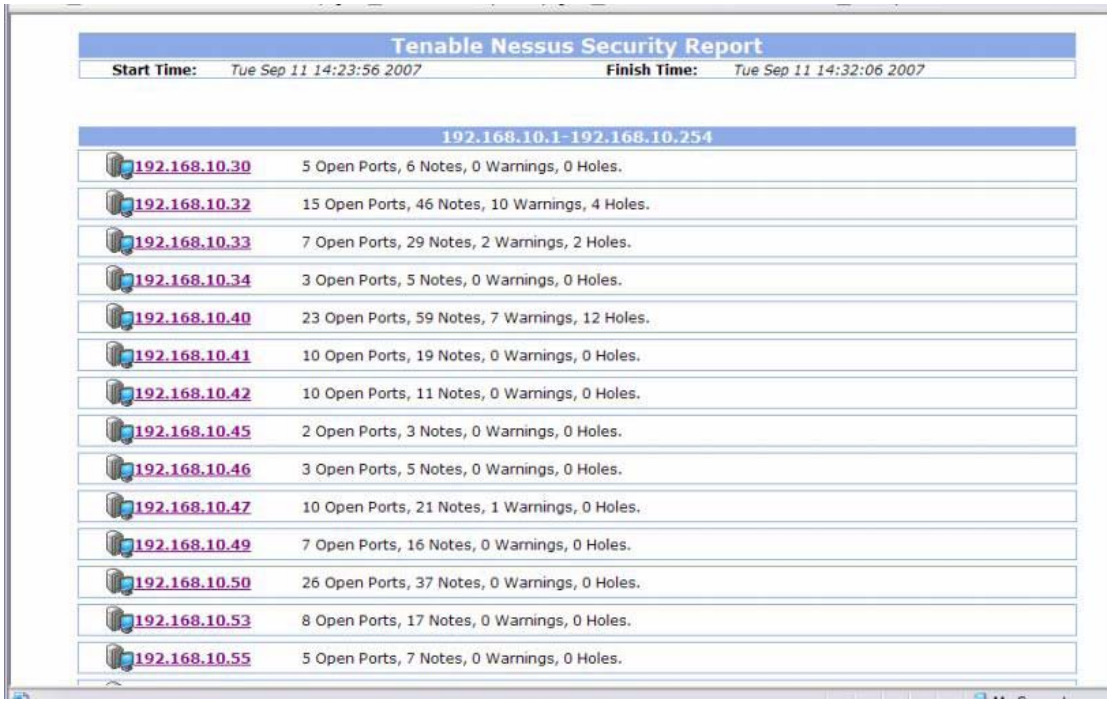
Los pasos a seguir para escanear las vulnerabilidades de las máquinas de la red de Uniplex se detallan a continuación:

Una vez instalado Nessus aparecerá la pantalla de bienvenida de Nessus. Para iniciar con el escáner se escoge la opción “tarea de iniciar el escáner”

A continuación se escoge la dirección IP de la máquina que se desea escanear, o del rango de direcciones IP.



Una vez finalizado el escáner, se podrá tener acceso a los resultados con la opción “ver reportes”, se escoge el reporte de la máquina a ser analizada y se verán resultados como los que se muestra a continuación.



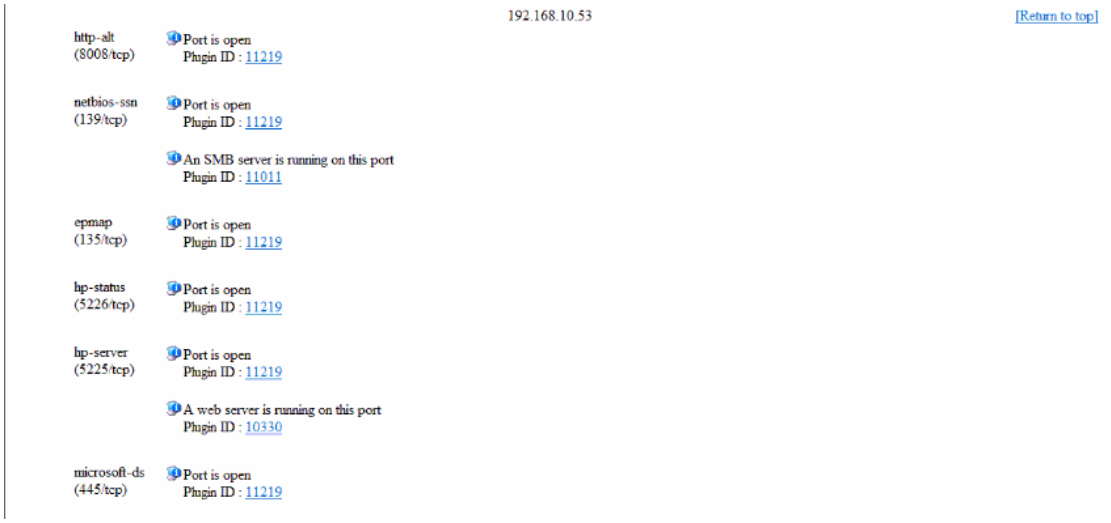
Tenable Nessus Security Report

Start Time: *Tue Sep 11 14:23:56 2007* **Finish Time:** *Tue Sep 11 14:32:06 2007*

192.168.10.1-192.168.10.254

192.168.10.30	5 Open Ports, 6 Notes, 0 Warnings, 0 Holes.
192.168.10.32	15 Open Ports, 46 Notes, 10 Warnings, 4 Holes.
192.168.10.33	7 Open Ports, 29 Notes, 2 Warnings, 2 Holes.
192.168.10.34	3 Open Ports, 5 Notes, 0 Warnings, 0 Holes.
192.168.10.40	23 Open Ports, 59 Notes, 7 Warnings, 12 Holes.
192.168.10.41	10 Open Ports, 19 Notes, 0 Warnings, 0 Holes.
192.168.10.42	10 Open Ports, 11 Notes, 0 Warnings, 0 Holes.
192.168.10.45	2 Open Ports, 3 Notes, 0 Warnings, 0 Holes.
192.168.10.46	3 Open Ports, 5 Notes, 0 Warnings, 0 Holes.
192.168.10.47	10 Open Ports, 21 Notes, 1 Warnings, 0 Holes.
192.168.10.49	7 Open Ports, 16 Notes, 0 Warnings, 0 Holes.
192.168.10.50	26 Open Ports, 37 Notes, 0 Warnings, 0 Holes.
192.168.10.53	8 Open Ports, 17 Notes, 0 Warnings, 0 Holes.
192.168.10.55	5 Open Ports, 7 Notes, 0 Warnings, 0 Holes.

