“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”

Erick A. Lamilla Rubio
José R. Patiño Sánchez
Ing. Ivonne Martín M.
Facultad de Ingeniería en Electricidad y Computación “FIEC”
Escuela Superior Politécnica del Litoral “ESPOL”
Campus Gustavo Galindo, Km. 30.5 vía Perimetral, Apartado 09-01-5863, Guayaquil, Ecuador
ellamilla@fiec.espol.edu.ec; jpatino@fiec.espol.edu.ec; jpatino@espol.edu.ec; imartin@adexus.com.ec

Resumen

El presente trabajo tiene como objetivo fundamental, diseñar e implementar políticas de seguridad informática en base a la norma 27002 para la empresa Uniplex S.A.En la cual se proporcionara lineamientos básicos de la seguridad de la información, gestión de riesgos y diferentes alternativas para el tratamiento de los mismos.

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.

Para la realización 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.

Palabras claves: Auditoría, Gestión de Seguridad de la Información, ISO 27002

Abstract

The present project aims to design and implement informatics security policies based on the regulation 27002 for the company Uniplex S.A. which provide basic guidelines for information security, risk management and alternatives for their treatment.

We will expose a risks treatment plan in which will identify appropriate actions as well as the responsibles for minimize the identified risks and then actually execute the implementation of the Project Management Information Security (PGSI) based on the selected controls and finally obtain as result the manual's procedures for the implementation of PGSI. For the system implementation will be based solely on the security's regulation for the information ISO-27002.

For the realization it will create a summary that involves the steps to implement security in the company Uniplex Systems SA in Guayaquil.

An audit will be conducted to determine the strengths and weaknesses of the company Uniplex Guayaquil on the security policies of informatics.

Will be established procedures and processes of security that incorporate a series of measures over the Faculty information assets. Knowing, assuming and managing the possible risks in a way documented, structured and efficient which is adaptable to future changes.

1. Introducción

En muchas organizaciones la seguridad de la información es tratada como un problema sólo tecnológico, sin tomar en cuenta que la seguridad de la información es un problema organizativo y de gestión, lo que con lleva a que las organizaciones no sean capaces de afrontar ataques provenientes de todos los ángulos.

No es suficiente contar con tecnología sofisticada, la gestión implica conocer la situación de lo que queremos tratar y tener claro hacia donde queremos ir, es decir, determinar un objetivo y tomar las acciones necesarias para conseguirlo.

La definición de un modelo para la gestión de la seguridad de la información implica involucrar a toda la organización y no sólo al área encargada de implantar el modelo, lo cual trae como resultado el éxito del proyecto tanto en su implantación como en su mantenimiento, es así que se debe fomentar el cambio cultural para concienciar acerca de importancia de la seguridad.

El objetivo de seguir una recomendación internacional con respecto a la seguridad de la información es tener un protocolo común para la medida y gestión de los riesgos de información.

Podemos entender como seguridad un estado de cualquier tipo de información (informático o no) que nos indica que ese sistema está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar su funcionamiento directo o los resultados que se obtienen del mismo. Para la mayoría de los expertos el concepto de seguridad en la informática es utópico porque no existe un sistema 100% seguro. Para que un sistema se pueda definir como seguro debe tener estas cuatro características:

- Integridad: La información sólo puede ser modificada por quien está autorizado y de manera controlada.
- Confidencialidad: La información sólo debe ser legible para los autorizados.
- Disponibilidad: Debe estar disponible cuando se necesita.
- Irrefutabilidad (No repudio): El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Dependiendo de las fuentes de amenaza, la seguridad puede dividirse en seguridad física, seguridad ambiental y seguridad lógica.

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.

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 procede a realizar la implementación del proyecto 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. Elaboraremos propuestas, manuales de usuario y recomendaciones para futuras mejoras tomando en cuenta el futuro crecimiento y escalabilidad de la zona a implementar.

2. Marco Teórico

En esta sección nos enfocamos en describir la evolución de las ISO de seguridad, conjuntamente con una descripción del ISO 27002 que es el documento principal de esta tesis.

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 las 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 norma ISO 27002:2005 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.
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:
Política de seguridad
Organización de la seguridad de la información
Gestión de activos
Seguridad de los recursos humanos
Seguridad física y del entorno
Gestión de operaciones y comunicaciones
Control de acceso
Adquisición, desarrollo y mantenimiento de sistemas de información
Gestión de los incidentes de seguridad de la información
Gestión de la continuidad del negocio
Cumplimiento

3. Diseño para la implementación del sistema de gestión de seguridad de la información en la red Lan del área de hardware en la empresa Uniplex Systems S.A. en guayaquil.

