Escuela Superior Politécnica del Litoral

CENTRO DE EDUCACIÓN CONTÍNUA

Diplomado en Auditoría Informática
V Promoción

PROYECTO

TEMA

"Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001, para la Dirección Regional INEC"

AUTOR

Carlos Saltos Peña

AÑO

2011

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

CENTRO DE EDUCACION CONTINUA

DIPLOMADO EN AUDITORIA INFORMATICA

V PROMOCIÓN

PROYECTO

TEMA

"ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, PARA LA DIRECCION REGIONAL LITORAL INEC"

AUTOR

CARLOS SALTOS PEÑA

AÑO

2011

RESUMEN

En el proyecto se propone una solución de seguridad a la Dirección Regional del Litoral (DILIT) del INEC, tomando como base estándares internacionales.

En el primer capítulo se dan a conocer los lineamientos bases de la seguridad de la información, una visión general sobre la gestión de riesgos, las diferentes alternativas para el tratamiento de los riesgos identificados, la evolución de la norma ISO 27001, y finalmente una descripción de la Norma ISO 27001:2005.

En el segundo capítulo se presenta una descripción de los 11 dominios del estándar ISO 27001, en el cual se documenta los procesos y procedimientos que ayudarán a garantizar la seguridad de la información.

En el tercer capítulo se realiza un análisis de la situación actual de INEC-DILIT, identificando los activos más relevantes para la institución y se realiza una identificación, análisis y evaluación de vulnerabilidades. Asi como el plan de tratamiento de los riesgos

En el cuarto capítulo se presenta una descripción sobre las acciones apropiadas así como a los responsables para minimizar los riesgos identificados, con el objeto de posteriormente realizar la implementación del SGSI en base a los controles seleccionados, para obtener finalmente el manual de procedimientos para la implementación del SGSI.

En el capítulo final se ofrecen las conclusiones y recomendaciones del proyecto.

ÍNDICE

INDICE DE FIGURAS

INDICE DE TABLAS

INTRODUCCIÓN

El presente proyecto tiene como objetivo la Implementación de un Sistema de Gestión de Seguridad de la Información para la Dirección Regional Litoral Inec en base a la Norma ISO 27001 con el fin de lograr una gestión de la información de manera organizada, adecuada y garantizando que los riesgos de seguridad de la red sean minimizados en base a los procedimientos para el tratamiento de los mismos.

Para poder realizar este proyecto se consideró como bases, las guías que se indican en la Norma ISO 27001, acorde a la realidad de la institución.

También se realizó un análisis preventivo y correctivo en mejora de la administración y gestión de la seguridad de la información, conforme a la Norma ISO 27001 identificando las vulnerabilidades presentes en la organización.

NECESIDAD DEL NEGOCIO

Dado que el INEC es la institución rectora de las estadísticas nacionales, tiene la necesidad de brindar datos de calidad basados en un entorno de seguridad razonable.

ALCANCE, OBEJTIVOS

El alcance del SGSI Dilit-Inec se centra en uno de sus procesos críticos del cual una vez realizado el análisis podría ser replicado a los otros procesos bases.

A continuación se describe el objetivo general y los específicos del proyecto

Objetivo General

Diseñar un sistema de Gestión de la Seguridad de la Información de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.

Objetivos Específicos

- Introducir a la Institución en la norma ISO/IEC 27001
- Diseñar un esquema que permita la posterior implantación del sistema de Gestión de la Seguridad de la Información.
- Identificación de activos críticos.
- Desarrollo basado en riesgos.
- Diagnosticar la situación de seguridad de la información institucional.
- Generación de políticas de Seguridad de la información.

METODOLOGIA

La propuesta metodológica se basa en los siguientes pasos, considerando el ciclo PDCA, en un plazo estimado de 3 meses:

1.- Formalización del Proyecto

Presentación y aprobación del proyecto por parte de Dirección General.

2.- Equipo de trabajo

Se asignará de forma directa al proyecto a un sólo funcionario del Departamento de Plataforma Tecnológica, con la participación en el caso de ser requerida de otros funcionarios de los diversos departamentos.

3.- Análisis de la organización

Se realiza un profundo análisis diferencial de seguridad, comparando la situación actual de la Institución con los requisitos de ISO 27001, determinando también otras medidas de seguridad adicionales que puedan ponerse de manifiesto durante el proceso de análisis. Se actuará sobre todos los 11 dominios.

PLAN DE TRABAJO

El siguiente esquema general de trabajo, es el que permitió el desarrollo exitoso del proyecto, consta de:

Preliminares administrativos (aceptación del tema por parte de la empresa y del CEC)

- ✓ Adecuación de un lugar de trabajo.
- ✓ Capacitación necesaria para iniciar el proyecto (compra de normas).

Inicio de Actividades

- ✓ Especificación del alcance.
- ✓ Análisis de la situación actual.
- ✓ Establecimiento de Requerimientos del SGSI.
- ✓ Identificación, análisis y evaluación de vulnerabilidades.
- ✓ Plan de tratamiento de riesgos.
- ✓ Estudio de factibilidad de aplicación de los controles.
- ✓ Selección de controles y objetivos de control.
- ✓ Costeo referencial de diseño e implementación.

CAPITULO I: INTRODUCCIÓN Y NORMAS ISO PARA LA SEGURIDAD DE LA INFORMACIÓN

1.1. CONCEPTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

1.1.1. INTRODUCCIÓN

Actualmente la seguridad de la información en muchas organizaciones es tratada como un problema tecnológico, sin considerar que la seguridad de la información es parte de la organización y de la gestión, lo que se traduce en que exclusivamente las mismas no puedan afrontar ataques provenientes de todos los ámbitos.

No es suficiente contar con tecnología sofisticada, la gestión implica conocer la situación de la que queremos tratar y estar claro hacia dónde queremos ir, es decir, determinar un objetivo, alcance y tomar las acciones necesarias para conseguirlo. La definición de un modelo de gestión de la seguridad de la información involucra a toda la organización y no sólo al área encargada de diseñar e implantar el modelo, lo cual trae como resultado el éxito o fracaso del proyecto tanto en su implantación como en su mantenimiento, es así que se debe fomentar un cambio de cultura para concienciar a toda la institución acerca de importancia de la seguridad.

1.1.2. DEFINICIÓN DE SEGURIDAD DE LA INFORMACIÓN

La información de una institución es uno de los activos más importantes que puedan tener por lo que tiene un valor alto para la organización y por lo tanto se deberían desarrollar diferentes mecanismos para asegurar de forma razonable una protección adecuada. Los objetivos generales de la seguridad de la información son proteger a la organización de amenazas, minimizar los daños y maximizar el retorno de las inversiones y las oportunidades del negocio.

Considerando que la información de una organización puede adoptar diversas formas, como: escrita en papel, impresa, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en vídeo o hablada, debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad:

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

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de procesos.

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

La seguridad de la información se consigue implantando un conjunto apropiado de controles, tales como políticas, procedimientos, estructuras organizativas y funciones de software cuyo objetivo es asegurar que se cumplen con los requisitos de seguridad de la información.

1.2. GESTIÓN DE RIESGOS

1.2.1. INTRODUCCIÓN

La gestión del riesgo es una parte fundamental de la Norma ISO 27001, los controles en el anexo A del estándar deberían ser seleccionados en base a los resultados de la evaluación del riesgo, por lo que se requiere medir y evaluar los riesgos así como revisar y reevaluar los riesgos en una etapa futura para asegurar que se tiene implantando una eficaz seguridad de información.

1.2.2. DEFINICIÓN RIESGO

Riesgo es el daño potencial que puede surgir por un proceso presente o un evento futuro. Diariamente en ocasiones se lo utiliza como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, el riesgo combina la probabilidad de que ocurra un evento negativo con cuánto daño dicho evento podría causar.

1.2.3. FUENTES RIESGO

Existen diferentes fuentes las cuales pueden tener un impacto en la organización. Una fuente es llamada amenaza. Una amenaza tiene el potencial de causar un incidente no deseado, el cual puede provocar daños a un sistema, a la organización y a los activos. Pueden ser amenazas de la naturaleza, accidentes causados por negligencia o amenazas intencionales causadas por acciones maliciosas. Para que una amenaza cause daño tendría que explorar la vulnerabilidad del sistema, aplicación o servicio.

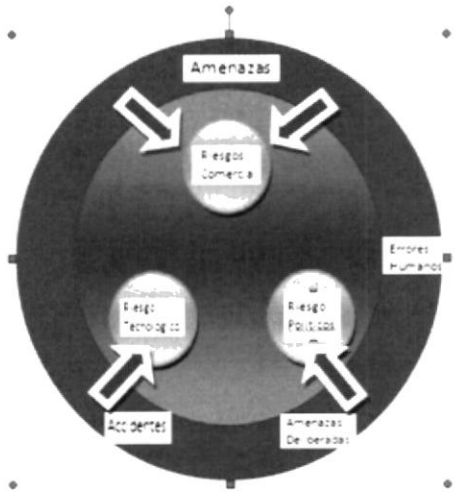

Figura 1.1 Fuentes de Riesgos

1.2.4. ANÁLISIS RIESGO

Para implantar un Sistema de Gestión de Seguridad de Información según ISO 27000, la organización requiere determinar el alcance del estándar en la organización, y en base a ese alcance identificar todos los activos de información. Luego es requerido un análisis de riesgo para identificar qué activos están bajo riesgo. El objetivo del análisis del riesgo es apreciar la magnitud del 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".

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.

• Recomendar las medidas apropiadas que deberían adoptarse para conocer, 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.

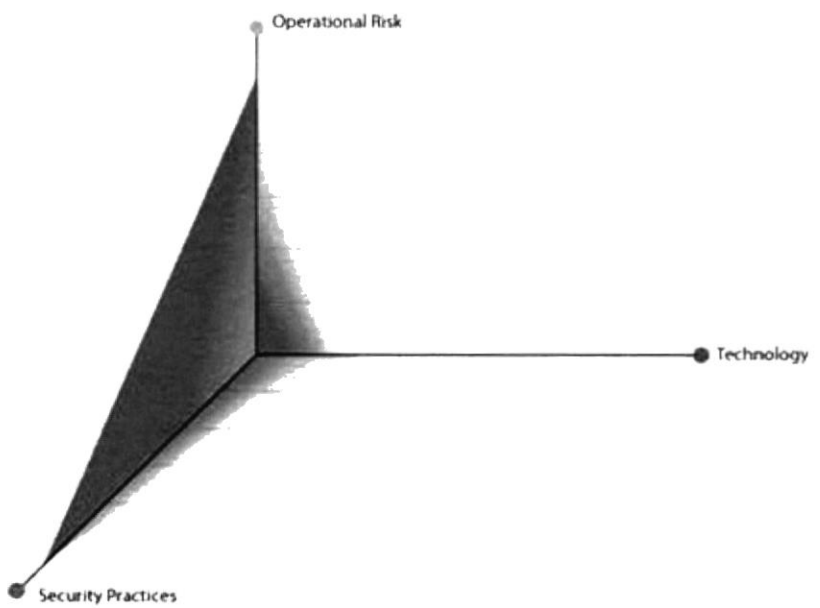

Figura 1.2 Método de Octave

Como se ilustra en la figura 1.2, 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

GUIAS 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.

1.2.5. PROCESO DE EVALUACIÓN DEL RIESGO

La figura 1.2 muestra el proceso de evaluación del riesgo que permite a una organización estar en conformidad con los requerimientos del estándar ISO 27001.

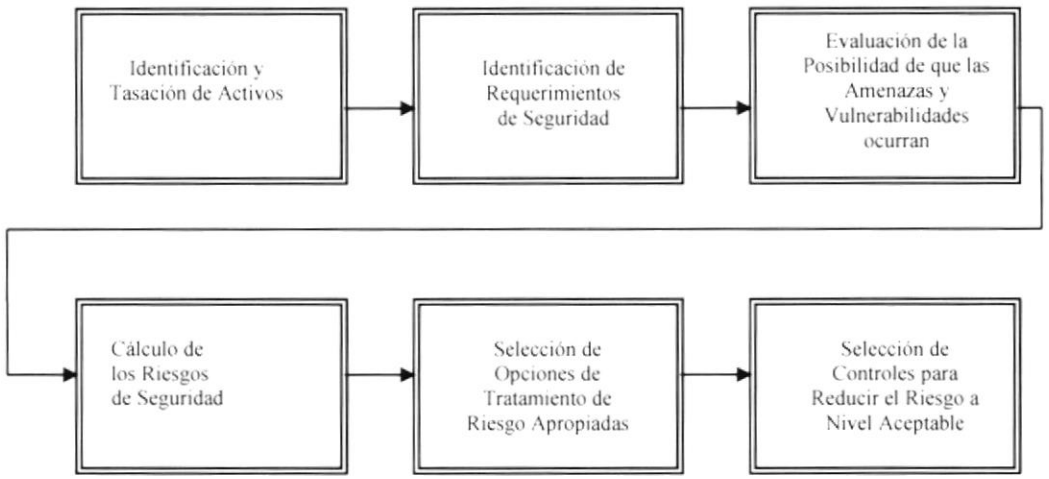

Figura 13. Proceso de Evaluación del Riesgos

Identificación y tasación de activos

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

1) Activos de información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad.

2) Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contienen resultados importantes del negocio.

3) Activos físicos: Equipos de comunicación y computación, medios magnéticos, ópticos y otros equipos técnicos.

4) Personas: Personal, clientes, suscriptores.

5) Imagen y reputación de la compañía.

6) Servicios: Servicios de computación y comunicación, otros servicios técnicos.

Para poder encontrar la protección adecuada para los activos, es necesario evaluar su valor en términos de su importancia para el negocio.

Identificación de requerimientos de seguridad

Con el objetivo de identificar los requisitos de seguridad de la organización, es recomendable 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 ello se identifican 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 satisfacer la organización, sus organismos de control, 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 eventualmente por las amenazas, causando incidentes no deseados, que pudieran terminar causando pérdidas, daño o deterioro a los activos.