A continuación se presenta el resultado de la auditoría a una máquina de la red de Uniplex, del cual se obtuvieron los siguientes resultados:



192.168.10.53 [Return to top]

http-alt (8008/tcp)	Port is open	Plugin ID : 11219
netbios-ssn (139/tcp)	Port is open	Plugin ID : 11219
	An SMB server is running on this port	Plugin ID : 11011
epmap (135/tcp)	Port is open	Plugin ID : 11219
hp-status (5226/tcp)	Port is open	Plugin ID : 11219
hp-server (5225/tcp)	Port is open	Plugin ID : 11219
	A web server is running on this port	Plugin ID : 10330
microsoft-ds (445/tcp)	Port is open	Plugin ID : 11219

microsoft-ds (445/tcp)

Port is open
Plugin ID : 11219

A CIFS server is running on this port
Plugin ID : 11011

Synopsis :

It is possible to obtain information about the remote operating system.

Description :

It is possible to get the remote operating system name and version (Windows and/or Samba) by sending an authentication request to port 139 or 445.

Risk Factor :

None

Plugin output :

The remote Operating System is : Windows 5.1
The remote native lan manager is : Windows 2000 LAN Manager
The remote SMB Domain Name is : CMS

192.168.10.53 resolves as JEFEVENTAS.
Plugin ID : 12053

Remote operating system : Microsoft Windows XP Service Pack 2
Confidence Level : 99
Method : MSRPC

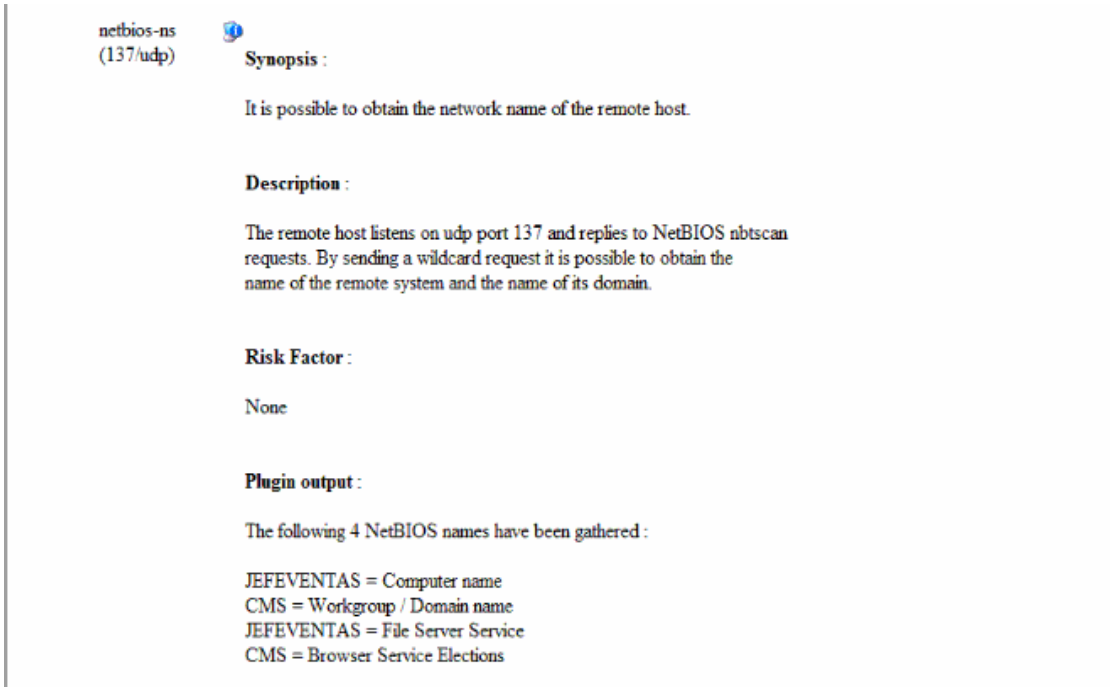
Not all fingerprints could give a match - please email the following to os-signatures@nessus.org :
HTTP:!:Server: Apache Tomcat/4.0.3 (HTTP/1.1 Connector)
SinFP:!:
P1:B11110:F0x12:W65535:O0204ffff:M1460:
P2:B11110:F0x12:W65535:O0204ffff010303000101080a0000000000000000001010402:M1460:
P3:B11000:F0x04:W0:O0:M0
P4:3004_2

The remote host is running Microsoft Windows XP Service Pack 2
Plugin ID : 11936

general/udp

For your information, here is the traceroute from 192.168.10.250 to 192.168.10.53 :
192.168.10.250
192.168.10.53

Plugin ID : 10287



Como se puede observar nos da información útil para hacer un diagnóstico de las vulnerabilidades de la red. Entre la información más importante proporcionada por el software están:

- Fecha de inicio y fin de escaneo.
- La IP de la máquina escaneada.
- Los puertos abiertos así como las aplicaciones que usan estos puertos
- El sistema operativo
- Los huecos de seguridad presentes en la máquina
- En el caso de exista alguna vulnerabilidad, Nessus propone un sitio web donde podemos buscar soluciones para cubrir esta vulnerabilidad

ANEXO I

FIREWALL

Para minimizar los riesgos que representa el acceso a Internet, se propone la implementación de un firewall para limitar el tráfico indeseable y cause daño a la Uniplex, en Firewall debe cumplir con los siguientes requerimientos:

Mínimo 3 interfaces de red Ethernet 10/100 Mbps tanto para la red interna, la zona DMZ de servidores y para la conexión a Internet.

El firewall debe manejar NAT o PAT para permitir el acceso a Internet de las computadoras de Uniplex.

Generación de logs para llevar un registro de todos los eventos, los cuales serán de gran utilidad al momento de realizar una auditoria o Uniplex sea víctima de algún ataque.

Interfaz gráfica de usuario basada en la WEB (https) para administración.

Las sesiones de administración remota debe ser encriptada y autenticada.

Tecnología de Firewall Statefull Inspector que integre del mismo fabricante motores de detección y prevención de intrusos, antivirus.

Capacidad de agregar, editar o borrar reglas del firewall en línea.

Priorización en tráfico de entrada/salida (Qos)

Sistema Operativo robusto.

Se ha analizado las características de los siguientes Firewalls:

- Firewall Cisco Serie ASA 5510
- D-Link - FIREWALL D-LINK DFL-1100
- 3COM

CISCO SERIE ASA 5510

La serie Firewall ASA 5510, es un equipo con un alto throutput y cuya aplicación esta destinada para SOHO y Grandes empresas, suministrando una seguridad y servicios de red muy robustos, tales como: virtual LAN (802.1q tag) support; Open Shortest Path First dynamic routing; Network Address Translation; Port Address Translation; content filtering (Java/ActiveX); URL filtering; authentication, authorization, and accounting (RADIUS/TACACS+) integration; soporte para leading X.509 public key infrastructure solutions; and Dynamic Host Configuration Protocol client, server, relay, and Point-to-Point Protocol over Ethernet support. Ademas, la serie Cisco PIX Security Appliances, tiene 56-bit Data Encryption Standard (DES), 168-bit Triple DES (3DES), o una encriptacion hasta 256-bit Advanced Encryption Standard (AES). Entregando servicios de alto rendimiento para VPN.