En esta sección se describirá la infraestructura actual 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 empresa en cuanto a seguridad para determinar el punto de partida para la implementación del Sistema de Gestión de Seguridad.

3.1. Análisis De La Situación Actual De La Intranet Corporativa

En este capitulo se habla de los antecedentes de la empresa así como de la ubicación física, además se recopila los datos tanto de red Lan/Wan, como de activos, servidores, y maquinas de uso del personal de Uniplex.

Para obtener la información se procedió a hacer una auditoria de activos en la cual se tuvo la colaboración de las diferentes personas encargadas de cada departamento. En la siguiente tabla se presenta el esquema en el cual se esta obteniendo los datos de cada servidor, desktop, laptop.

TABLA 1. Característica del servidor Domino Lotus

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	

En la auditoria que se hizo también se conoció que se iba a dar un cambio en la red Wan (incremento de ancho de banda) pero solo se consideraron los datos hasta febrero de este año, aparece la información de la red Lan en el siguiente grafico.

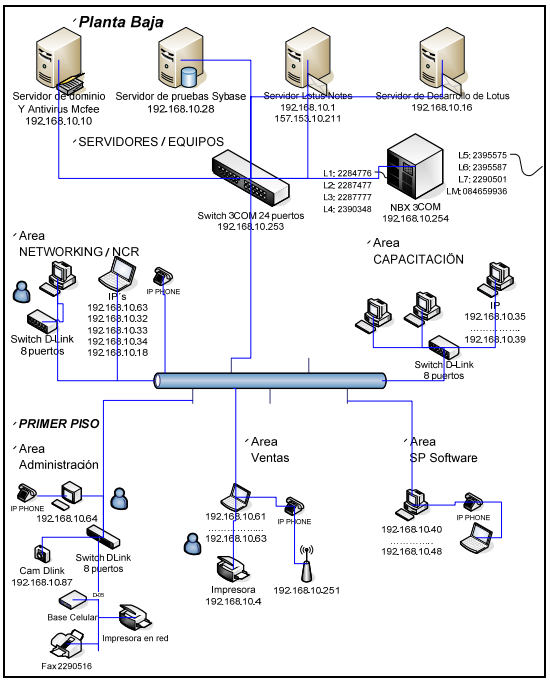

Figura 1. Red LAN de Uniplex

En el análisis acerca de las aplicaciones se hace énfasis en lo que ocurre a nivel de servidores y de restricciones generales para cada usuario de la empresa, por ejemplo con el sistema Lotus existe seguridad a nivel de acceso a cada una de las aplicaciones, 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.

También se audita las funciones de responsabilidad de cada departamento y encargado así como la seguridad física que existe

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 dependiendo de la realidad de la empresa.

Se hace uso de la herramienta Gesdoc Iso de Lotus la cual contiene todos los parámetros de procesos generales y de cada departamento, como muestra se expone el siguiente proceso:

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

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:

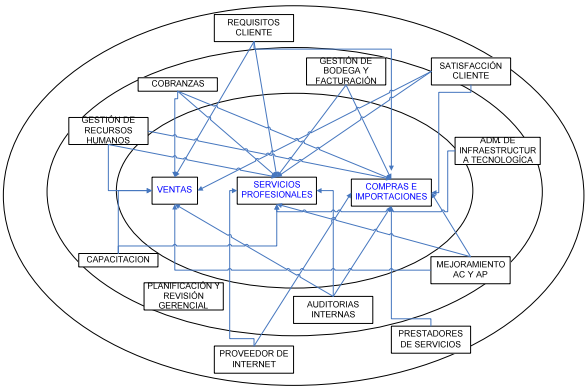

Figura 2. Método de las eclipses para procesos.

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.

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

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.

Se efectúa la escala de valoración en la cual se detalla las tablas respectivas que contienen los estándares para confidencialidad, integridad, 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, en la cual se dispone criterios para determinar las categorías de las amenazas, y de las vulnerabilidades.

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

Software

Activos Físicos

Servicios

Personas

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) de los parámetros anteriormente expuestos.

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.

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.

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.

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
	A1: Fuego	Baja	Es baja la probabilidad de

Figura 3. Extracto de tabla de exposición de 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.