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 criterios de seguridad de la información y otros activos;

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

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 institución.
2	Uso interno	Puede solo ser revelada y proporcionado en la Institución (no disponible a terceras partes). Si el contenido fuera revelado, no hubiera mucho efecto en las operaciones.
3	Secreto	Puede ser solo revelado y proporcionado a partes especificas y departamentos. Si el contenido fuera revelado, hubiera un gran efecto en las operaciones.
4	Alta confidencialidad	Puede ser solo revelado y proporcionado a partes especificas. Si el contenido fuera revelado, hubiera un efecto irrecuperable en las operaciones.

Tabla 1.1 Estándares para confidencialidad

Activos de información (Integrida	Clase	Descripción
1	No necesaria	Usado solo para consulta. No tiene posibles problemas
2	Necesaria	Si el contenido fuera falsificado, hubiera problema, pero estos no afectarían mucho las operaciones.
3	Importante	Si la integridad se perdiera, hubiera un efectofatal en las operaciones.

Tabla 1.2. 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
2	Mediano	Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones. 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.

Tabla 1.3. 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	Categoría	Descripción
1	Bajo	Hay una baja probabilidad. La frecuencia de ocurrenciaes 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 ocurrenciaes una vez al mes o más.

Tabla 1.4 Criterios para determinar las categorías de las amenazas

Vulnerabilidades		
Probabilidad de Ocurrencia	Categoría	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 1.5. Criterios para determinar las categorías de las vulnerabilidades

1.2.6. SELECCIÓN DE OPCIONES PARA EL TRATAMIENTO DEL RIESGO

Cuando los riesgos han sido identificados y evaluados, la organización debería identificar y evaluar la acción más apropiada para tratar los riesgos, lo que se conoce como el Plan de Tratamiento de Riesgos (PTR), que es un documento o conjunto de ellos, de vital importancia para el SGSI. El objetivo fundamental es describir de forma bien clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, qué recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las posibles prioridades en la ejecución de las actualizaciones.

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 controles pertinentes para disminuirlos a niveles de aceptación previamente identificados por la empresa.

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

Aceptación del riesgo

Es probable que en la empresa se presenten 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 generalmente adoptada para la

organización, cuando es muy difícil, tanto técnica como económicamente llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente factible, transferir el riesgo a un tercero, como una empresa 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.
Lo que debe estar claro, es que al terciarizar 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 organización.

Selección de controles para reducir los riesgos a un nivel aceptable

La selección de controles debe ser sustentada por los resultados de la evaluación del riesgo. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y qué forma debe tener.
Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados, tales como:

- Uso de controles.
- Transparencia del usuario.

- Ayuda otorgada a los usuarios para desempeñar su función.
- Relativa fuerza de controles.
- Tipos de funciones desempeñadas.

1.2.7. RIESGO RESIDUAL

Una vez que las decisiones del tratamiento del riesgo han sido implementadas, siempre habrá un riesgo residual. Es necesario calcular en cuánto las decisiones del tratamiento del riesgo ayudan a reducir el riesgo, y cuánto queda de riesgo residual. El riesgo residual es definido como "aquel riesgo que queda en la empresa después de haber implementado el plan de tratamiento del riesgo".

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 describe en forma general en el capítulo II.

1.4. ESTRUCTURA DEL SISTEMA DE GESTIÓN

1.4.1. INTRODUCCIÓN

Un Sistema de Gestión es una herramienta de la que dispone la Gerencia para dirigir y controlar un determinado ámbito.

Las empresas tienen la posibilidad de implantar un número variable de estos Sistemas de Gestión para mejorar la organización y beneficios sin imponer una carga a la organización.

1.4.2. OBJETIVO

Los Sistemas de Gestión se aplican en el marco de todas las actividades que se ejecutan en la organización y son válidos solo si cada uno de ellos interactúa con los demás armónicamente.

El objetivo de los estándares de Gestión de ISO es llegar a un único Sistema de Gestión que contemple todos los aspectos necesarios para la organización, basándose en el ciclo PDCA y el proceso de mejora continua.

1.4.3. OPERATIVIDAD DE LOS SISTEMAS DE GESTIÓN

Los Sistemas de Gestión adaptados al tipo particular de organización, debe operar de tal manera que se dé la confianza apropiada; es decir que:

- Sean bien comprendidos por la totalidad de los protagonistas
- Operan en forma eficaz
- Los resultados satisfacen las expectativas de las partes interesadas
- Se enfatiza las acciones preventivas ante cualquier clase de problemas

1.5. NORMAS ISO 27000

1.5.1. 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 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.

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.

1.5.2. DEFINICIÓN DE LAS NORMAS ISO 27000

La serie ISO 27000 es una Familia de Estándares internacionales para Sistemas de Gestión de Seguridad de la Información (SGSI), que propone

requerimientos de sistemas de gestión de seguridad de la información, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

• ***ISO 27000***

Contiene términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

• ***ISO 27001***

Es la norma principal de requerimientos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual serán certificados por auditores externos los SGSI de las organizaciones. Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, lista en forma de resumen los objetivos de control y controles que desarrolla la ISO17799:2005 (ISO27002), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI.

• ***ISO 27002 (ISO 17799)***

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 cláusulas. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO17799:2005.

• ***ISO 27003***

En fase de desarrollo; probable publicación en Octubre de 2008. Contendrá una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

• ***ISO 27004***

Especificá las métricas y las técnicas de medida aplicables para determinar la eficiencia y efectividad de la implantación de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

• ***ISO 27005***

Consiste en una guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI.

• ***ISO 27006***

Especificá el proceso de acreditación de entidades de certificación y el registro de SGSI.

1.5.3. BENEFICIOS DE LAS NORMAS ISO 27000

Entre los beneficios que se obtienen por la implementación del conjunto de normas ISO 27000 en una organización, se tiene:

- ✓ Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- ✓ Reducción del riesgo de pérdida, robo o corrupción de información. Los clientes tienen acceso a la información a través medidas de seguridad.
- ✓ Los riesgos y sus controles son continuamente revisados.
- ✓ Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- ✓ Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- ✓ El sistema se integra con otros sistemas de gestión (ISO9001, ISO14001, OHSAS).
- ✓ Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- ✓ Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- ✓ Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

✓ Reduce costes y mejora los procesos y servicio. Aumenta la motivación y satisfacción del personal.

✓ Seguridad garantizada en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

1.5.4. NORMATIVAS DE REFERENCIA

Para la aplicación de la norma ISO 27001:2005, es indispensable tener en cuenta la versión de ISO 27002:2005

1.6. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

1.6.1. INTRODUCCIÓN

Antecedentes

La poca seguridad que hubo en los orígenes del boom de Internet hizo detonar la alarma, de tal forma que la seguridad de la información empezó a tomarse en serio, tanto en el ámbito empresarial, como comercial y por supuesto jurídico-legal.

Se cree que un código de normas de la seguridad apoyaría los esfuerzos de los gerentes de tecnología de la información en el sentido que facilitaría la toma de decisión de compra, incrementaría la cooperación entre los múltiples departamentos por ser la seguridad el interés común y ayudaría a consolidar la seguridad como prioridad empresarial.

Desde su publicación por parte de la Organización Internacional de Normas en diciembre de 2000, ISO 17799 surge como la norma técnica de seguridad de la información reconocida a nivel mundial. ISO 17799 se define como "un completo conjunto de controles que incluye las prácticas exitosas de seguridad de la información".

Norma ISO 27001

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto sobre el que se construye ISO 27001.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información son conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Alcance de la Norma ISO 27001

ISO/IEC 27001:2005 es una norma que establece los requisitos de los sistemas de gestión de la seguridad de la información. Esta norma está diseñada para asegurar la selección de los controles de seguridad adecuados y proporcionados para proteger la información y dar la confianza a partes interesadas incluyendo a los clientes de una empresa.

Objetivo de la Norma ISO 27001

Entre los objetivos que se pretenden cumplir con la Norma ISO 27001, tenemos:
Potenciar un servicio final: Esta opción supone la implantación de un SGSI ligado a los servicios y/o procesos de negocio. De esta forma, se da un valor añadido a los mismos, bañándolos de una capa de seguridad adicional.

Reforzar los servicios y procesos internos: Esta filosofía pretende implantar el SGSI para fortalecer determinados servicios y procesos internos, en los que una mejora en la seguridad pueda suponer una ventaja para la organización.

Potenciar la gestión interna: Por último, otra de las filosofías que a veces se utiliza para decidir el alcance es identificar aquellas partes de la organización en las que la implantación del SGSI, como sistema de gestión, sirva para potenciar y estructurar la gestión interna. Es quizás una de las filosofías más discutibles, ya que existen multitud de sistemas de gestión centrados en distintos aspectos y quizás el de la seguridad pueda no ser el más indicado en todos los casos, pero en determinadas situaciones puede ser una opción.

1.6.2. REQUISITOS DE LA DOCUMENTACION DEL SGSI

Un Sistema 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.

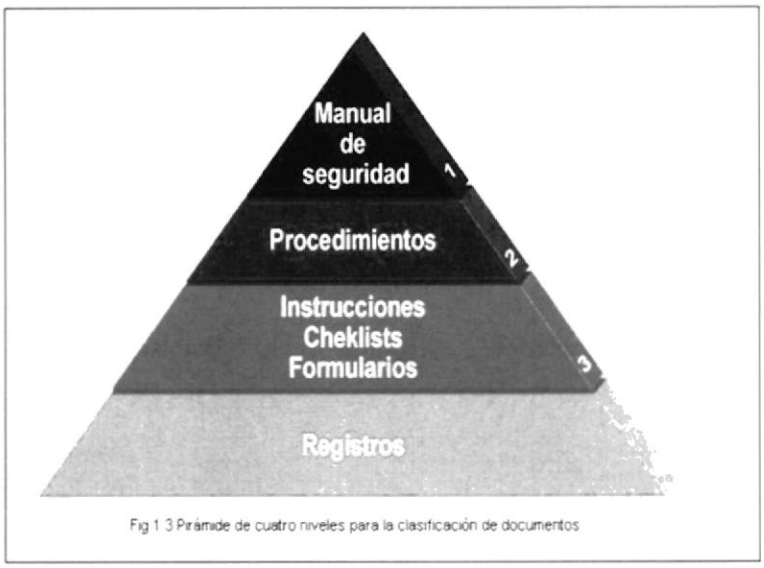

Fig 1.3 Pirámide de cuatro niveles para la clasificación de documentos

La documentación de un SGSI deberá incluir:

Documentos de Nivel 1

Forman el manual de seguridad. Son los siguientes:

Alcance del SGSI: ámbito de la organización que queda sometido al SGSI. 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.

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 SGSI, 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 SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

1.6.3. CONTROL DE DOCUMENTOS

Todos los documentos requeridos por el SGSI 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 re aprobaciones 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.

1.6.4. RESPONSABILIDADES DE ADMINISTRACIÓN

a) La administración proveerá evidencias de sus compromisos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del ISMS a través de una serie de acciones.

b) **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).

1.6.5. IMPLEMENTACION DE UN SGSI

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, 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 SGSI:

Plan (Establecer el SGSI)

- Definir el alcance del SGSI en términos del negocio.
- Definir una política de seguridad

- Definir una metodología de evaluación del riesgo apropiada para el SGSI 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 27001 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 SGSI)

- 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 SGSI.
- Gestionar los recursos necesarios asignados al SGSI 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 (Monitorizar y revisar el SGSI)

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión
- Revisar regularmente la efectividad del SGSI
- 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 SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección
- Actualizar los planes de seguridad
- Registrar acciones y eventos

Act (Mantener y mejorar el SGSI)

La organización deberá regularmente:

- Implantar en el SGSI 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 logren los objetivos previstos.

CAPITULO II: DESCRIPCIÓN DE LOS 11 DOMINIOS DEL ESTÁNDAR ISO 27001

2.1. POLÍTICA DE SEGURIDAD

2.1.1. DOCUMENTO DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La gerencia debe aprobar el documento de política de seguridad de información y es deber de la gerencia publicar este documento a toda la organización.

2.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

2.2.1. ORGANIZACIÓN INTERNA

Se debe establecer una estructura de la seguridad de la información, de tal manera que satisfaga todos los requerimientos, para lo cual es indispensable la participación de los representantes de las diferentes áreas dentro de la organización para cubrir las distintas necesidades.

2.2.2. PARTES EXTERNAS

El acceso de terceros a los recursos de tratamiento de información no debe comprometer la seguridad de la información.

2.3. ADMINISTRACIÓN DEL RECURSO

2.3.1. RESPONSABILIDAD PARA LOS RECURSOS

Se debe asignar a los recursos de la organización, propietarios quienes serán los responsables de mantener una protección adecuada.

2.3.2. CLASIFICACIÓN DE LA INFORMACIÓN

Dar a cada recurso la protección adecuada de acuerdo a su clasificación, esta clasificación se dará en base a niveles de sensibilidad y criticidad.

2.4. SEGURIDAD DE RECURSOS HUMANOS

2.4.1. SEGURIDAD EN LA DEFINICIÓN DEL TRABAJO Y LOS RECURSOS

Asegurar que cada persona dentro de la organización comprenda sus responsabilidades, ya que es un factor que influye en la preservación de la seguridad de la información.

2.4.2. DURANTE EL EMPLEO

Asegurar que los empleados, contratistas y usuarios de una tercera parte estén conscientes de sus responsabilidades, de tal manera que sus roles sean ejecutados adecuadamente. Además debe conocer las políticas establecidas y aplicarlas.

2.4.3. TERMINACIÓN O CAMBIO DE EMPLEO

Manejar de manera ordenada la terminación o cambio de empleo, en donde está incluido el retiro de los derechos de acceso, retorno de equipos y finalizar con las responsabilidades respectivas.

2.5. SEGURIDAD FÍSICA Y AMBIENTAL

2.5.1. LAS ÁREAS SEGURAS

Los recursos importantes para el tratamiento de la información deben ser ubicados en áreas seguras de tal manera que se provenga el acceso no autorizado.

2.5.2. SEGURIDAD DE LOS EQUIPOS

Garantizar la continuidad del negocio mediante la protección adecuada de los activos de la organización.

2.6. GESTIÓN DE COMUNICACIONES Y OPERACIONES

2.6.1. PROCEDIMIENTOS Y RESPONSABILIDADES DE OPERACIÓN

Establecer responsabilidades y procedimientos para la gestión y operación de todos los recursos de tratamiento de información, de tal manera que se consiga reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

2.6.2. GESTIÓN DE SERVICIOS EXTERNOS

Establecer un nivel apropiado de seguridad de la información y entregar el servicio de acuerdo con el contratista.