Comienzo de la página 5 Razones para la compra de la serie Cisco ASA 5500 Security

Appliances adaptable

1. Confianza y seguridad VPN protegida de amenazas-Tecnologícas Confianza basada en Cisco PIX Security Appliance ® y VPN de Cisco Serie 3000 Concentrador tecnología. El Cisco ASA 5500 Series es la primera solución para ofrecer VPN SSL e IPsec protegidos por los servicios líderes en el mercado la tecnología de firewall.

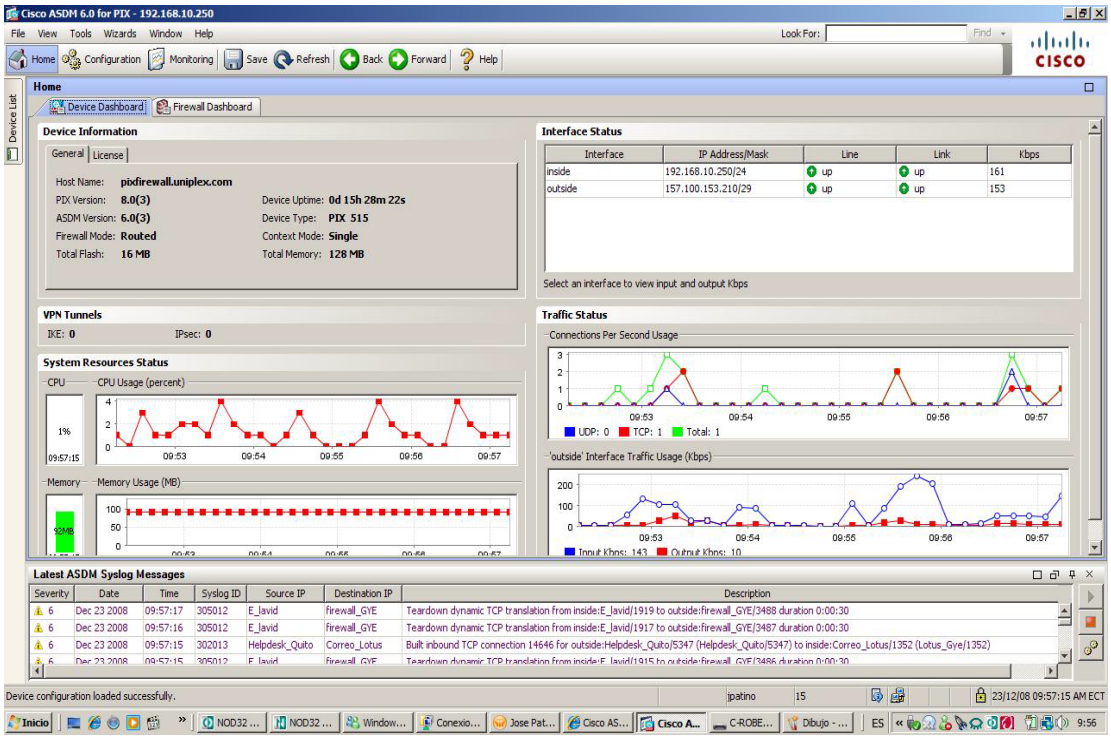
2. Líderes en la industria de Servicios de Seguridad de Contenido Trend Micro combina la experiencia de protección de amenazas y control de los contenidos de Internet en el borde con Cisco demostrado proporcionar soluciones antivirus, anti-spyware, bloqueo de archivos, anti-spam, anti-phishing, bloqueo y filtrado de URL y

filtrado de contenidos.

3. Servicios avanzados de prevención de intrusiones
   Proporciona dinámico, con funciones completas, servicios de prevención de intrusos para poner fin a una amplia gama de amenazas, incluyendo gusanos, ataques de nivel de aplicación, sistema operativo a nivel de los ataques, rootkits, spyware, peer-to-peer para compartir archivos y mensajería instantánea.

4. Ricos de gestión y supervisión de servicios
   Emite intuitiva único dispositivo de gestión y supervisión de servicios de Cisco a través de la adaptación de Seguridad del Administrador de dispositivos (ASDM), y de clase empresarial multidevice servicios de gestión de Seguridad de Cisco a través de Management Suite.

5. Reducción de Costes de Operaciones y Despliegue
   Al proporcionar una interfaz de diseño y en consonancia con las soluciones de seguridad de Cisco, el Cisco ASA 5500 Serie permite significativamente más bajos costes de propiedad para el despliegue inicial de seguridad y el día a día la gestión.



Precio: 2100 dólares

Dlink DFL-1100 Firewall Enterprise VPN

El DFL-1100 de D-Link es un firewall de fácil uso, diseñado para medianas y grandes empresas que requieran un precio/rendimiento superior. Este dispositivo es una potente solución de seguridad que integra traducción de dirección de red (NAT), firewall, filtrado de contenidos, protección IDS, gestión del ancho de banda y soporte de red privada virtual (VPN). El DFL-1100 incluye soporte de enlace WAN, puerto LAN de confianza y puerto DMZ para correo electrónico local y servidores web. Gracias a la intuitiva interfaz basada en web, el proceso de instalación del DFL-1100 resulta fácil y sencillo para el usuario.

Aplicación de seguridad multifunctional

El DFL-1100 ofrece funciones típicamente requeridas por las empresas para los firewalls de calidad, como SPI (Stateful Packet Inspection), detección/eliminación de paquetes intrusos, VPN integrada, puerto DMZ físico, IPs con mapeo múltiple y múltiples servidores virtuales. El

DFL-1100 conecta fácilmente su oficina a un módem de banda ancha, de cable o DSL, a través de un puerto WAN externo 10/100BASE-TX

Plenas funciones de firewall

El DFL-1100 ofrece verdaderas funciones de firewall, que incluyen modo NAT, modo PAT (Port Address Translation), modo transparente*, modo de enrutamiento y SPI. También soporta configuración del servidor virtual y política personalizada. Los administradores pueden gestionar fácilmente la red a través de las estadísticas gráficas del sistema de registro/monitorización.

Soporte VPN IPSec de alto rendimiento

El DFL-1100 dispone de soporte VPN, lo que permite crear múltiples túneles IPSec para sitios/clientes remotos. El IPSec del DFL-1100 usa una potente encriptación con DES, 3DES, AES y gestión automatizada de claves a través de IKE/ISAKMP. Desde el DFL-1100 puede activarse un túnel VPN hacia un sitio remoto o un usuario móvil para asegurar el flujo de tráfico por medio de la triple encriptación DES. De este modo el usuario puede acceder confidencialmente a información importante y transferirla. Los múltiples túneles VPN pueden crearse fácilmente sin necesidad de configurar políticas IKE (Internet Key Exchange).
Lista de control de acceso (ACL)

El bloqueo de URL forma parte de las características básicas del DFL-1100. Esta función permite limitar el acceso a sitios internet no deseado. Se registran los registros del tráfico de internet en tiempo real, las alarmas de ataques de internet y los avisos de las actividades de navegación web; toda esta información puede recibirse a través de una notificación de correo electrónico.