Se describe las principales responsabilidades de los miembros implicados en la seguridad de la información para la gestión de los riesgos basados en los dominios

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

Figura 4. Ejemplo de cálculo para la valoración del riesgo

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.

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.

Se redacta un documento de políticas de seguridad de la información para el uso del personal de la empresa, así como se elabora la factibilidad de los controles respectivos para hacer frente a los riesgos y vulnerabilidades encontradas.

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.

4. IMPLEMENTACIÓN DEL PROYECTO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA INTRANET DE UNIPLEX

Aquí se detallan los parámetros y procedimientos de la implementación del proyecto en la empresa.

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 en base a los análisis realizados en el capítulo 3 y a los controles seleccionados para el manejo de vulnerabilidades y riesgos.

Se detalla también aspectos legales del ecuador que tiene que ver con las tecnologías, robo de activos e información y propiedad intelectual.

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 a lo dicho anteriormente 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	Funcionamiento no	

Figura 5. Extracto de tabla tratamiento de riesgos

4.3. Implementación de los Controles Seleccionados Acorde al Manual de Procedimientos

En este 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.

Se detalla cada uno de los documentos que se han redactado para controlar o eliminar las vulnerabilidades y riesgos encontrados, dando énfasis a todos los parámetros desde como hacer uso de las contraseñas, manejo de software, respaldos hasta la seguridad misma tanto física como de la información.

Se asigno responsabilidades sobre la seguridad de la información, se especifico el proceso de autorización de recursos para el tratamiento de la información,

también para la gestión de activos de la red, el procedimiento para capacitación, recursos humanos, seguridad física para el tratamiento de robo, eventos naturales, etc.

A continuación se muestra el diagrama del departamento en la cual se baso para el plan ante eventos de desastres naturales o robo.

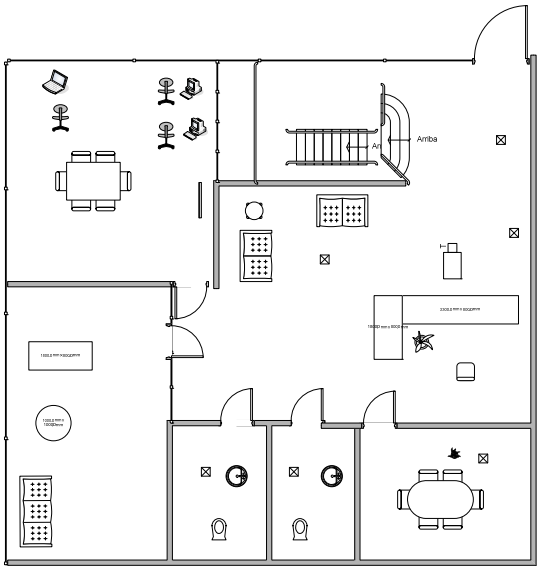

Figura 6. Esquema físico de las instalaciones de Uniplex

4.3. 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.

TABLA 2. Ejp Costo de Diseño

RECURSO	DESCRIPCION	CANTIDAD	COSTO TOTAL ($)
Personal	Viáticos y Comisiones por dos meses	2	1000
Varios	Documentación de Norma ISO 27002	1	100
TOTAL			1100

5. Conclusiones y Resultados

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

Una de las ventajas de la norma ISO 27002 es que puede ser implementada tanto en empresas pequeñas como en grandes organizaciones.

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.

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.

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.

5. Agradecimientos

Primordialmente agradecemos a Dios por toda la paciencia, sabiduría brindada para la ejecución de nuestra tesis, por habernos llenado de dedicación perseverancia para la buena realización de la misma.

A nuestros padres por todo el amor y el apoyo constante. A nuestros amigos, amigas y demás personas que de alguna y otra forma nos ayudaron para emprender y culminar nuestra tesis.

6. Referencias

[1]ISO – IEC., Estándar Internacional ISO/IEC 27001. Tecnología de la Información – Técnicas de Seguridad – Sistemas de Gestión de Seguridad de la Información – Requerimientos No. de Referencia: ISO/IEC 27001:2005., Primera Edición. Octubre 15 del 2005.

[2]ISO – IEC., Estándar Internacional ISO/IEC 17799. Tecnología de la Información – Técnicas de Seguridad – Código para la práctica de Seguridad de la Información., Segunda Edición. Junio 15 del 2005.

[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 PRA. Plan de Seguridad Informática (PSI) Argentina, (Tesis de la Facultad de Ingeniería en Sistemas de La Universidad de Córdova)., Octubre 2002.

[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