2.6.3. PLANIFICACIÓN Y ACEPTACIÓN DEL SISTEMA

Garantizar el funcionamiento del sistema, además el sistema debe ser escalable de modo que permita crecimientos futuros y asegurar la continuidad del negocio.

2.6.4. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Evitar crear agujeros de seguridad mediante la prevención y detección de software malicioso.

2.6.5. GESTIÓN INTERNA DE RESPALDO

Garantizar la continuidad del negocio, mediante la preservación de los servicios del tratamiento de la información y comunicaciones.

2.6.6. GESTIÓN DE LA SEGURIDAD DE REDES

Proteger la información de las redes y tener una infraestructura estable de redes de comunicaciones.

2.6.7. UTILIZACIÓN DE LOS MEDIOS DE INFORMACIÓN

Usar apropiadamente los medios de información de tal manera que se minimicen los daños a los activos.

2.6.8. INTERCAMBIO DE INFORMACIÓN

Garantizar la seguridad de la información, mantener la integridad para lo cual se debe seguir procedimientos que controlan los intercambios de información.

2.6.9. SERVICIOS DE COMERCIO ELECTRÓNICO

Garantizar el uso adecuado del comercio electrónico y evitar la pérdida de seguridad.

2.6.10. MONITORIZACIÓN

Asegurar que los sistemas se usan adecuadamente y cumplen los requerimientos establecidos, en caso de incidentes de seguridad estos deben ser registrados.

2.7. CONTROL DE ACCESOS

2.7.1. REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS

Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio. Se deberían tener en cuenta para ello las políticas de distribución de la información y de autorizaciones.

2.7.2. GESTIÓN DE ACCESO DE USUARIOS

Se debería establecer procedimientos formales para controlar la asignación de los derechos de acceso a los sistemas y servicios.

Estos procedimientos deberían cubrir todas las etapas de acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios.

2.7.3. RESPONSABILIDADES DE LOS USUARIOS

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de la eficacia de las medidas de control de acceso, en particular respecto al uso de contraseñas y a la seguridad del material puesto a su disposición.

2.7.4. CONTROL DE ACCESO A LA RED

Hay que asegurarse que el acceso de los usuarios a las redes y sus servicios no comprometan la seguridad de dichos servicios, por medio de:

a) Interfaces adecuadas entre la red de la organización y las redes públicas o las privadas de otras organizaciones;

b) Mecanismos adecuados de autenticación para los usuarios y los equipos;

c) Control de los accesos de los usuarios a los servicios de información.

2.7.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO

Las prestaciones de seguridad a nivel de sistema operativo se deberían utilizar para restringir el acceso a los recursos del computador, los que deberían ser capaces de:

a) Identificar y verificar la identidad de cada usuario autorizado, y si procede, el terminal o la ubicación física del mismo;

b) Registrar los accesos satisfactorios y fallidos al sistema;

c) Registrar el uso de privilegios especiales al sistema;

d) Generar una alarma cuando se quebrante las políticas de seguridad;

e) Suministrar mecanismos, adecuados de autenticación;

f) Cuando proceda, restringir los tiempos de conexión de usuarios.

2.7.6. CONTROL DE ACCESO A LAS APLICACIONES

Se deberían restringir el acceso lógico al software y a la información sólo a los usuarios autorizados.

2.7.7. INFORMÁTICA MÓVIL Y TELETRABAJO

Se deberían considerar los riesgos de trabajar en un entorno desprotegido cuando se usa informática móvil y aplicar la protección adecuada. En el caso del teletrabajo la organización debería implantar protección en el lugar del teletrabajo y asegurar que existen los acuerdos adecuados para este tipo de trabajo.

2.8. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

2.8.1. REQUISITOS DE SEGURIDAD DE LOS SISTEMAS

Todos los requisitos de seguridad, incluyendo las disposiciones para contingencias, la infraestructura, las aplicaciones de negocio y las aplicaciones

desarrolladas por usuario; deberían ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

2.8.2. SEGURIDAD DE LAS APLICACIONES DEL SISTEMA

Se deberían diseñar dentro de las aplicaciones las medidas de control y las pistas de auditoria o los registros de actividad. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida. Se pueden requerir medidas y controles adicionales en los sistemas que procesen o tengan impacto sobre activos sensibles, valiosos o críticos para la organización.

2.8.3. CONTROLES CRIPTOGRÁFICOS

Se deberían usar sistemas y técnicas criptográficas para proteger la información sometida a riesgo, cuando otras medidas y controles no proporcionen la protección adecuada.

2.8.4. SEGURIDAD DE LOS ARCHIVOS DEL SISTEMA

El mantenimiento de la integridad del sistema debería ser responsabilidad del grupo de desarrollo o de la función del usuario a quien pertenezcan las aplicaciones del sistema o el software.

2.8.5. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE

Se deberían controlar estrictamente los entornos del proyecto y de soporte. Los directivos responsables de los sistemas de aplicaciones también lo deberían ser de la seguridad del entorno del proyecto o su soporte. Se deberían asegurar de la revisión de todo cambio propuesto al sistema para comprobar que no debilite su seguridad o la del sistema operativo.

2.8.6. GESTIÓN DE VULNERABILIDAD TÉCNICA

Se pretende reducir riesgos, resultado de la explotación de vulnerabilidades técnicas publicadas. La misma que debe ser puesta en ejecución de una manera eficaz, sistemática, y repetible con las medidas tomadas para confirmar su

eficacia.

2.9. GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

2.9.1. DIVULGACIÓN DE EVENTOS Y DE DEBILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Para asegurar los eventos y las debilidades de la seguridad de la información asociados a los sistemas de información, los procedimientos formales de la divulgación y de escalada del acontecimiento deben estar en lugar. Todos los empleados, contratistas y usuarios de los terceros deben ser enterados de los procedimientos para divulgar diversos tipos de eventos y de debilidad que pudieron tener un impacto en la seguridad de activos de organización.

2.9.2. ADMINISTRACIÓN DE INCIDENTES Y MEJORA DE LA SEGURIDAD DE LA INFORMACIÓN

Se deben definir las responsabilidades y procedimientos para manejar acontecimientos y debilidades de la seguridad de la información con eficacia una vez que se hayan divulgado. Un proceso de la mejora continua se debe aplicar a la respuesta, supervisión, evaluación, y administración total de los incidentes de seguridad de la información.

2.10. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

2.10.1. ASPECTOS DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio debería incluir controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales. Así como reducir la interrupción causada por desastres y fallas de seguridad.

2.11. CUMPLIMIENTO

2.11.1. CUMPLIMIENTO DE REQUISITOS LEGALES

Con este control se busca evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo

requisito de seguridad. El diseño, operación, uso y gestión de los sistemas de información puede estar sujeto a requisitos estatutarios, regulatorios y contractuales de seguridad.

2.11.2. REVISIÓN DE LA POLITICA DE SEGURIDAD Y CONFORMIDAD TÉCNICA

Se requiere asegurar la conformidad de los sistemas con las políticas y normas de seguridad. Se deberían hacer revisiones regulares de la seguridad de los sistemas de información.

2.11.3. CONSIDERACIONES SOBRE LA AUDITORIA DE SISTEMAS

Con este control se busca maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema; estableciendo la necesidad de controles para salvaguardar los sistemas operativos y las herramientas de auditoria durante las auditorias del sistema.

CAPÍTULO III: DISEÑO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

En este capítulo se describe la infraestructura actual de la red de DILIT-INEC, los datos obtenidos son resultado de la información recogida en colaboración del administrador de la red de, inventario realizado y revisión de las instalaciones físicas de la red.

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

3.1.1. ANTECEDENTES

Dilit-Inec es una persona jurídica de derecho público, sin fines de lucro, a las demás leyes pertinentes de la República del Ecuador y a su Estatuto, aprobado mediante Acuerdo Ministerial mediante Decreto No. 323 del 27 de Abril de 1976 publicado en el Registro Oficial No. 82 del 7 de Mayo del mismo año.

Fue creada con el objetivo principal de desarrollar proyectos estadísticos nacionales, bajo los principios de universalidad de la información y libre acceso ; como una herramienta para solventar los diferentes intereses de organismos públicos y privados contando con infraestructura, tecnología de calidad y los soportes necesarios para su funcionamiento.

La Misión de Dilit-Inec es prestar servicios de estadísticas de importancia de acuerdo a los diferentes intereses nacionales.

3.1.2. INFRAESTRUCTURA DE LA RED DE LA INSTITUCIÓN

Ubicación física

La Dirección Regional Litoral del Instituto Nacional de Estadística y Censos opera en un Edificio propio, ubicado en las calles Hurtado y Tungurahua, con vigilancia las 24 horas del día.

El edificio posee tres pisos, distribuidos en dos áreas, las que se encuentran separadas por las escaleras de acceso. En la planta baja funcionan las áreas de Administración de la Plataforma Tecnológica, Comunicación Social, Recepción, Financiero, Servicios Administrativos e Investigaciones Económicas, en el piso superior se encuentra el área de Jurídico, Análisis Estadístico, Dirección General, y en el piso superior, tenemos a Recursos Humanos, Planificación e Investigaciones Sociodemográficas. Con respecto a la disposición física de los servidores de la Institución, estos se encuentran ubicados en planta baja del edificio, en el Área de Administración de la Plataforma Tecnológica que cuenta con una alarma de seguridad para su acceso.

Los pisos ocupados son de concreto, cuentan con cableado estructurado categoría 5, 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

La red LAN cuenta con 4 servidores, 114 estaciones de trabajo de las cuales 4 son clones y 12 son portátiles que se encuentran, distribuidas entre los jefes departamentales como se muestra en la figura 3.1

En el cuarto de servidores se tiene:

- 1 Switch 2024 Baseline 3Com de 24 puertos, de los cuales actualmente se encuentran 14 puertos utilizados.
- Switch 2016 Baselina 3Com de 16 puertos, de los cuales se encuentran 11 puertos en uso.

En la planta baja se tiene:

- 1 Switch 2024 Baseline 3Com de 48 puertos, de los cuales 40 se encuentran utilizados.
- Acces Point D link 642
- En la planta uno se tiene:
- 1 Switch 2024 Baseline 3Com de 48 puertos, de los cuales 26 se encuentran utilizados.
- 1 Acces Point D link 642

En la planta dos se tienen:

- 1 Switch 2024 Baseline 3Com de 48 puertos, de los cuales 41 se encuentran utilizados.
- 1 Acces Point D link 642
- La velocidad de transmisión por la red es de 10 /100 Megabits por segundo.

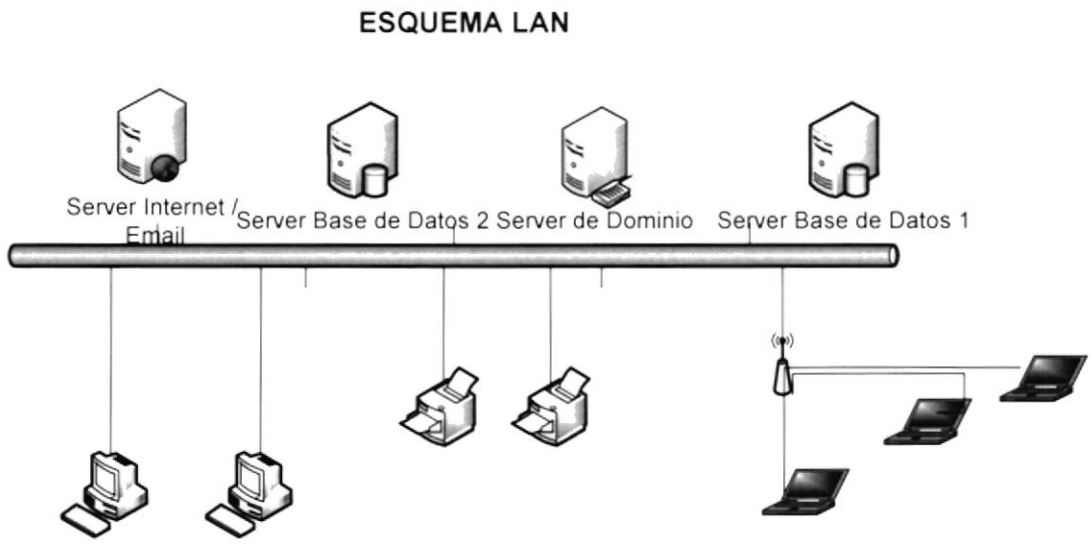

Figura 3.1 Diagrama Lan de la red

Datos de los servidores

A continuación se detallan los seis servidores con los que cuenta la DILIT-INEC:

Base de Datos: Utiliza como base de datos el software Sybase 12.5 levantado sobre el sistema operativo Windows 2003 server r2 usado por el área de Investigaciones Económicas, con las siguientes características del hardware:

Aplicación	Base de Datos	
Procesador	4 Intel Xeon	2.80 Ghz
Disco Duro	600 Gb	
Memoria	12 Gb RAM	
Dirección IP	192.168.10.200	
Sistema Operativo	Windows 2003 Server R2	

Tabla 3.1 Características del servidor de Base de Datos

Base de Datos: Utiliza como base de datos el software Sybase 12.5 levantado sobre el sistema operativo Windows 2003 server r2 usado por el área de Investigaciones Económicas, con las siguientes características del hardware:

Aplicación	Base de Datos	
Procesador	4 Intel Xeon	2.80 Ghz
Disco Duro	600 Gb	
Memoria	12 Gb RAM	
Dirección IP	192.168.10.201	
Sistema Operativo	Windows 2003 Server R2	

Tabla 3.2 Características del servidor de Base de Datos

Internet y Correo Electrónico: Utiliza los beneficios del sistema operativo Linux, el aplicativo Squid para levantar el servidor de correo electrónico, con las siguientes características físicas:

Aplicación	Internet, Correo Electrónico	
Procesador	2 Intel Xeon	2.80 Ghz
Disco Duro	300 Gb	
Memoria	8 GB RAM	
Dirección IP	WAN: 200.107.42.52	LAN: 192.168.10.204
Sistema Operativo	Centos Versión 5.4	

Tabla 3.3. Características de servidor de correo electrónico e internet

Dominio: Para el servicio de Dominio se utiliza el Active Directory, del sistema operativo Windows 2003 Server R2.