El DFL-1100 soporta la autentificación Radius, por lo que puede usarse un servidor Radius ya existente y la información de usuario.

Protección total

Las avanzadas características del DFL-1100, en lo que a seguridad del usuario en la red se refiere, incluyen el filtrado de contenidos, el IDS (Intrusion Detection System) y la gestión del ancho de banda. El filtrado de contenidos permite filtrar o proteger la red con políticas personalizables. La gestión del ancho de banda garantiza el ancho de banda para los distintos servicios.

El DFL-1100 protege la red de los ataques. El dispositivo puede ser configurado para que registre todos los ataques, localice la dirección IP desde la que se ha realizado el ataque, envíe la notificación del ataque a una determinada dirección de correo electrónico y establezca políticas que restrinjan el tráfico entrante de direcciones IP de origen específicas. Los administradores de red pueden indicar las direcciones de correo electrónico a las que deben enviarse los mensajes de alerta del DFL-1100. Cuando se detecta una intrusión, el DFL-1100 la registra y envía un mensaje de alerta de correo eléctrico; de este modo, el administrador puede comprobar el fichero de registro del router para descubrir qué ha pasado.

El DFL-1100 puede operar hasta con 200.000 sesiones proporcionando 1.000 túneles VPN a 1.000 conexiones remotas que necesiten una conexión fiable y segura con la red de una empresa.

Puerto DMZ, Puerto LAN de confianza

El DFL-1100 incluye un puerto LAN 10/100BASE-TX autosensible para conectarlo a la red interna de una oficina, y un puerto físico DMZ (Demilitarized Zone) que puede conectarse a los servidores web, de correo electrónico o FTP, para acceder a internet. La función DMZ es muy útil ya que descongestiona el tráfico del servidor que proviene de la red interna, y protege a los otros ordenadores de la oficina de ataques de Internet, que quedan ocultos tras el firewall.

Principales Características:

- 1 Puerto LAN 10/100BASE-TX, 1 puerto DMZ 10/100BASE-TX, 1 puerto WAN 10/100BASE-TX para conexión de módem de cable/DSL, 1 puerto de backup 10/100BASE-TX
- Soporta tunelización VPN IPSec
- Soporta VPN IPSec pass throughput
- Modo cliente agresivo/principal para VPN
- Protección de firewall SPI (Stateful Packet Inspection)
- Denegación de servicio (DoS) y bloqueo de ataque DDoS
- Traducción de dirección de red (NAT) / Traducción del puerto de la dirección de red (NAPT)
- Soporta ALG (Application Level Gateway) NAT, Protocolo SYSlog y servidor virtual.
- Soporte de cliente PPPoE incorporado.
- Control de servidor/cliente DHCP y paterno
- Filtrado de contenidos, bloqueo de URL/dominio y comprobación de palabra clave
- Gestión de configuración basada en web y monitorización en tiempo real

Precio: 2071 dólares

3Com Email Firewall - Firewall - EN, Fast EN - 1U

Fabricado por: 3COM

Descripción: El 3Com Email Firewall es un dispositivo de desktop o de montaje en rack, con tecnología BorderWare.
Se suministra con una suscripción de un año completo al servicio Security Connection de BorderWare, que proporciona actualizaciones automáticas para los filtros anti-spam, el software antivirus y el sistema operativo integrado.

Las licencias de usuario, de actualización y de renovación del 3Com Email Firewall se ofrecen por separado del dispositivo hardware, ofreciéndole así un precio asequible y una escalabilidad de tipo "invierta según crezca".

Descripción del producto 3Com Email Firewall firewall

Tipo de dispositivo Firewall
Tipo incluido Externo - 1U
Dimensiones (Ancho x Profundidad x Altura) 42.2 cm x 38.1 cm x 4.4 cm
Peso 6 kg
Localización Centroeuropa
Procesador 1 x Intel Celeron 2.4 GHz
RAM instalada (máx.) 256 MB
Disco duro 40 GB x 1 - IDE/ATA
Protocolo de interconexión de datos Ethernet, Fast Ethernet

Características Prevención contra ataque de DoS (denegación de servicio)

Alimentación CA 120/230 V (50 - 60 Hz)

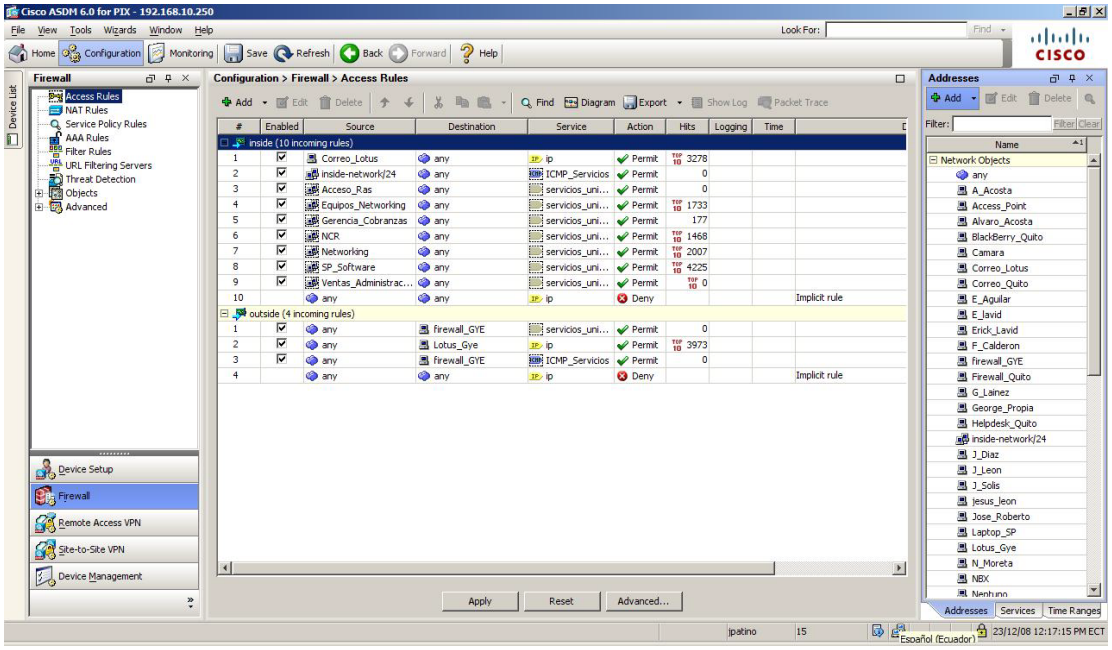
Garantía del fabricante 1 año de garantía

Precio: 1351 dólares

Elección del Firewall

Después de haber analizado las características de los tres firewalls, se escogió el firewall Cisco ASA ya que se ajuste a los requerimientos de Uniplex, este dispositivo a más de brindar el servicio de firewall nos brinda características adicionales de seguridad como VPN integrada, soporta denegación de servicio y bloqueo de ataque DDoS, NAT, PAT, filtrado de contenidos, bloqueo de URL/dominio y comprobación de palabra clave, monitorización en tiempo real; estas funciones adicionales de seguridad contribuyen a la reducción de riesgos identificados en la empresa en el análisis de riesgos.

Tras haber presentado esta solución a la Gerencia de la empresa, se aprobó este control de seguridad debido a los costos económicos factibles que esta implica (ver anexo costos de firewall). El firewall propuesto inicialmente entre las más importantes características ofrecía además el servicio de detección de intrusos, por esta razón también se ha propuesto implementar Snort para cubrir este control de seguridad, ambas peticiones hasta la fecha están en consideración


Cisco ASDM 6.0 for PIX - 192.168.10.250
File View Tools Wizards Window Help
Look For:
Find
Home Configuration Monitoring Save Refresh Back Forward Help
cisco
Device List
Firewall
Access Rules
NAT Rules
Service Policy Rules
AAA Rules
Filter Rules
URL Filtering Servers
Threat Detection
Objects
Advanced
Device Setup
Firewall
Remote Access VPN
Site-to-Site VPN
Device Management
Configuration > Firewall > Access Rules
Add Edit Delete Find Diagram Export Show Log Packet Trace
Enabled Source Destination Service Action Hits Logging Time
inside (10 incoming rules)
1 Correo_Lotus any ip Permit 3278
2 inside-network/24 any ICMP_Servicios Permit 0
3 Acceso_Ras any servicios_uni... Permit 0
4 Equipos_Networking any servicios_uni... Permit 1733
5 Gerencia_Cobranzas any servicios_uni... Permit 177
6 NCR any servicios_uni... Permit 1468
7 Networking any servicios_uni... Permit 2007
8 SP_Software any servicios_uni... Permit 4225
9 Ventas_Administrac... any servicios_uni... Permit 0
10 any any ip Deny Implicit rule
outside (4 incoming rules)
1 any firewall_GYE servicios_uni... Permit 0
2 any Lotus_Gye ip Permit 3973
3 any firewall_GYE ICMP_Servicios Permit 0
4 any any ip Deny Implicit rule
Apply Reset Advanced...
Addresses
Add Edit Delete
Filter: Filter Clear
Name
Network Objects
any
A_Acosta
Access_Point
Alvaro_Acosta
BlackBerry_Quito
Camara
Correo_Lotus
Correo_Quito
E_Aguilar
E_Javid
Erick_Javid
F_Calderon
Firewall_GYE
Firewall_Quito
G_Lainez
George_Propia
Helpdesk_Quito
inside-network/24
J_Diaz
J_Leon
J_Solis
jesus_leon
Jose_Roberto
Laptop_SP
Lotus_Gye
N_Moreta
NBX
Addresses Services Time Ranges
jpatino 15
Español (Ecuador) 23/12/08 12:17:15 PM ECT

ANEXO J

MRTG (MULTI ROUTER TRAFFIC GRAPHER)

Para implementar un control que permita verificar la utilización del tráfico de la red, que nos puede servir para detectar un posible fallo de seguridad en la red, pues si detectamos un incremento considerable en el tráfico de la red se puede determinar problemas en la misma, ya sea debido a un virus o un programa que esté consumiendo gran cantidad de recursos no permitidos. A continuación se detalla la configuración del aplicativo MRTG en el servidor Linux (solo se pudo hacer pruebas en el para sacar las muestras para esta tesis, actualmente ya no esta disponible), para de esta manera aprovechar los recursos actualmente disponibles en la empresa.

Equipamiento lógico

En la opción aplicaciones de CentOS se procedió a instalar el paquete MRTG con el CD de instalación. Para poder ejecutar automáticamente el MRTG y mantener actualización del uso de tráfico cada 5 minutos se configura el planificador de tareas CRONTAB como se indica a continuación:

Planificador de Tareas (CRONTAB)

Cron se podría definir como el "equivalente" a Tareas Programadas de Windows. Los usuarios habilitados para crear su archivo crontab se especifican en el archivo cron.allow. De

manera análoga, los que no lo tienen permitido figuran en /etc/cron.d/cron.deny, o /etc/cron.deny, dependiendo de la versión. Archivo crontab para MRTG:

```
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root
HOME=/
# run-parts
01 * * * * root nice -n 19 run-parts /etc/cron.hourly
50 0 * * * root nice -n 19 run-parts /etc/cron.daily
22 4 * * 0 root nice -n 19 run-parts /etc/cron.weekly
42 4 1 * * root nice -n 19 run-parts /etc/cron.monthly
```

El formato de configuración de cron es muy sencillo.

El símbolo Numeral "#" es un comentario, todo lo que se encuentre después de ese carácter no será leído por cron.

El momento de ejecución se específica de acuerdo con la siguiente tabla:

Minutos: (0-59)

Horas: (0-23)

Días: (1-31)

Mes: (1-12)

Día de la semana: (0-6), siendo 1=Lunes, 2=Martes, ... 6=sábado y 0=Domingo

Para especificar todos los valores posibles de una variable se utiliza un asterisco (*).

La última columna corresponde al path absoluto del binario o script que se quiere ejecutar

Procedimientos de configuración del MRTG

Se crea un directorio de trabajo:

mkdir –p /var/www/mrtg/Uniplex

Por razones de seguridad se saca un respaldo del archivo de configuración mrtg.cp /etc/mrtg/mrtg.cfg /etc/mrtg/mrtg.cfg-OLD

Configuración SNMP

1. Se procedió a la configuración del protocolo SNMP en el archivo ubicado en /etc/snmp/snmpd.cfg

a. Se creó una comunidad pública de solo lectura.

	Sec.name	**Source**	**Comunity**
Com2sec	Readonly	default	Edi654@tion

Donde com2sec mapea un nombre de una comunidad pública a un nombre seguro.

b. Se creó un grupo para las diferentes versiones SNMP

	groupName	**SecurityModel**	**SecurityModel**
Group	MyROGroup	V1	readonly
Group	MyROGroup	V2c	readonly
Group	MyROGroup	Usm	readonly

c. Se creó vista para permitir el acceso a los diferentes grupos de las MIBs.

	name	**incl/excl**	**subtree**	**mask(optional)**
View	All	include	.1	80

Donde: all indica que recorrerá todo árbol a partir del nodo .1 (iso) hasta el nivel del árbol 80

Se indica los permisos que tendrá el grupo creado anteriormente para la gestión de información en el dispositivo.

	group	Context sec.model	Sec.level	prefix	read	write	Notif.
Access	MyROGRoup	“ “	Noauth	exact	all	none	none

En el cuadro anterior se indica los permisos que se otorgan como son: nivel de seguridad no autenticación, además se otorga permisos sólo para lectura y no para escritura ya que el servicio de mrtg que se utilizara no lo necesitará.