Aplicación	Servidor de Dominio	
Procesador	4 Intel Xeon	2.80 Ghz
Disco Duro	300 Gb	
Memoria	12 GB	
Dirección IP	192.168.10.205	
Sistema Operativo	Windows Server 2008 Enterprise Edition	

Tabla 3.4. Características del servidor de dominio

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 estaciones de trabajo tienen instalado el antivirus Mcafee, así como Microsoft Office XP Sp3 Profesional, utilizan como navegador Web a Microsoft Internet Explorer 8.0 y Mozilla Firefox 3.6, tienen instalado además Acrobat Reader. A continuación se detallan las características de los equipos:

CPU	HP 6000 Pro	
Procesador	Intel Core 2 Duo	2.66 Ghz
Disco Duro	80 equipos con 250 GB	18 equipos con 500 GB
Memoria	80 equipos con 3 GB	18 equipos con 4 GB
Sistema Operativo	Windows XP Professional con Service Pack 3	

Tabla 3.5. Característica de los equipos de cómputo desktops Clon

CPU	7 portátiles HP Elitebook	
Procesador	Core i3	2.66 Ghz
Disco Duro	320 GB	
Memoria	4 GB	
Sistema Operativo	Windows XP Professional con Service Pack 3	

Tabla 3.6. Características de las computadoras portátiles EliteBook

CPU	4 equipos desktops	
Procesador	Intel	2.80 Ghz
Disco Duro	320 GB	
Memoria	2 GB	
Sistema Operativo	Windows XP Professional con Service Pack 3	

Tabla 3.7. Características de los equipos de cómputo desktops Imax

CPU	4 portátiles HP Compaq	
Procesador	Intel	2.80 Ghz
Disco Duro	80 GB	
Memoria	1 GB	
Sistema Operativo	Windows XP Professional con Service Pack 3	

Tabla 3.8. Características de las computadoras portátiles HP Compaq

CPU	1 portátil Acer	
Procesador	Intel	1.86 Ghz
Disco Duro	100 GB	
Memoria	1 GB	
Sistema Operativo	Windows XP Professional con Service Pack 3	

Tabla 3.9. Características de la computadora portátil Acer

Además en la red LAN se encuentran conectadas 10 impresoras de las cuales 4 son HP LaserJet 4540N, 5 impresoras Epson LX – 300 y 1 impresora Fargo. 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

Se cuenta con tres enlaces: un enlace a Internet y otro enlace para datos y un Enlace ADSL (asincrónico) de 1.024/1024 Kbps contratado a la compañía Telconet y que es utilizado para acceso del departamento Financiero.
Enlace de Fibra 2 Mbps contratado con la compañía Megadatos de Internet.
Enlace de Fibra 1.5 Mbps contratado con la compañía Megadatos para comunicación con Oficina Matriz.

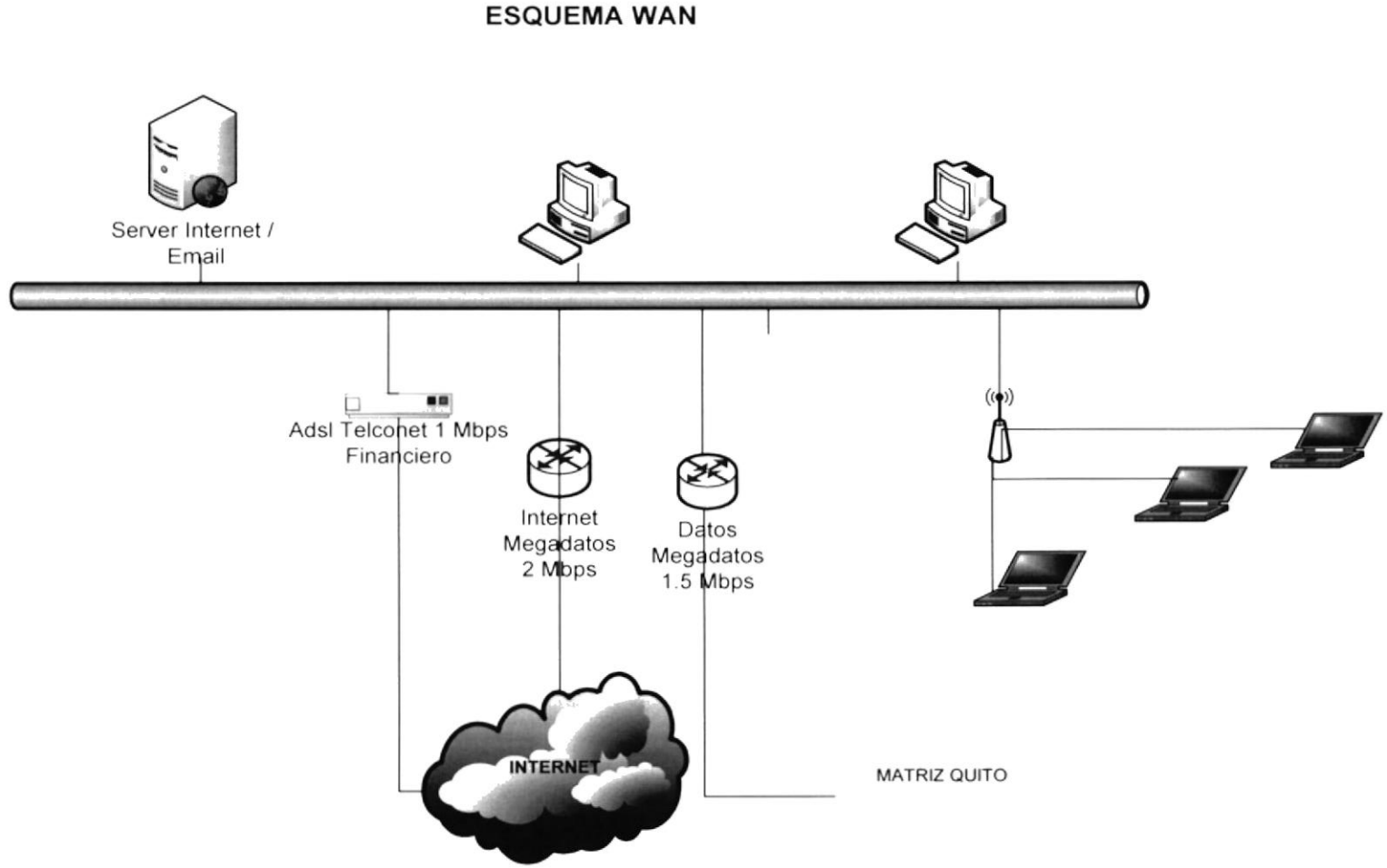

Figura 3.2 Diagrama Wan de la red

Se cuenta con 2 router cisco y un modem que son propiedad de los proveedores del servicio de Internet. Los que se encuentran conectados al Switch 3 Com para proveer tanto del servicio de Internet a la red interna como el acceso de los prestadores hacia los servidores.

Enlaces de comunicación

Dilit-Inec cuenta para su funcionamiento con dos enlaces de Internet, a continuación se da una descripción de cada uno de los enlaces:

Proveedor	Megadatos
Teléfono	2687600 – 2667610
Contacto	Carlos Cevallos
Ancho de Banda	2-2Mbps Corporativo
Contrato	No. 970576
Direcciones IP	200.107.42.52
Descripción Enlace	Dedicado exclusivamente a correo interno e Internet

Tabla 3.10. Características del enlace con Megadatos

Proveedor	Telconet
Teléfono	2680555
Contacto	Ejecutivo Técnico Última Milla: Byron Ponce ext 2520. Ejecutivo Técnico Internet: Pedro Sosa. Ejecutivo SAC (Atención al Cliente Corporativo): Roberto Guerrero ext. 2225.
Ancho de Banda	1024/1024 kbps Metro Ethernet
Contrato	No. 855799
Direcciones IP	201.217.111.170
Descripción Enlace	Dedicado exclusivamente al uso del sistema para Departamento Financiero

Tabla 3.11. Características del enlace con Telconet

3.1.3. SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADA ACTUALMENTE EN LA INSTITUCIÓN

Para proporcionar una visión de la situación actual de la seguridad, se realizó un análisis para determinar el grado de seguridad y saber cómo la institución ha venido salvaguardando las ventajas competitivas.

Seguridad de las Comunicaciones

Correo Electrónico

Antecedentes

- ✓ Dilit-Inec cuenta con un sistema único de correo tanto para mail interno como externo, este se encuentra alojado en el servidor interno que se utiliza para la navegación de Internet, se encuentra bajo Linux y es administrado a través de SendMail, el mismo que fue configurado en su momento por un proveedor de la compañía y q actualmente es administrado por el encargado de TIC.
- ✓ A nivel institucional, se tiene adquirido en NIC un dominio (inec.gob.ec), el mismo que es el dominio de todas las cuentas de correo que se crean.
- ✓ El correo es Microsoft Outlook u Owa,debe estar instalado en cada una de las maquinas clientes que tengan autorizado su uso.
- ✓ 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.
- ✓ Si un empleado necesita una dirección de mail, porque su puesto de trabajo lo amerita, el Gerente del área al que pertenece le avisa vía electrónica al encargado de TIC, y éste crea la cuenta de correo respectiva.

Hallazgos

- ✓ 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

Antecedentes

- ✓ Dilit-Inec adquirió a inicios del 2007 170 licencias corporativas del antivirus McAfee, con lo cual se tienen protegidos a los diferentes servidores (licencia para servidor) y a el número de máquinas indicadas (licencias Cliente), incluidas las computadoras (laptops).
- ✓ No han existido muchos inconvenientes con virus, a excepción de algunos dispositivos extraíbles.
- ✓ Desde Internet se actualizan las listas de virus, el mismo que se actualiza en el Servidor para que sean replicadas a las pcs clientes.
- ✓ Como contingencia tienen en su escritorio un icono apuntando a la última actualización bajada de Internet. No se hacen chequeos ocasionales para ver si se han actualizado los antivirus.

Hallazgos

- ✓ 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, sólo en esos casos.

Ataques de red

Antecedentes

- ✓ 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 de este tipo.

Hallazgos

- ✓ 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

Antecedentes

- ✓ El archivo que contiene las passwords se encuentra en otro directorio, al cual solo el root tiene permisos para accederlo, éste es un archivo shadow, donde están encriptados. 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 encriptado con el dato almacenado que también está cifrado, si ambos son diferentes el logeo será fallido.
- ✓ Para modificar las passwords, Linux accede a los datos simulando ser root, por lo que es posible la transacción.

Hallazgos

- ✓ El archivo de los passwords del sistema no se almacena en el directorio por default del Linux, en el /etc/passwd, aquí solo se almacena un archivo con los nombres y demás datos de usuarios.
- ✓ Este archivo está en texto plano y puede ser accesible ya que no está encriptado.

Seguridad de las Aplicaciones

Seguridad de Base de Datos

Antecedentes

- ✓ En la institución se utiliza Sybase 12.5 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 de Sybase.
- ✓ El nivel de acceso a la aplicación, se lo realiza a través del propio aplicativo, en el módulo de administración, donde se registran y se dan los accesos respectivos a cada uno de los usuarios del sistema informático.
- ✓ La única persona que puede tener acceso a los archivos de la base de datos es el administrador del sistema y todo aquel que opere el servidor de

aplicaciones (es decir las personas que tengan acceso físico al equipo y con clave).

- ✓ Cada una de las transacciones efectuadas en las distintas tablas de la base de datos, se almacenan en el registro de Auditoria propio de la base, con lo que se puede determinar entre otras cosas que usuario, desde que máquina y en que fecha realizó alguna transacción.

Hallazgos

- ✓ Los aplicativos que administran la base de datos disponen de recursos suficientes para su funcionamiento, ya que aproximadamente solo el 45% de los recursos del servidor están en uso, el resto está ocioso.

Control de Aplicaciones en PC's

Antecedentes

- ✓ 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 Encargado de TIC la instalación respectiva.

Hallazgos

- ✓ 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 y en aquellas maquinas que requieren acceso al sistema se les instala el aplicativo de Power Builder para que se pueda ejecutar la aplicación desarrollada.
- ✓ 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 de TIC 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, no se documentan los cambios que se realizan, quien hizo el cambio, ni la fecha de las modificaciones.

Seguridad Física

Control de acceso físico al centro de cómputo

Antecedentes

- ✓ La sala de equipos se encuentra ubicado cerca de la puerta principal de acceso a la institución, dentro del Departamento de Plataforma Tecnológica que permanece cerrado con una única llave, de la que es custodio el Jefe del Departamento, 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: en horarios laborales se ubican en el exterior e interior de la misma, y cuando se cierra la empresa cuentan con un guardia en la entrada del edificio, las áreas correspondientes a Atención al Cliente y al área Administrativa Financiera manejan un sistema de alarma, el mismo que debe ser activado cada noche previo a la salida de las áreas respectivas. 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 Tecnologías de Información y Comunicaciones.
- ✓ En horas de oficina hay un control de entrada que identifica a los empleados y registra su hora de entrada y de salida.

Hallazgo

- ✓ 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.

Control de acceso a los equipos

Antecedentes

- ✓ No ha existido de lo que se conoce robo de datos usando medios externos.
- ✓ Los servidores del centro de cómputo no se apagan en horarios no laborales, debido a que se debe acceder a ellos por otras áreas en horario 365x7x24, permanecen prendidos las 24 horas del día.

Hallazgo

- ✓ Dispositivos como lectoras de CD/DVD, memorias SD están habilitadas y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos.
- ✓ No se realizan controles periódicos sobre los dispositivos de hardware instalados en las PC´s, de manera que alguien podría sacar o poner alguno.
- ✓ Después de completar la instalación de algún equipo, el administrador del sistema no realiza chequeos rutinarios o periódicos, solo revisa los equipos ante fallas en los mismos de forma reactiva, o por un problema reportado por el usuario.

Estructura del Edificio

Antecedentes

- ✓ Cuando se construyó el edificio de la institución, no se tuvo en cuenta el diseño del centro de cómputo y sus condiciones de seguridad.