Para generar el archivo de configuración para supervisar a la red LAN de la Corporación, se utilizó el siguiente comando:

```
cfgmaker \
--global "workdir: /var/www/mrtg/CMS" \
--global "Options[_]: bits,growright" \
--output /etc/mrtg/mrtg.cfg \
--community=Edi654@tion \
192.168.10.1 \
192.168.10.2 \
192.168.10.3 \
```

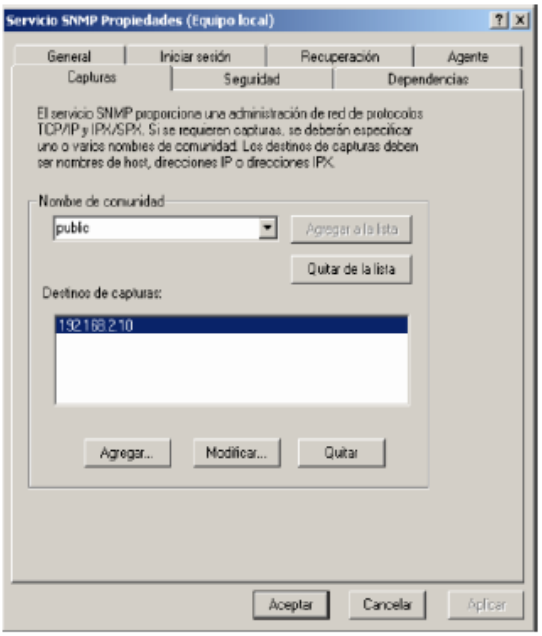
Donde **Edi654@tion** es el nombre de la comunidad, por seguridad no se ha establecido el nombre de la comunidad por default.

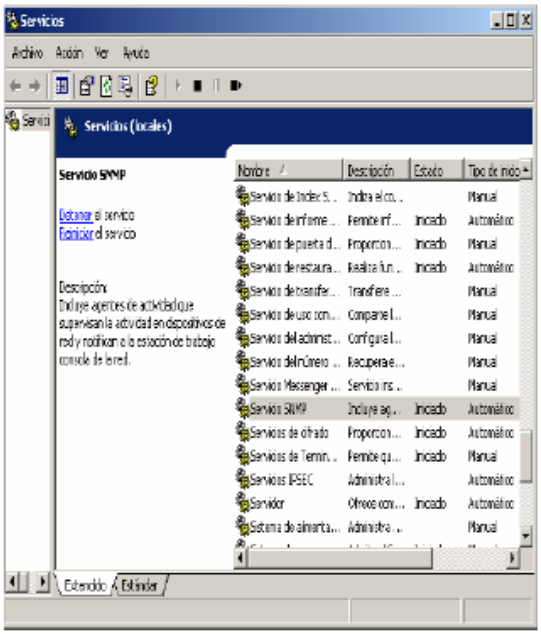
a. Configuración de SNMP en el dispositivo monitorizado

Para nuestro caso se procedió a monitorizar dispositivos operando bajo el sistema operativo Windows, para lo cual se realizo el siguiente procedimiento.

1. Previo levantar servicio snmp se procedió a la instalación de Service Pack 2 requerido por este sistema.

2. En Herramientas administrativas se selecciona Servicios en donde se comprueba si el servicio snmp esta inicializado y adecuadamente configurado (direccion ip, comunidad,seguridad).





Comprobaciones

Para hacer que mrtg se ejecute de forma automática cada 5 minutos, se instala croad en la ruta /etc/cron.d/mrtg.

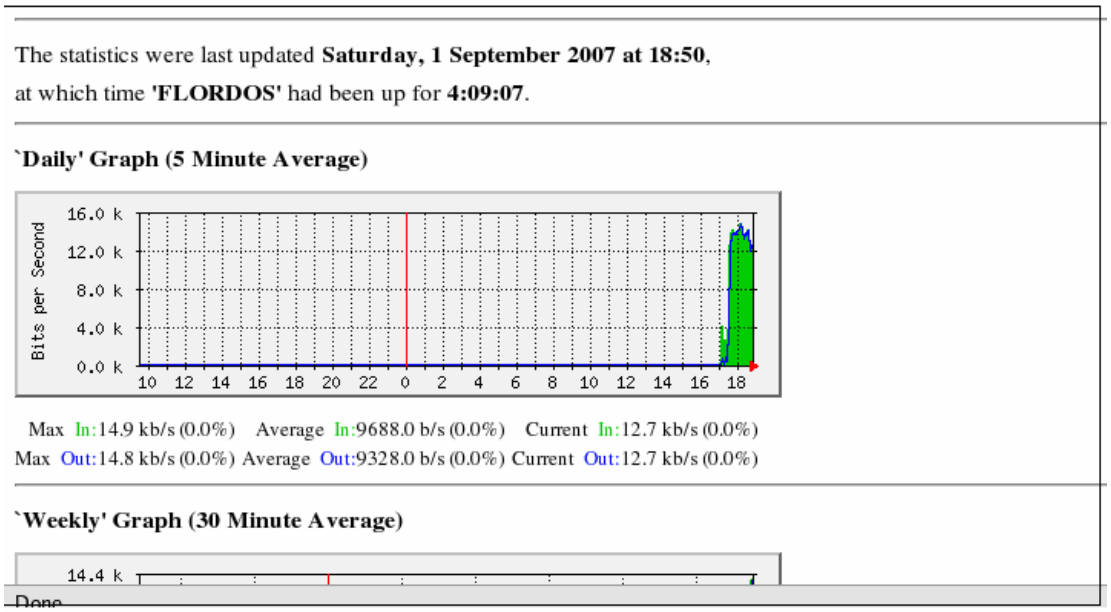
Para generar un reporte del monitoreo de tráfico, se utiliza el siguiente comando:

env LANG=C mrtg /etc/mrtg/mrtg.cfg

Se debe reiniciar el servicio Apache para que se cargue la configuración especificada en /etc/httpd/conf.d/mrtg.conf, con la que se permitirá acceder hacia los reporte MRTG a través de interfaz por protocolo http Service httpd restart

Para observar los resultados del monitoreo con MRTG se accedió a la página http://127.0.0.1/mrtg/CMS/192.168.10.85_2.html, en este caso se observará el reporte de la máquina con la dirección 192.168.10.85.

RESULTADOS

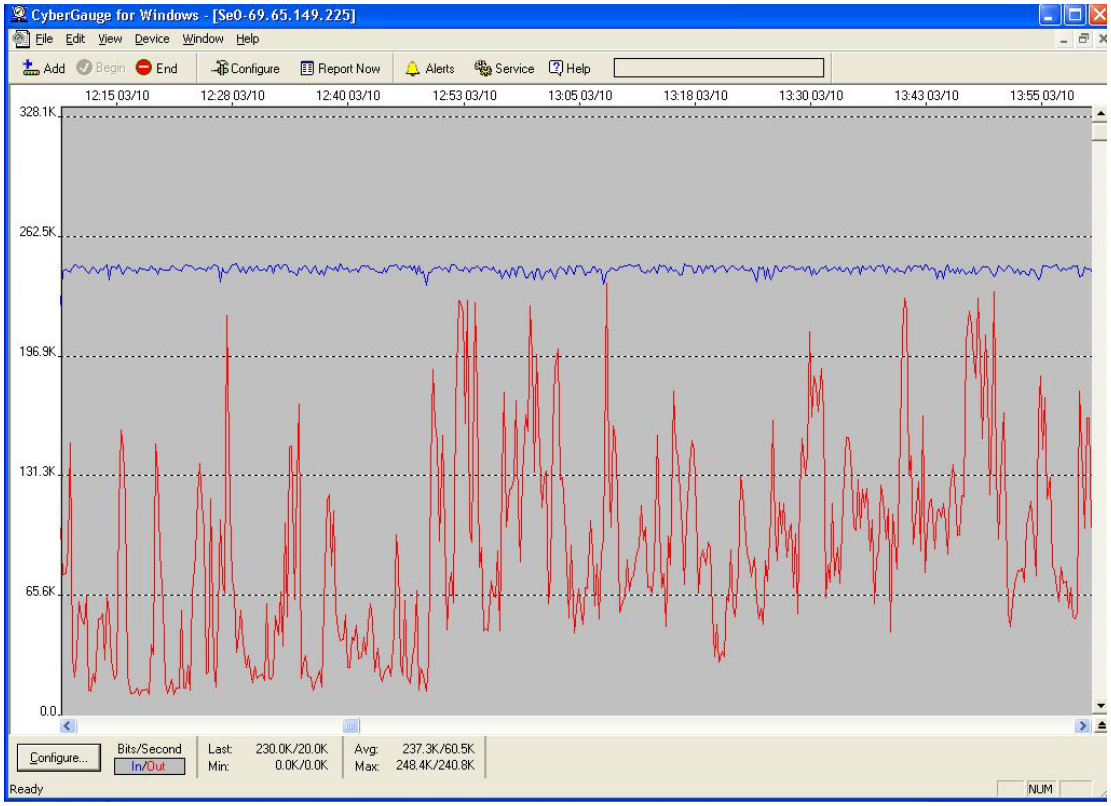


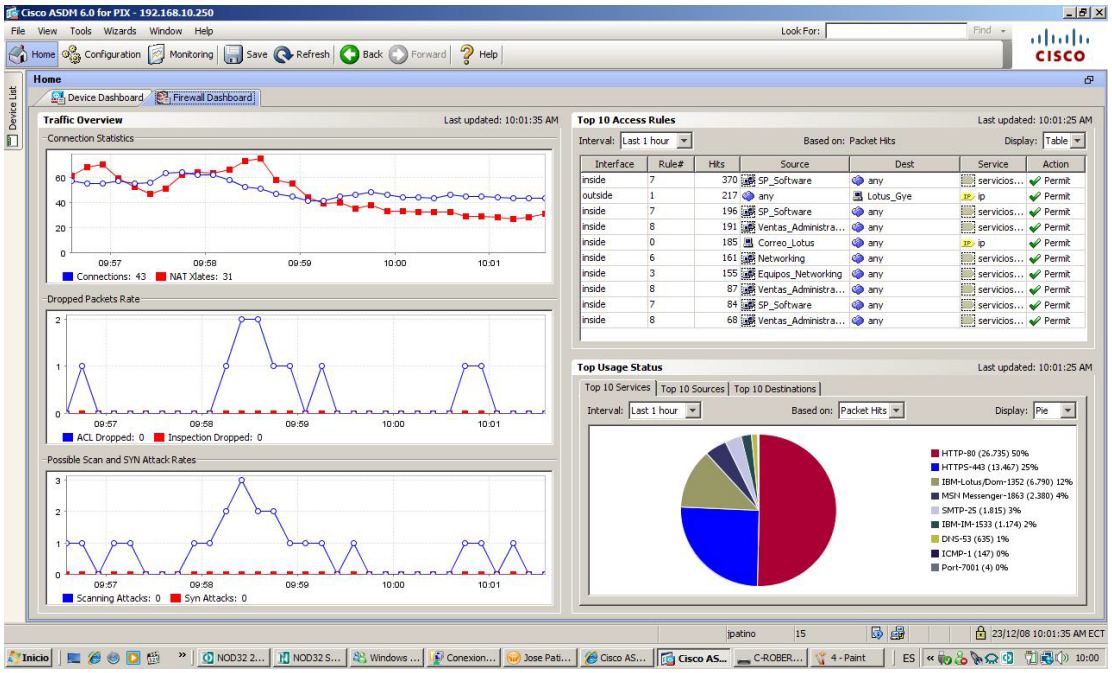
El reporte se tomo en Uniplex durante un período mínimo de trabajo, el tráfico que se obtuvo es el indicado en el gráfico.

Esta herramienta será utilizada como un control de red para determinar los patrones de tráfico normales, y en el caso que haya tráfico inesperado determinar a tiempo algún intento de ataque a red de la Corporación y detenerlo para evitar cualquier tipo de consecuencias.

Nota: Todo este proceso de configuración para monitorear el ancho de banda del tráfico de red usado diariamente se lo puede realizar con otra herramienta gratuita como lo es el

CyberGauge60 el cual es de fácil instalación y uso. También el propio firewall ASA provee ese monitoreo.





ANEXO K

CONDUCTA COMERCIAL

A continuación se detalla los puntos principales en cuanto a seguridad que deberían darse a conocer a los empleados, para que tengan conocimiento cuales son las responsabilidades de seguridad que se comprometen a cumplir una vez que son miembros de la empresa.

Confidencialidad

Si usted tiene conocimiento de una situación poco ética o ilegal, debe informar al superior inmediato de cada área cualquier cosa que sepa o haya oído acerca de la situación ilegal.

Conducta Personal

La reputación de Uniplex depende de usted, si los responsables de cada área encuentran una conducta dentro o fuera del trabajo que afecta en forma adversa su desempeño, el de otros empleados, o los interese de la empresa; usted está sujeto a medidas disciplinarias, incluido despido.

Ambiente de Trabajo

Los empleados de Uniplex que se los encuentre comprometidos en acoso o discriminación, o que han utilizado mal sus posiciones de autoridad en este aspecto, estarán sujetos a medidas disciplinarias, incluido el despido. De igual forma está prohibido en el ambiente de

trabajo: Amenazas, Comportamiento Violento, Posesión de armas, uso de aparatos de grabación incluidos vídeos de teléfonos y cámaras web, para propósitos distintos a los aprobados por el responsable de cada área; y Uso, distribución, venta o posesión de drogas ilegales o cualquier sustancia controlada, excepto para propósitos médicos aprobados.