- ✓ Las paredes externas del centro de cómputos son del mismo tamaño de las paredes de todo el piso, existe una ventana pequeña que da hacia fuera del edificio, tiene una puerta pequeña de madera con un área de 10x40 Institución de vidrio para poder ver hacia el interior.

Hallazgo

- ✓ El centro de cómputo está actualmente ubicado en la entrada del edificio.

Dispositivos de Soporte

Antecedentes

En la institución disponen de los siguientes dispositivos para soporte del equipamiento informático:

- ✓ Aire acondicionado para el centro de cómputo: la temperatura se mantiene entre 19°C y 20°C. solo para esta área, con el fin de mantener esta temperatura todos los días.
- ✓ UPS: (Uninterruptible Power Supply) en el centro de cómputo hay un UPS en serie que pueden mantener los servidores y funcionando por aproximadamente 4 horas.
- ✓ Cada computadora tiene su propio UPS que las protege durante 15 minutos aproximadamente para poder resguardar los datos y apagar el computador durante una falla de energía.
- ✓ Descarga a tierra: Existe una conexión a tierra que funcionan como descarga para el edificio.

Hallazgo

- ✓ Sólo funciona un módulo de batería del ups.

Cableado Estructurado

Antecedentes

- ✓ La instalación del cableado fue tercerizada, 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.
- ✓ 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.

Hallazgo

- ✓ Los 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.

Administración del centro de procesamiento de datos

Responsabilidad del Equipo de Sistemas

Antecedentes

- ✓ Existe un responsable general del área de Tecnologías de Información y Comunicaciones, que es el Encargado de TIC. Él es el que planifica y delega las tareas a un único empleado del área de sistemas, 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.

Hallazgo

- ✓ No hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad.

Mantenimiento

Antecedentes

- ✓ Solicitud de mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de tecnologías, se comunican telefónicamente con el encargado explicando su situación.
- ✓ Mantenimiento preventivo: Se tenía contratado un servicio de mantenimiento de hardware con una empresa externa, pero actualmente ese trabajo es realizado por el personal de TIC.

- ✓ 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 atención al público tienen mayor prioridad que el resto. En la escala siguen las de financiero, dirección, investigaciones económicas y sociodemográficas 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 con su respectivo rotulo de inventario, al igual que las licencias.

Hallazgo

- ✓ Cada requerimiento no se registra en un documento.

Instaladores

Antecedentes

- ✓ Los instaladores de las aplicaciones utilizadas en la empresa se encuentran en sus CD´s originales almacenados en un armario del centro de cómputo.

Licencias
Antecedentes

- ✓ Están actualmente licenciados todos los equipos con Windows XP sp3 y 33 equipos con Microsoft Office 2007. Se adquirieron las licencias de la Base de Datos Sybase, de las diferentes versiones del Microsoft 2003 y 2008 server, y de las herramientas de desarrollo.

Backup

Antecedentes

- ✓ 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.

Hallazgo

- ✓ 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 unidades extraíbles.

Documentación

Antecedentes

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.

Hallazgo

- ✓ 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 SGSI

Para el establecimiento de los requerimientos del SGSI es necesario determinar la estructura organizacional de la organización, 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 SGSI dependiendo de la realidad de la Institución.

3.2.1. ESTRUCTURA ORGANIZACIONAL POR PROCESOS DE LA INSTITUCIÓN

Para tener una visión clara del alcance del establecimiento de SGSI 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 27001:2005.

A continuación de detalla la estructura organizacional por procesos y las funciones respectivas de cada proceso y subproceso, así como las organizaciones externas:

Subproceso "Gestión de Recursos Humanos"

Informe de reclutamiento y selección
Informes consolidados de evaluación de desempeño Acciones de personal registradas y contratos Consolidación del plan de capacitación
Informe de ejecución del plan de capacitación
Nómina de pago
Reportes estadísticos
Informes de sumarios administrativos y vistos buenos

Subproceso "Gestión de Servicios Administrativos"

Plan de transporte
Informes de ejecución del plan de transporte
Plan de adquisiciones
Informes de ejecución del plan de adquisiciones
Planes de mantenimiento
Informe de ejecución de los planes de mantenimiento

Inventario de bienes muebles e inmuebles
Informes para el pago de servicios básicos
Informe de servicios informáticos
Informe de proveeduría
Plan de mejoramiento de calidad

Informe del Plan de mejoramiento

Subproceso de "Plataforma Tecnológica"

Plan informático

Informe de ejecución del Plan Informático

Informe de desarrollo de Software

Plan de mantenimiento de Software y Hardware Plan de mejoramiento de procesos automatizados Informes de administración de redes de conectividad

Informe de ejecución del plan de mejoramiento

Plan informático de contingencia

Informe de ejecución del plan de contingencia

PROCESO DE GESTIÓN FINANCIERA

Subproceso de "Gestión Recursos Financieros"

Proforma presupuestaria

Informe de ejecución de la pro forma Informes y reportes de estados financieros

Informes de control previo y concurrente Informes de saldos financieros

Reformas presupuestarias Liquidación presupuestaria Consolidación financiera

Registro de transacciones económicas con afectación presupuestaria

Cédulas presupuestarias codificadas

Plan de mejoramiento de la calidad

Informe de ejecución del plan de mejoramiento

Subproceso "Administración de Caja"

Informes de pagos a terceros Informes de cobros a terceros Informes de pagos de nómina

Informes de custodia de garantías y valores

Informes de control previo

Programación mensual conjunta de administración de caja

Plan de mejoramiento de la calidad

Informe de ejecución del plan de mejoramiento

Proceso "Planificación"

Plan estratégico y operativo

Informes de ejecución del plan estratégico y operativo Informes de gestión de procesos gobernantes Informes de gestión de procesos habitantes de apoyo Informes de gestión de habilidades de asesoría Informes de gestión de procesos de valor agregado

Reportes del Sistema Común de Información para los usuarios

Informe de convenios y compromisos de gestión

Plan de mejoramiento de la Calidad

Plan e informe de mejoramiento continúo de la calidad de gestión

Proceso "Asesoría Jurídica"

Demandas y Juicios

Informe de criterios jurídicos Contratos y convenios Informes Legales Periódicos

Plan e Informe de mejoramiento de la calidad

Proceso "Comunicación Social"

Atención al cliente

Aceptación de clientes

Recepción de quejas, reclamos, sugerencias, consultas

Resolución de quejas para lo cual se coordina con el área indicada

Operación de las políticas de promoción de la salud Operación de la información, comunicación y educación Operación de la participación comunitaria

Proceso "Investigaciones Económicas"

Ingreso de nuevos clientes en el sistema

Definición de planes y coberturas acorde a las necesidades.

Ingreso y revisión de datos recopilados

Generación de metodologías de Investigación

Generación parcial de tabulados.

Proceso "Investigaciones Sociodemográficas"

Ingreso de nuevos clientes en el sistema

Definición de planes y coberturas acorde a las necesidades

Ingreso y revisión de datos recopilados

Generación de metodologías de Investigación

Generación parcial de tabulados.

Proceso "Geografía Estadística"

Plan Operativo de Geografía Estadística
Informe Trimestral del Plan Operativo
Cartografía Censal
Mapas Censales
Planos Censales
Mapas de Cobertura vegetal y uso actual del suelo
División Política Administrativa

ORGANIZACIONES EXTERNAS

Clientes

Los clientes pueden ser considerados de dos maneras:

1. Individual.
2. Corporativo.

Proveedores de Internet

Empresas que prestan el servicio de Internet, para nuestro caso, son: Telconet y Megadatos.

3.2.2. DEFINICIÓN DEL ALCANCE DEL SGSI

Una vez que ya se tienen identificados los procesos que forman parte de la empresa, se determinará el alcance del SGSI 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 elipses, en el cual se deben definir e 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 como procesos principales a los siguientes:

- Geografía Estadística.
- Producción de Estadísticas Económicas.
- Producción de Estadísticas Sociodemográficas.
- Comunicación Social y Relaciones Públicas.

El segundo paso de este método es identificar la elipse 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 cuáles son los recursos indispensables para que la empresa pueda cumplir con sus objetivos de negocio.

Por motivos de recursos disponible se centrara en uno de sus procesos críticos como es el de **Producción de Estadísticas Económicas,** del cual una vez realizado el análisis podría ser replicado a los otros procesos bases.

El proceso de **Producción de Estadísticas Económicas,** se basa en el diseño, ejecución y socializaciòn de proyectos de investigaciones económicas siendo el proyecto más representativo el Censo Nacional Econòmico.

Esta información se obtiene del siguiente diagrama:

ESTRUCTURA ORGANIZACIONAL POR PROCESOS

HABITANTES DE APOYO

DESARROLLO ORGANIZACIONAL
GESTIÓN DE RECURSOS HUMANOS
GESTIÓN DE SERVICIOS ADMINISTRATIVOS
ADMINISTRACIÓN DE LA PLATAFORMA TECNOLÓGICA
GESTIÓN FINANCIERA
GESTIÓN DE RECURSOS FINANCIEROS
ADMINISTRACIÓN DE CAJA

GOBERNANTE

GESTIÓN ESTRATÉGICA
DIRECTOR REGIONAL

HABITANTE DE ASESORÍA

PLANIFICACION INSTITUCIONAL
ASESORÍA JURÍDICA

DE VALOR AGREGADO

Figura 3.3 Estructura Organizacional por Procesos.

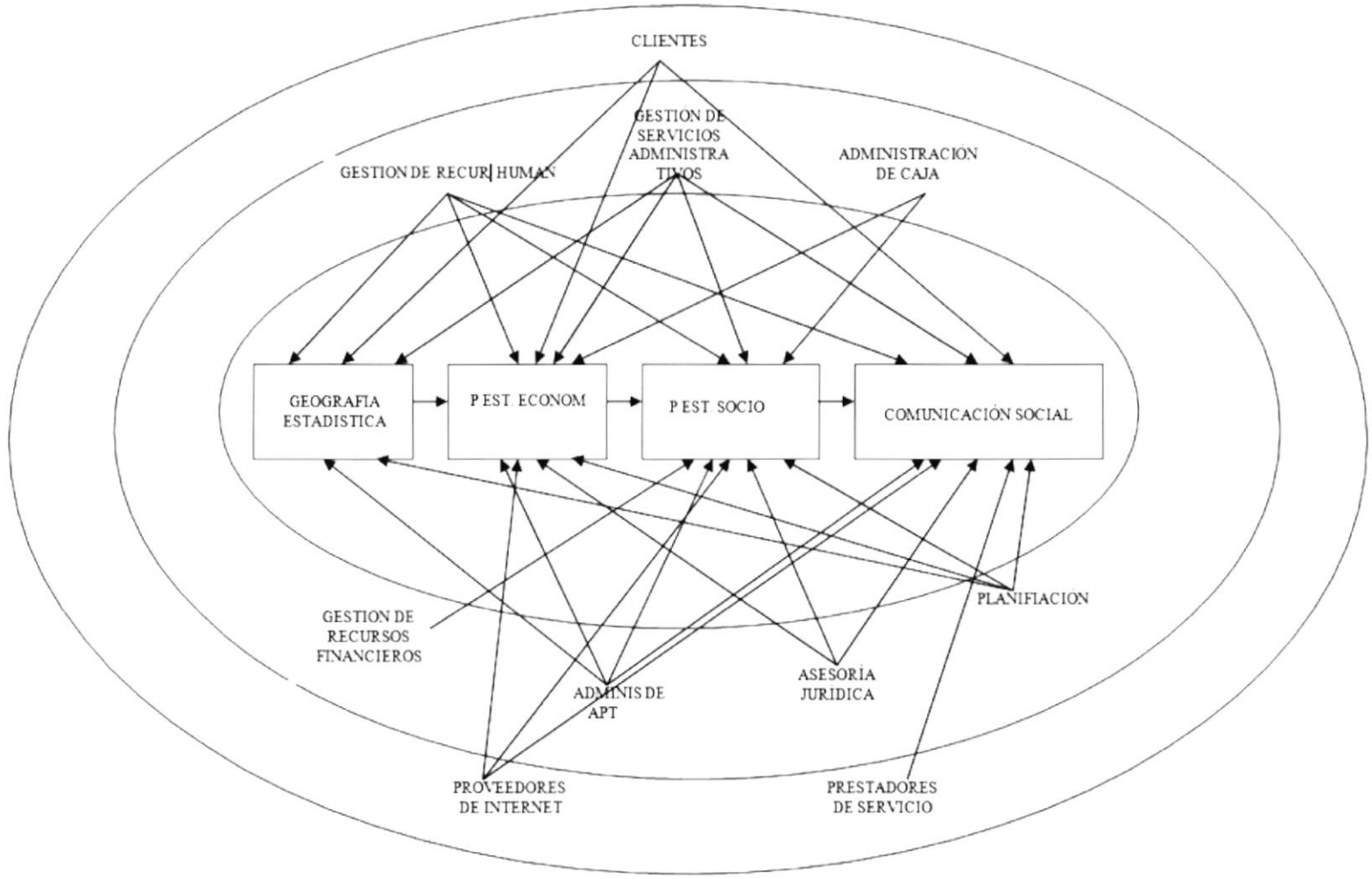

Figura 3.4 Método de Eclipses para los procesos

3.3. IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE VULNERABILIDADES

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 Institución. A continuación se detallan algunas metodologías.

3.3.1. 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 27001.

3.3.2. IDENTIFICACIÓN DE ACTIVOS

Para la identificación de los activos se utilizaron los datos proporcionados por los administradores, 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

Documentación 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 Facturas Memos Oficios Reglamento del SRI Reglamento de contraloría Papel Tarjetas de Afiliación

Activos Auxiliares	
Descripción	Otros dispositivos que ayudan al funcionamiento de la organización
Activos	Suministros de oficina tales como calculadoras, teléfono, entre otros.

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.
Activos	Windows Server 2003 R2 Enterprise Edition Windows Server 2008 Enterprise Edition Linux CentOs 5.4 Windows XP Profesional SP 3

Paquete de programas o software estándar	
Descripción	El software estándar o paquete de programas es un producto comercializado como tal 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 McAfee 8.7. Software de atención al cliente, Microsoft Visio SPSS Nero Suite Microsoft Visual Estudio Microsoft Project Adobe Illustrator

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 Power Buider para acceso a la información de usuarios

Activos Físicos

Hardware Portátil	
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 para la recepción, la transmisión o la emisión de datos.
Activos	Impresoras, Copiadoras, Teléfonos, Fax

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 Servidor de Dominio Servidor Proxy Server

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	CD/DVD-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	tecnología Ethernet, cables, Switch, MODEM, Acces Point

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 brindados por un prestador.
Activos	Línea telefónica, central telefónica, redes telefónicas internas.