Privacidad del Empleado de Uniplex

La información personal de los empleados compartida con terceras personas sólo con la aprobación del empleado, excepto cuando Uniplex tenga que liberar la información para satisfacer con los requisitos legítimos de una compañía o empresa que considere necesaria esta información para realizar operaciones de negocios con la empresa. Los mensajes o información personales que usted considere privados no deben ser colocados o mantenidos en ningún parte del sitio del trabajo, como los sistemas telefónicos, sistemas de oficina, archivos electrónicos, escritorios, estanterías, cajones u oficinas.

Protección de los activos de Uniplex

La empresa tiene una gran variedad de activos, los cuales incluyen activos físicos y la información propietaria extremadamente valiosa como la propiedad intelectual y la información confidencial. Es crítico proteger todos estos activos. Usted es responsable de proteger la propiedad de Uniplex confiada a usted y de ayudar a proteger los activos de la compañía en general.

Usted debe estar alerta de cualquier situación o incidente que pueda llevar a la pérdida, mal uso, o robo de las propiedades de la compañía.

Información Propietaria

La información propietaria es resultado de ideas, trabajo duro e innovación de muchos de los empleados de la empresa y de inversiones sustanciales hechas en la empresa, por lo cual Uniplex se vería dañada por revelaciones no autorizadas de su información propietaria o el uso no autorizado de dicha información por cualquier persona fuera de la empresa.

Se debe tener cuidado de evitar la revelación involuntaria de información propietaria, para lo cual nunca discuta con ninguna persona no autorizada la información propietaria que Uniplex considere confidencial o que no se haya hecho pública. Además no se debe discutir dicha información con personas autorizadas cuando se encuentre en presencia de personas no autorizadas.

Dicha información se debe usar solamente para el negocio, esta obligación aplica sin importar si usted desarrolló o no la información dentro de Uniplex.

Derechos de propiedad intelectual

Cuando usted ingresa a Uniplex firma el contrato en el cual cede todos sus derechos, títulos e intereses en la propiedad intelectual que usted desarrolla cuando está empleado en ciertas calidades, tales como gerenciales, técnicas planeación de productos, programación, científica, u otra calidad profesional. La propiedad intelectual que se cede son ideas, inventos, programas de computador y documentos que se relacionen con el negocio actual o anticipado de la empresa.

Al salir de Uniplex

Si usted deja la compañía por cualquier razón, usted debe devolver toda la propiedad de la empresa, incluidos los documentos y medios que contengan información propietaria y usted no puede revelar o usar la información propietaria de Uniplex.

Prohibición en todos los contactos con Competidores

No discuta políticas de precios, términos de contratos, costos, inventarios, planes de mercadeo y de productos, encuestas y estudios de mercado, planes y capacidades de producción, y cualquier otra información propietaria o confidencial. Si un competidor trae cualquiera de estos temas, así sea en forma suave y con una aparente inocencia, usted debe objetar, parar la conversación inmediatamente y decirle a competidor que bajo ningún concepto discutirá estos asuntos, si es necesario se debe salir de la reunión.

Recepción de Información que puede ser Confidencial o tener Restricciones de Uso

Para evitar el riesgo de que Uniplex sea acusada de malversación o mal uso de la información confidencial o restringida de alguien, es necesario considerar varios puntos como son:

1.- El recibo de información confidencial o restringida no puede llevarse a cabo mientras no se haya acordado formalmente los términos de su uso por parte de Uniplex y del otro tercero en un contrato escrito y aprobado.

2.- usted no puede hacer uso de la información, copiarla, distribuirla o revelarla a menos que lo haga de conformidad con los términos del contrato.

Adquisición de Software

Se debe tener especial cuidado al adquirir software de otros. Como propiedad intelectual, el software está protegido por derechos de autor, y también puede estar protegido por leyes de patentes o secreto comercial.

Si usted adquiere software para el equipo personal de su propiedad, usted no debe copiar ninguna parte de dicho software en ningún trabajo de desarrollo que usted haga para la empresa, colocar dicho software en cualquier sistema de computador poseído por Uniplex, en forma general llevar dicho software a las instalaciones de Uniplex.

Es su responsabilidad asegurarse de que todo el software de terceros que usted esté usando esté licenciado en forma apropiada y que usted lo use solamente de conformidad con los términos de su licencia.

Conflicto de intereses

Su vida privada es suya, sin embargo usted es miembro de Uniplex tanto dentro como fuera del trabajo y puede resultar un conflicto de intereses si usted compromete en alguna actividad o anticipada cualquier interés personal, a costa de los intereses de la empresa. Un conflicto es proporcionar ayuda a una organización que comercializa productos y servicios que compiten con los servicios de la empresa.

Cuando usted dé su opinión sobre temas públicos, se deba asegurar que lo haga como individuo, no debe dar la apariencia de que está hablando o actuando a nombre de Uniplex.

Sanciones Previstas por Incumplimiento

Se aplicarán las sanciones provistas por las leyes que rigen actualmente la constitución, a quienes incumplan lo dispuesto en las Políticas de Seguridad y se aplicarán las acciones pertinentes de acuerdo al caso.

Las sanciones sólo pueden imponerse mediante un acto administrativo que así lo disponga cumpliendo las formalidades impuestas por los preceptos constitucionales.

BIBLIOGRAFÍA

1. ISO – IEC., Estándar Internacional ISO/IEC 27001, Primera Edición. Octubre 15 del 2005. Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos No. de Referencia: ISO/IEC 27001:2005

2. ISO – IEC., Estándar Internacional ISO/IEC 17799, Segunda Edición. Junio 15 del 2005. Tecnología de la Información – Técnicas de Seguridad – Código para la práctica de Seguridad de la Información.

3. ICONTEC, Norma Técnica Colombiana, Tecnología de la Información. Técnicas de Seguridad. Código de Práctica para la Gestión de la Seguridad de la Información, Edición Noviembre 16 del 2007 Referencia NTC-ISO/IEC 27002.

4. MARÍA DOLORES CERINI – PABLO IGNACIO PARA., Plan de Seguridad Informática (PSI) Argentina – Octubre 2002, (Tesis de la Facultad de Ingeniería en Sistemas de La Universidad de Córdova).

5. RENÉ DAMIÁN PADILLA BENITEZ – LUIS FELIPE URQUIZA AGUIAR., “Rediseño de la Red WAN de Petrocomercial con QoS” (Tesis, Facultad

de Ingeniería Eléctrica y Electrónica, Escuela Politécnica Nacional, Quito, Enero 2008)

6. UNIPLEX SYSTEM S.A., Información obtenida y basada en la Empresa auditada bajo la responsabilidad del Sr. José Patiño Sánchez a partir del mes de Febrero del 2008 Guayaquil – Ecuador.

7. WEBSIDE, información obtenida de los siguientes vínculos de Red:
   http://www.ongei.gob.pe/publica/metodologias/Lib5007/21.HTM
   http://sgsi-iso27001.blogspot.com/