Energía	
Descripción	Servicios y medios (fuentes de energía y cableado) necesarios para la 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.
Activos	Portal de información (Página Web de la empresa)

Personas

Empleados	
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 Regional

3.3.3. IDENTIFICACIÓN DE REQUERIMIENTOS

Se identificará los requerimientos de los activos en base a los objetivos del negocio, aspectos legales para de esta manera identificar las obligaciones del SGSI. 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)

3.3.4. VALORACIÓN DE LOS ACTIVOS

El objetivo es identificar la valoración de todos los activos dentro del alcance del SGSI, 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 que el proceso pueda cumplir con las operaciones del negocio.

A continuación se presenta la tabla de valoración de activos de l proceso de **Producción de Estadísticas Económicas:**

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
	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
PCs 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.

Tabla 3.12. Valoración de Activos

ACTIVOS	ELEMENTOS DE INFORMACIÓN	VALOR	RAZÓN
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.
	Disponibilidad	3	Es indispensable que los servidores estén accesibles al menos el 100% en las horas laborables, para no afectar a los clientes Internos y externos.
Equipos de Oficina	Confidencialidad	2	Información de negocio que se imprima o se fotocopie necesita confidencialidad.
	Integridad	2	Se necesita los equipos de Oficina (impreosra)), pero si eventualmente falla se puede seguir trabajando.
	Disponibilidad	2	Si bien son necesarios los equipos, se puede trabajar aunque no estén dsponibles
Soporte Electrónico	Confidencialidad	2	Cuando se tenga información de negocio almacenada en estos equipos es necesaria su protección.
	Integridad	1	Es un medio temporal para almacenar Información
	Disponibilidad	1	No es requerido, cuando la información es Redundante
Documentación y Registros	Confidencialidad	3	Debido a que la documentación maneja 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

Tabla 3.12. Valoración de Activos

ACTIVOS	ELEMENTOS DE INFORMACIÓN	VALOR	RAZÓN
Establecimiento	Confidencialidad	1	Es un edificio pùblico
	Integridad	3	Se debe proteger la integridad fisica 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
	Confidencialidad	2	Se debe proteger que las lineas no sean interceptadas para que no se
Servicio de Comunicacion	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 clientes, reclamos, etc.
Servicio de energia 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
Servicio de correo electrónico	Confidencialidad	4	Debe tener confidencialidad porque probablemente esté viajando información de la institución que debe manejar solo ciertos departamentos y especialmente si la información viaja por una red pública
	Integridad	2	Los datos no deben ser modificados, pero en el caso que se pierda la integridad al utilizar el servicio de correo electrónico, los datos originales podrán ser
	Disponibilidad	2	El correo electrónico debe estar disponible en horas de trabajo, pero en el caso de que no esté disponible, existen otros médios como servicio de fax, teléfono, etc.
Aplicación P. builder 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 modificacionesen 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
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.

Tabla 3.12. Valoración de Activos

ACTIVOS	ELEMENTOS DE INFORMACIÓN	VALOR	RAZÓN
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 el registro 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.
Sistemas operativos	Confidencialidad	4	Los datos de los clientes, que es información personal es procesada en el 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

Tabla 3.12. Valoración de Activos

3.3.5. IDENTIFICACIÓN DE AMENAZAS Y VULNERABILIDADES

El objetivo es identificar las amenazas a las que se exponen los activos dentro del alcance del SGSI y las vulnerabilidades que pueden ser explotadas por las amenazas. A continuación detallamos las amenazas principales clasificadas por activos de información.

Activos	Amenazas
Fisico	Fuego / Daño por agua / Desastres naturales / Corte suministro elèctrico / Degradaciòn del Hardware / Virus de computadora.
Comunicaciòn	Fuego / Daño por agua / Desastres naturales / Corte suministro elèctrico / Degradaciòn del Hardware / Virus de computadora/ Errores de configuraciòn.
Energìa	Fuego / Daño por agua / Desastres naturales / Corte suministro elèctrico / Degradaciòn del Hardware / Condiciones inadecuadas de temperatura.
Documentacion y Registros	Fuego / Daño por agua / Desastres naturales / Corte suministro elèctrico / Condiciones inadecuadas de temperatura
Software	Errores de usuarios/ Errores de configuraciòn/ Escape de informaciòn / Alteraciòn de informaciòn / Divulgaciòn de informaciòn / Errores de actualizaciòn, Virus de computadora / Corrupciòn de archivos.

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, en el proceso de **Producción de Estadísticas Económicas**.

ACTIVO	AMENAZAS	VULNERABILIDADES
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 noadecuado 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 software 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 hardware	Falta de mantenimiento adecuado
	Inautorizada copia de software o información ropietaria	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 fectados

Tabla 3.13 Amenazas y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
PCs de oficina	Acceso no autorizado a las PCs de oficina	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 cndicionado
	Instalación no autorizada o cambios de Software	Falta de control de acceso
	Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de software 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 hardware	Falta de mantenimiento adecuado
	Inautorizada copia de software información propietaria	Falta de políticas
	Ataque destructivo	Falta de protección física
	Robo	Falta de protección física adecuada
Servidores	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
	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 hardware	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 hardware	Falta de Mantenimiento
	Ataque destructivo	Falta de protección física
	Uso no previsto	Falta de políticas Falta de control de acceso

Tabla 3.13 Amenazas y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Soporte electrónico	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados
	Condiciones inadecuadas de temperatura y/o humedad	Susceptibidad al calor y humedad
	Ataque destructive	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 física adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados por
	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	Falta de conocimiento de los empleados
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema
	Contratos no completos	Falta de control para el establecimiento de contratos
	Ataque destructive	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
	Divulgación de información	Falta de acuerdos de confidencialidad
Establecimiento	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
	Degradación del servicio y Equipos	Falta de mantenimiento adecuado
	Errores de configuración	Falta de conocimiento del
	Manipulación de la Configuración	Falta de control de acceso
	Uso no previsto	Falta de políticas
	Ataque destructivo	Falta de protección física

Tabla 3.13 Amenazas y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
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
	Ataque destructive	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
Aplicación Power Builder para acceso a la información de usuarios	Errores de los usuarios	Falta de conocimiento del uso de la 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	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	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

Tabla 3.13 Amenazas y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Uso no previsto	Falta de políticas de seguridad
Sistemas operativos	Negación de Servicio	Capacidad insuficiente de los Recursos
	Errores de Configuración del servicio	Falta de capacitación del administrador Incompleto o incorrecto documentación del sistema
	Virus de Computación. Fuerza Bruta y ataques de Diccionario	Falta de Protección actualizada
	Falta de capacidad de Restauración	Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas Instalación de software 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 3.13 Amenazas y Vulnerabilidades

3.3.6. 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 la Institución.

Valoración:

A= probabilidad de ocurrencia de la amenaza, en base a los registros de los últimos 2 años.

V= Nivel de vulnerabilidad.

A continuación se presenta la tabla de exposición al riesgo del proceso de **Producción de EstadísticasEconómicas:**

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
Hardware Portátil	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la institución
	V1: Falta de protección contra fuego	Media	Actualmente no se tiene 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	[redacted]	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	[redacted]	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	[redacted]	No se encuentran definidas políticas de seguridad
	A9: Incumplimiento con	[redacted]	El porcentaje de fallas en la

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	controles de seguridad		seguridad es alto
	V9: Falta de conocimiento de seguridad por parte del personal		No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A10: Degradación del hardware	Medio	Los equipos ya han presentado varias fallas de hardware
	V10: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento continuo de los equipos
	A11: Copia no autorizada de software o información propietaria	Medio	Se han encontrado Cd piratas de software con licencia.
	V11: Falta de políticas		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		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
	V13: Falta de protección física		No se tiene una adecuada protección física dentro de la Institución.
PCs de oficina	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la institución
	V1: Falta de protección contra fuego	Media	Actualmente no se tiene 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: Acceso no autorizado a las PCs de oficina	Media	Existen diferentes motivos para acceso al equipo sin autorización, ya sea por curiosidad, malicia
	V4: Falta de Protección por desatención de equipos		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	Media	Los portátiles no se conectan a un UPS general, únicamente cuentan con la batería

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	Acondicionado		
	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 hay la posibilidad que con herramientas no autorizadas monitoreen la red y las contraseñas que viajan por la misma
	A7: Incumplimiento con la legislación	Baja	No se presentan registros
	V7: Falta de conocimiento de protección de derechos de software por parte de los empleados		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		No se encuentran definidas políticas de seguridad
	A9: Incumplimiento con controles de seguridad		El porcentaje de fallas en la seguridad es alto
	V9: Falta de conocimiento de seguridad por parte del personal		No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A10: Degradación del Hardware	Medio	Los equipos ya han presentado varias fallas de Hardware
	V10: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento continuo de los equipos
	A11: Inautorizada copia de software o información propietaria	Medio	Se han encontrado Cd piratas de software con licencia.
	V11: Falta de políticas		No se encuentran definidas políticas de seguridad para conocimiento de los usuarios
	A12: Ataque destructivo	Baja	No se ha presentado este problema
	V12:Falta de protección		La seguridad del edificio es muy escasa
	A13: Robo	Media	Se tiene registrado un caso de robo de equipos
	V13: Falta de protección física		No se tiene una adecuada protección física dentro de la institución

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la institución
	V1: Falta de protección contra fuego	Media	Actualmente no se tiene ninguna protección contra fuego, como extintores.
Servidores	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 baño, del cual no 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	[redacted]	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	Medio	Existe siempre la posibilidad que alguien no autorizado logré ingresar a través de la red
	V7: Código malicioso desconocido	Medio	Esto puede pasar, pues siempre sale nuevo código dañino que no es reconocido por los antivirus.
	A8: Degradación o Falla del Hardware	Medio	Son equipos que no han sido actualizados de hardware hace mucho tiempo
	V8: Falta de mantenimiento adecuado	Medio	No se realiza un mantenimiento preventivo y correctivo adecuado
	A9: Manipulación de la configuración	[redacted]	No se tiene registros de este tipo de problemas
	V9: Falta de control de acceso	[redacted]	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 deseguridad	Media	Se han presentado registros de intentos de ingreso a los servidores sin autorización

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	V10: Falta de conocimiento de seguridad por parte del personal		Los empleados de la empresa tienen muy poco conocimiento de las políticas de seguridad
	A11: Incapacidad de Restauración		No se encuentra definido un plan de contingencia
	V11: Falta de planes de continuidad del negocio		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	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		No se realiza continuo monitoreo de los servidores
	A14: Ataque destructivo	Baja	No se ha presentado este problema
	V14: Falta de protección Física		La seguridad del edificio es muy escasa
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la institución
	V1: Falta de protección contra fuego	Media	Actualmente no se tiene 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 hardware	Media	Se han presentado problemas en algunas impresoras y teléfonos
	V4: Falta de Mantenimiento		No se realiza un mantenimiento de los equipos, los mismos que utilizados por todos los usuarios.
	A5: Ataque destructivo	Baja	En la institución no seha presentado este problema
	V5: Falta de protección Física		La seguridad del edificio es muy escasa
	A6: Uso no previsto		Se han encontrado a varios usuarios con uso no adecuado del teléfono y las impresoras
	V6.1: Falta de Políticas		No se encuentran definidos procedimientos para un uso adecuado de los equipos

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	V6.2: Falta de Control de Acceso		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 la institución.
	V1: Falta de protección contra fuego	Media	Actualmente no se tiene 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		Los CD, disquetes son susceptibles a la humedad
	A5:Ataque destructive	Baja	No se ha presentado este problema.
	V5: Falta de protección Física		La seguridad de estos elementos es muy escasa.
	A6:Escape de Información		Se han presentado pérdidas en la oficina.
	V6: Manipulación inadecuada de información		No se tiene un procedimiento aprobado de manipulación de la información.
	A7: Robo		Se han presentado pérdidas en la oficina
	V7:Falta de atención del Personal		El personal deja descuidadas sus cosas.
Documentación y Registros.	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se
	V1: Falta de protección contra fuego	Media	Actualmente no se Tiene 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	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

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	A4: Pérdida de información	Media	Se han presentado problemas debido a fallas de los empleados
	V4.1: Errores de los empleados		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 onfidencialidad
	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 compañia 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	No se hapresentado este problema.
	V9: Falta de protección Fisica		La seguridad de estos elementos es muy escasa.
	A10: Incapacidad de restauración		No se encuentra definido un plan de contingencia.
	V10: Falta de planes de continuidad del negocio		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.

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
Empleados	A1: Errores de los empleados y acciones equivocadas	[redacted]	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
Establecimiento	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la institución
	V1: Falta de protección contra fuego	Media	Actualmente no se tiene 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	[redacted]	La institución cuenta con 2 guardias que controla todo el Edificio.
	V3.2: Falta de políticas	[redacted]	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 Comunicación	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector donde se encuentra la institución.
	V1: Falta de protección contra fuego	Media	Actualmente no se tienen ninguna protección contra fuego, como extintores.
	A2: Daños por agua	Baja	No se ha registrado este tipo de incidente

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	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 serviciode 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 institución 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 no se tiene ninguna protección contra fuego, como extintores.
	A2: Daños por agua	Media	Al año se presentan algunos registros de daños causados por

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	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 usuarios 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 P. builder 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	Baja	El administrador es una persona preparada con experiencia.

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	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 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	Baja	No se ha registrado este Incidente.
	V4: Falta de procedimientos aprobados		No se cuenta con procedimiento de actualización de este softwarre.
	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 Acceso		En vista de que no se lleva actualizaciones del aplicativo, es más fácil explotar esta ulnerabilidad
	A7: Abuso de privilegios de acceso	Baja	No se ha registrado ningún Incidente.
	V7: Falta de políticas de seguridad		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		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		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 usuarios deben recibir entrenamiento en cómo usar los servicios.

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	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 institución	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 no se tiene 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 fácilmente afectados por desastres naturales	Media	No existen protecciones requeridas para enfrentar daños 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 public.
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 ProtecciónActualizada	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 software estándar no senecesita ningún tipo de control de acceso de acceso.

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	A4: Falta de capacidad de restauración	Baja	No se ha registrado este tipo de incidente.
	V4: Falta de copias de backup continuas		No se tiene copias de respalda para restauración.
	A5: Uso no previsto		El personal en algunas ocasiones haceuso de estas herramientas con fines personales.
	V5: Falta de políticas de Seguridad		Actualmente no se tienen una política aprobada, está en proceso de desarrollo todavía.
Sistemas operativos	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 institución.
	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 actualizada		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		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		No se cuenta conun procedimiento para las actualizaciones.
	V 5.2: Instalación de SW no autorizado		Esta vulnerabilidad puede ser fácilmente debido a que no se sigue ninguna política de seguridad.
	A 6: Controles de Seguridad no cumplidos		No se han definido controles de seguridad, razón por la cual ciertos controles no han sido cumplidos

Tabla 3.14. Exposición del Riesgo

ACTIVOS	AMENAZAS	VALOR	DESCRIPCIÓN
	V 6: Falta de Políticas de Seguridad		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		El control de acceso puede ser fácilmente vulnerado debido a la débil seguridad física de los equipos de cómputo.
Medios y Soporte	A1: Acceso no autorizado a la información	Media	Se han encontrado máquinas personales conectadas a la Red.
	V1: Falta de protección Física	Media	No se tiene una adecuada protección física dentro de la institución.
	A 2: Robo	Baja	No se ha registrado ningún Incidente
	V 2: Falta de protección Física		No se tiene una adecuada protección física dentro de la institución.
	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)		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		No cuenta con ningún tipo de monitoreo de la red.

Tabla 3.14. Exposición del Riesgo

3.4. PLAN DE TRATAMIENTO DE RIESGOS PARA IDENTIFICAR ACCIONES, RESPONSABILIDADES Y PRIORIDADES EN LA GESTIÓN DE LOS RIESGOS

A continuación describimos las principales responsabilidades que se suguiere de acuerdo a la norma, a los miembros implicados en la seguridad de la información para la gestión de los riesgos basados en los dominios:

- El **Área de Plataforma Tecnológica** es la responsable 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 Regional y Jefatura Administrativa Financiera y

con el área de Auditoria 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 Sistemas** es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

- El **Proveedor del Sistema Informático** 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 Proveedor del Sistemas también es responsable de informar al Encargado de Sistemas sobre toda actividad sospechosa o evento insólito.

- El **Comité de Seguridad de la Información** del Organismo, procederá a revisar y proponer a la máxima autoridad del Organismo 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 área1, 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 del Organismo y coordinar el proceso de administración de la continuidad de las actividades del Organismo.

- Los usuarios son responsables de cumplir con todas las políticas de la

Institución relativa 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 la Institución a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Institución 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.
- 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 la Institución y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

El **Comité de Seguridad de la Información** tendrá a cargo el mantenimiento y la presentación para la aprobación de la Política, ante la máxima autoridad de la Institución, 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 institución 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.

3.5. VALORACIÓN DEL RIESGO DEL SGSI

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 4.1. Ejemplo de cálculo para la valoración del riesgo

En base a la información obtenida en el capítulo anterior 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. La organización seleccionó que el 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 que nos ayudara identificar 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 3.15. Niveles de Riesgos

Aquellos riesgos con niveles menores a 4 como se muestra en la tabla anterior, son aquellos que se van a aceptar.

ACTIVO	VALOR ACTIVO	AMENAZA	VALOR AMENAZA	VULNERABILIDAD	VALOR VULNERABILIDAD	TOTAL RIESGO
Hardware Pórtatil	3	A1	1	V1	1	3
		A2	1	V2	1	3
		A3	1	V3	2	6
		A4	2	V4	3	18
		A5	2	V5	2	12
		A6	1	V6	2	6
		A7	1	V7	3	9
		A8	2	V8	3	18
		A9	3	V9	3	27
		A10	2	V10	2	12
		A11	2	V11	3	18
		A12	1	V12	3	9
		A13	2	V13	3	18
Pcs de Oficina	3	A1	1	V1	1	1
		A2	1	V2	1	3
		A3	1	V2	1	3
		A4	2	V4	3	18
		A5	2	V5	2	12
		A6	1	V6	2	6
		A7	1	V7	3	9
		A8	2	V8	3	18
		A9	3	V9	3	27
		A10	2	V10	2	12
		A11	2	V11	3	18
		A12	1	V12	3	9
		A14	2	V13	3	18
Servidor	3	A1	1	V1	1	3
		A2	1	V2	1	3
		A3	1	V3	1	3
		A4	1	V4	2	6
		A5	2	V5	3	18
		A6	2	V6	2	12
		A7	2	V7	2	12
		A8	2	V8	2	12
		A9	1	V9	3	9
		A10	2	V10	3	18
		A11	3	V11	3	27
		A12	2	V12	2	12
		A13	1	V13	3	9
		A14	1	V14	3	9

Tabla 3.16. Niveles Totales de Riesgos

ACTIVO	VALOR ACTIVO	AMENAZA	VALOR AMENAZA	VULNERABILIDAD	VALOR VULNERABILIDAD	T OTAL RIESGO
Equipos de Oficina	2	A1	1	V1	1	3
		A2	1	V2	1	2
		A3	1	V3	1	2
		A4	2	V4	3	12
		A5	1	V5	3	6
		A6	2	V6.1	3	12
		A6	2	V6.2	3	12
Soporte Electrónico	2	A1	1	V1	2	4
		A2	1	V2	1	2
		A3	1	V3	1	2
		A4	1	V4	3	6
		A5	1	V5	3	6
		A6	3	V6	3	18
		A7	3	V7	3	18
Documentacion y Registro	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	1	V3	1	3
		A4	2	V4.1	3	18
		A4	2	V4.2	2	12
		A5	2	V5	2	12
		A6	1	V6	2	6
		A7	1	V7	2	6
		A8	2	V8	1	6
		A9	1	V9	3	9
		A10	3	V10	3	27
		A11	2	V11	1	6
Empleados	2	A1	3	V1	2	12
		A2	2	V2	2	8
		A3	2	V3	1	4
Establecimiento	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	2	V3.1	3	18
		A3	2	V3.2	3	18
		A4	1	V4	1	3

Tabla 3.16. Niveles Totales de Riesgos

ACTIVO	VALOR ACTIVO	AMENAZA	VALOR AMENAZA	VULNERABILIDAD	VALOR VULNERABILIDAD	T OTAL RIESGO
Servicio de Comunicaciones	3	A1	1	V1	1	3
		A2	1	V2	1	3
		A3	1	V3	2	6
		A4	2	V4	3	18
		A5	1	V5	2	6
		A6	1	V6	2	6
		A7	2	V7	2	12
		A8	1	V8	3	9
		A9	3	V9	3	27
Servicio de Energia	3	A1	1	V1	1	3
		A2	2	V2	1	3
		A3	1	V3	1	3
		A4	1	V4	1	3
Servicio email	4	A1	1	V1	2	8
		A2	1	V2	3	12
		A3	1	V3	3	12
		A4	3	V4	3	36
		A5	2	V5	3	24
Aplicación P Builder	4	A1	2	V1	1	8
		A2	1	V2	1	4
		A3	1	V3	2	8
		A4	1	V4	3	12
		A5	1	V5	2	8
		A6	1	V6	3	12
		A7	1	V7	3	12
		A8	2	V8	3	24
Portal de Informacion	3	A1	1	V1	3	9
		A2	1	V2	2	6
		A3	2	V3	2	12
		A4	1	V4	1	3
Suministros de Oficina	2	A1	1	V1	3	6
		A2	1	V2	1	2
		A3	1	V3	1	2

Tabla 3.16. Niveles Totales de Riesgos

ACTIVO	VALOR ACTIVO	AMENAZA	VALOR AMENAZA	VULNERABILIDAD	VALOR VULNERABILIDAD	TOTAL RIESGO
		A4	3	V4.1	1	6
		A4	3	V4.2	1	6
Imagen Empresa	2	A1	1	V1	3	6
Paquete Software	3	A1	1	V1	2	6
		A2	3	V2	3	27
		A3	1	V3	2	6
		A4	1	V4	3	9
		A5	3	V5	3	27
Sistemas Operativos	4	A1	1	V1	2	8
		A2	1	V2.1	2	8
		A2	1	V2.2	2	8
		A3	2	V3	3	24
		A4	2	V4	3	24
		A5	1	V5.1	3	12
		A5	1	V5.2	3	12
		A6	3	V6	3	36
		A7	1	V7	3	12
Medios y Soporte	3	A1	2	V1	2	12
		A2	1	V2	3	9
		A3	1	V3	1	3
		A4	1	V4	3	9
		A5	1	V5	3	9

Tabla 3.16. Niveles Totales 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:

3.6. 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	Aceptación
	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 confiable del UPS o 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 destructive	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
PCs de oficina	Fuego	Falta de protección contra fuego	Aceptación
	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 al Equipo	Falta de Protección por desatención de equipos	Reducción
	Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Reducción
	Instalación no autorizada o cambios de Software	Falta de control de acceso	Reducción

Tabla 3.17 Tratamiento de Riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
	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 hardware	Falta de mantenimiento	Reducción
	Inautorizada copia de software	Falta de políticas	Reducción
	Ataque destructive	Falta de protección física	Reducción
	Robo	Falta de protección física	Reducción
Servidores	Fuego	Falta de protección contra Fuego	Aceptación
	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 hardware	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 destructive	Falta de protección física	Reducción
Equipos de Oficina	Fuego	Falta de protección contra Fuego	Aceptación
	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 hardware	Falta de Mantenimiento	Reducción
	Ataque destructive	Falta de protección física	Reducción
	Uso no previsto	Falta de Políticas Falta de Control de Acceso	Reducción
Soporte	Fuego	Falta de protección contra	Aceptación

Tabla 3.17 Tratamiento de Riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
Electrónico		Fuego	
	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 destructive	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	Aceptación
	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 incompletes	Falta de control para el establecimiento de contratos	Reducción
	Ataque destructive	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 empleados	Reducción
	Divulgación de información confidencial	Falta de acuerdos de Confidencialidad	Reducción
Establecimientos	Fuego	Falta de protección contra Fuego	Aceptación
	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	Aceptación
	Daños por agua	Falta de protección física Adecuada	Aceptación

Tabla 3.17 Tratamiento de Riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
	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 destructive	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	Aceptación
	Daños por agua	Falta de protección física Adecuada	Aceptación
	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
Aplicación P. builder	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
	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 falsa	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 la institución.	Falta de procedimiento Aprobados	Reducción
Suministro De	Fuego	Falta de protección contra Fuego	Aceptación

Tabla 3.17 Tratamiento de Riesgos

ACTIVOS	AMENAZAS	VULNERABILIDADES	PTR
Oficina	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 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 Actualizada	Reducción
	Falta de capacidad de restauración	Falta de copias de backup continuas	Reducción
	Pérdida de Servicio	Actualizaciones incorrectas	Reducción
	Pérdida de Servicio	Instalación de software 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 3.17 Tratamiento de Riesgos

En base a las vulnerabilidades identificadas en DILIT-INEC se detallarán los controles que minimizan en mejor medida las mismas.

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Hardware Portátil	A4	V4	Falta de protección por desatención de equipos	9.1.5	Acceso fácil al hardware	Diseño de lineamientos para trabajar en áreas seguras	Dirección
				11.1.1		Implementación de políticas de seguridad de acceso	Dirección / dueño de información
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usuarios sobre la protección de equipos	Sistemas
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales
	A5	V5	Mal funcionamiento del ups	9.2.2	Daño de equipo	Evitar la interrupción de servicios	Sistemas - SSAA
				14.1.3		Diseñar e implantar plan de contingencia	Dirección / dueño de información
				14.1.5		Revisión del plan de continuidad del negocio	Sistemas
	A6	V6	Falta de control de acceso	6.1.4	Instalación de software no necesarios en equipos	Implantación de procesos de autorización	Jefes Departamentales
				6.2.3		Elaborar lineamientos de aplicaciones con terceros	Sistemas - SSAA
				12.2.2		Incorporación de revisiones en las aplicaciones	Sistemas
	A7	V7	Falta de control de protección de derechos de autor	8.2.2	Problemas legales	Informar a los empleados sobre leyes y normativas	RRHH
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales
	A8	V8	Falta de políticas aplicadas	5.1.1	Utilización de recusos para fines diferentes al negocio	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas
				6.1.4		Implantación de procesos de autorización	Jefes Departamentales
				8.1.3		Informar a los empleados sobre las condiciones contractuales	RRHH
				8.2.1		Informar sobre las responasbiliades de los empleados	RRHH
				8.2.2		Informar a los empleados sobre leyes y normativas	Jefes Departamentales
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas
	A9	V9	Falta de conocimiento de seguridad por parte del personal	8.2.2	Violaciones a las seguridades	Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				13.1.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Hardware Portátil				13.2.1		Implementación de procedimientos para agilitar tiempo de respuesta en incidentes	Jefes Departamentales
	A10	V10	Falta de mantenimiento	9.2.4	Fallas de hardware	Diseño y ejecución del plan de mantenimiento	Sistemas- SSAA
	A11	V11	Falta de politicas	5.1.1	Uso de equipo para copias de software ilegales	Elaboración de documento de políticas de seguridad de la información	Dirección - Sistemas
				15.1.2		Informar a los empleados sobre la normativa de propiedad intelectual	Juridico
				15.1.4		Infromar a los empleados sobre la ley de estadística	Juridico
	A12	V12	Falta de protección fisica adecuada	9.1.1	Fuga de información	Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
	A13	V13	Falta de protección física adecuada	7.1.1	Robo de equipos	Elaboración y mantenimiento de inventario de equipos	SSAA
				7.1.2		Asignación de bienes a los empleados	SSAA
				7.1.3		Difusión d guias de utilización adecuadda de los recursos	Sistemas
				9.1.1		Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas
Pcs de Oficina	A4	V4	Falta de protección por desatención de equipos	9.2.5	Acceso fácil al equipo	Elaboración de procedimientos para uso de las fpi fuera de la institución	Dirección-SSAA
				11.1.1		Implementación de políticas de seguridad de acceso	Dirección / dueño de información
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Pcs de Oficina	A5	V5	Mal funcionamiento del ups	9.2.2	Daño de equipo	Evitar la interrupción de servicios	Sistemas - SSAA
				14.1.3		Diseñar e implantar plan de contingencia	Dirección / dueño de información
				14.1.5		Revisión del plan de continuidad del negocio	Sistemas
	A6	V6	Falta de control de acceso	6.1.4	Ejecución de programas tipo livecd para monitorear la red	Implantación de procesos de autorización	Sistemas
				6.2.3		Elaborar lineamientos de aplicaciones con proveedores de terceros	Sistemas - SSAA
				12.2.2		Incorporación de pistas de auditorias en las aplicaciones	Sistemas
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
	A7	V7	Falta de control de protección de derechos de autor	8.2.2	Problemas legales	Informar a los empleados sobre leyes y normativas	RRHH
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales
	A8	V8	Falta de politicas	5.1.1	Utilización de recusos para fines diferentes al negocio	Elaboración de documento de politicas de seguridad de la información	Dirección-Sistemas
				6.1.4		Implantación de procesos de autorización	Sistemas
				8.1.1		Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				8.1.3		Informar a los empleados sobre las condiciones contractuales	RRHH
				8.2.1		Informar sobre las responasbiliades de los empleados	RRHH
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas
	A9	V9	Falta de conocimiento de seguridad por parte del personal	8.2.2	Violaciones a las seguridades	Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Pcs de Oficina				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				13.2.1		Implementación de procedimientos para agilitar tiempo de respuesta en incidentes	Jefes Departamentales
	A10	V10	Falta de mantenimiento	9.2.4	Fallas de hardware	Diseño y ejecución del plan de mantenimiento	Sistemas- SSAA
	A11	V11	Falta de políticas	5.1.1	Uso de equipo para copias de software	Elaboración de documento de políticas de seguridad de la información	Dirección
				15.1.2		Informar a los empleados sobre la normativa de propiedad intelectual	Juridico
				15.1.4		Informar a los empleados sobre la ley de estadistica	Juridico
	A12	V12	Falta de protección física adecuada	9.1.1	Fuga de información	Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
	A13	V13	Falta de protección física adecuada	7.1.1	Robo de equipos	Elaboración y mantenimiento de inventario de equipos	SSAA
				7.1.2		Asignación de bienes a los empleados	SSAA
				7.1.3		Difusión de guias de utilización adecuadda de los recursos	Sistemas
				9.1.1		Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas
Servidores	A4	V4	Falta de protección de archivos	10.8.3	Corrupción de archivos	Elección de transportación por medios seguros	Sistemas-SSAA
				12.2.2		Incorporación de revisiones en las aplicaciones	Sistemas
				12.4.3		Politcas de restricción al acceso	Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Servidores	A5	V5	Incapacidad de diferenciar entre petición real y falsa	10.6.1	Inhabilitación de recursos	Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				11.4.1		Informar sobre el uso de politicas de la red	Sistemas
				11.4.2		Proveer mecanismo para no comprometer la seguridad cuando se conecten usuarios externos a la institución	Sistemas
				11.4.3		Proveer mecanismo de autenticación de nodos en la red	Sistemas
				11.4.4		Proveer mecanimso de control sobre puertos que pueden permitir accesos no autorizados	Sistemas
				11.4.6		Monitear la red para detectar potenciales brechas de seguridad	Sistemas
				12.6.1		Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
	A6	V6	Mal funcionamiento del ups	9.2.2	Daño de equipo	Evitar la interrupción de servicios	Sistemas - SSAA
				14.1.3		Diseñar e implantar plan de contingencia	Dirección / dueño de información
				14.1.5		Revisión del plan de continuidad del negocio	Sistemas
	A7	V7	Funcionamiento de código malicioso	10.6.1	Degradación de equipos	Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				11.4.1		Informar sobre el uso de politicas de la red	Sistemas
				11.4.2		Proveer mecanismo para no comprometer la seguridad cuando se conecten usuarios externos a la institución	Sistemas
				11.4.3		Proveer mecanismo de autenticación de nodos en la red	Sistemas
				11.4.4		Proveer mecanimso de control sobre puertos que pueden permitir accesos no autorizados	Sistemas
				12.6.1		Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
	A8	V8	Falta de mantenimiento	9.2.4	Fallas de hardware	Diseño y ejecución del plan de mantenimiento	Sistemas- SSAA
	A9	V9	Falta de control de acceso	9.1.1	Manipulación no autorizada de las configuraciones	Proveer de una adecuada protección fisica	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Servidores				11.2.2		Proveer procedimiento de revisión de privilegios de usuarios	Sistemas
				11.2.4		Revisión delaccesos a las aplicaciones críticas	Sistemas
				11.5.2		Proveer a cada usaurio de un identificador único con el fin de poder tener registros posteriores	Sistemas
	A10	V10	Falta de conocimiento de seguridad por parte del personal	8.2.2	Violaciones a las seguridades	Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				13.1.1		Implementar procedimientos de divulgación formal de debilidades de la segruidad de la información asi como su respuesta	Dirección-Sistemas
				13.2.1		Implementar responsabiliaddes y procedimientos para respusta ágil a los incidentes	Dirección-Sistemas
	A11	V11	Falta de plan de continuidad del negocio	10.5.1	Perdidas de configuraciones, disponibilidad, entre otros	Implentación de politica de respaldos de información	Sistemas-Jefes departamentales
				14.1.1		Implementar controles para la identificación y reducción del riesgo	Dirección-Jefes departamentales
				14.1.3		Diseñar e implantar plan de contingencia	Dirección / dueño de información
	A12	V12	Falta de conexiones seguras	10.6.1	Posibiliad de snifers en la red	Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				11.4.2		Proveer mecanismo para no comprometer la seguridad cuando se conecten usuarios externos a la institución	Sistemas
				11.4.4		Proveer mecanimso de control sobre puertos que pueden permitir accesos no autorizados	Sistemas
				11.5.2		Proveer a cada usaurio de un identificador único con el fin de poder tener registros posteriores	Sistemas
				12.6.1		Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
	A13	V13	Falta de monitoreo de servidores	10.10.2	Daño en el servidor	Monitoero apopiadao del servidor para detectar brechas de seguridad	Sistemas
				10.10.4		Registrar lo detectado por los administradores y operadores del servidor	Sistemas
				10.10.5		Verificación de los registros de fallas del servidor	Sistemas
				11.4.2		Proveer mecanismo para no comprometer la seguridad cuando se conecten usuarios externos a la institución	Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Servidores				11.4.4		Proveer mecanimso de control sobre puertos que pueden permitir accesos no autorizados	Sistemas
	A14	V14	Ataque destructivo	9.1.1	Robo de equipo	Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección-SSAA
Equipos de Oficina	A4	V4	Falta de mantenimiento	9.2.4	Fallas de hardware	Diseño y ejecución del plan de mantenimiento	Sistemas- SSAA
	A5	V5	Ataque destructivo	12.6.1	Robo de suministro	Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
				13.1.1		Implementar procedimientos de divulgación formal de debilidades de la segruidad de la información así como su respuesta	Dirección-Sistemas
	A6	V6.1	Falta de políticas	5.1.1	Uso de equipos para fines no institucionales	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas
	A6	V6.2	Falta de control de acceso	6.1.4	Uso de equipos para fines no institucionales	Implantación de procesos de autorización	Jefes Departamentales
				8.1.1		Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				8.1.3		Informar a los empleados sobre las condiciones contractuales	RRHH
				8.2.1		Informar sobre las responasbiliades de los empleados	RRHH
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Soporte Electrónico	A5	V5	Falta de protección física	9.2.1	Posibilidad de robo o daño de soportes	Ubicar al equipo en lugar adecuado para prevenir acceso no autorizados	Sistemas
				11.7.1		Establecer políticas y medio necesarios para el uso seguro de dispositivos	Sistemas
	A6	V6	Manipulación no adecuada de información	10.7.1	Fuga de información	Establecer procedimientos de uso de medios removibles	Dirección
				10.7.3		Establecer procedimiento adecuado de manipulación de la información	Dirección-Jefes departamentales
				11.3.3		Establecer políticas de limpieza de escritorio	Dirección
	A7	V7	Falta de atención del personal	7.1.1	Robo de soportes	Elaboración y mantenimiento de inventario de equipos	SSAA
				7.1.2		Asignación de bienes a los empleados	SSAA
				7.1.3		Difusión d guías de utilización adecuada de los recursos	Sistemas
				9.1.1		Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
				11.3.2		Informar a los usuarios sobre la protección de equipos	Sistemas
Documentación y Registro	A4	V4.1	Errores de los empleados	5.1.1	Mal funcionamiento de los respaldos	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas
				6.1.3		Asegurar entrenamiento adecuado de los empleados	RRHH
				8.1.1		Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
	A4	V4.2	Almacenamiento no protegido	9.1.1	Daño de documentos por fuerza bruta	Proveer de una adecuada protección física	Dirección-SSAA

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Documentación y Registro				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
				11.1.1		Implementación de políticas de seguridad de acceso	Dirección / dueño de información
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
	A5	V5	Almacenamiento no protegido	9.1.1	Daño de documentos por fuerza bruta	Proveer de una adecuada protección física	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
				11.1.1		Implementación de políticas de seguridad de acceso	Dirección / dueño de información
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
				15.1.3		Proteger los recursos críticos de la organización	Dirección
				15.1.4		Informar a los empleados sobre la ley de estadística	Jurídico
	A6	V6	Falta de conocimiento de seguridad por parte del personal	6.1.5	Violaciones a las seguridades	Revisión de los acuerdos de confidencialidad de acuerdo a la institución	Jefes departamentales
				10.7.3		Establecer procedimiento adecuado de manipulación de la información	Dirección-Jefes departamentales
	A7	V7	Falta de documentación actualizada del sistema	10.7.4	No existencia de documentación de cambios	Proteger la documentación del sistema de accesos no autorizados	Jefes departamentales
				12.5.1		Establecer procedimiento de control de cambios	Jefes departamentales
	A8	V8	Falta de control para el establecimiento de contratos	6.2.3	Violaciones a las normativas legales	Elaborar lineamientos de aplicaciones con terceros	Sistemas - SSAA
	A9	V9	Falta de protección física	9.1.1	Posibilidad de robo o daño de documentos	Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
	A10	V10	Falta de plan de continuidad del negocio	10.5.1	Perdidas de respaldos	Implentación de política de respaldos de información	Sistemas-Jefes departamentales

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Documentación y Registro				14.1.3		Diseñar e implantar plan de contingencia	Dirección / dueño de información
	A11	V11	Falta de entrenamiento de los empleados de las políticas	6.1.3	Modificación no autorizada de información	Asegurar entrenamiento adecuado de los empleados	RRHH
Empleados	A1	V1	Falta de entrenamiento y oportuno entrenamiento	8.1.1	Violaciones a los reglamentos	Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				8.1.2		Establecer política de selección de personal	RRHH
				8.2.1		Informar sobre las responsabilidades de los empleados	RRHH
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
	A2	V2	Falta de acuerdos definidos para reemplazo de empleados	8.2.1	Mala elección de los reemplazos	Informar sobre las responsabilidades de los empleados	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
	A3	V3	Falta de acuerdo de confidencialidad	6.1.5	Divulgación de información sensitiva	Violaciones a las seguridades	Revisión de los acuerdos de confidencialidad de acuerdo a la institución
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
Establecimiento	A3	V3.1	Falta de protección física	9.1.2	Robo de bienes	Proveer a los empleados medios de seguridad en sus oficinas	Dirección
				11.1.1		Implementación de políticas de seguridad de acceso	Dirección / dueño de información
				13.1.2		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
	A3	V3.2	Falta de políticas	5.1.1	Acceso no autorizada por personal	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Servicio de Comunicaciones	A4	V4	Falta de mantenimiento	9.2.4	Mal funcionamiento por error de la configuración	Diseño y ejecución del plan de mantenimiento	Sistemas- SSAA
	A5	V5	Falta de conocimiento del administrador	10.10.1	Mayor tiempo de respuesta ante una falla	Documentar procedimientos de actualización	Sistemas
				11.7.2		Implementar políticas para teletrabajo	Sistemas
	A6	V6	Falta de control de acceso	11.7.2	Problemas en cambio de configuración	Implementar políticas para teletrabajo	Sistemas
	A7	V7	Falta de políticas	5.1.1	Uso para fines no institucionales	Utilización de recursos para fines diferentes al negocio	Elaboración de documento de políticas de seguridad de la información
				6.1.1		Apoyo de la Dirección las actividades de seguridad de la información	Dirección
				8.1.1		Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				8.1.3		Informar a los empleados sobre las condiciones contractuales	RRHH
				8.2.1		Informar sobre las responsabilidades de los empleados	RRHH
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usuarios sobre la protección de equipos	Sistemas
	A8	V8	Falta de protección adecuada	9.1.1	Manipulación o robo de los cables	Proveer de una adecuada protección física	Dirección-SSAA
				9.1.2		Implementar controles físicos en las entradas	Dirección-SSAA
				9.1.3		Proveer a los empleados medios de seguridad en sus oficinas	Dirección
	A9	V9	Falta de acuerdos con terceros	10.2.1	Mayor tiempo de habilitación de servicios ante una caída	Realizar acuerdos de niveles de servicio con proveedores	Jefes departamentales

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Servicio de Comunicaciones				10.2.2		Revisión de los acuerdos de niveles de servicio	Jefes departamentales
Servicio email	A1	V1	Falta de conocimiento de uso del servicio	7.1.3	Violaciones a las normativas internas	Difusión d guías de utilización adecuada de los recursos	Sistemas
				10.1.1		Documentar procedimientos de actualización	Sistemas
	A2	V2	Falta de control de acceso	10.6.1	Suplantación de usuario	Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				11.2.1		Establecer procedimiento de registro de ingreso y salida de usuarios	Dirección
				11.2.4		Revisión del accesos a las aplicaciones criticas	Sistemas
	A3	V3	Falta de establecimiento de una conexión segura	10.6.1	Por medio de un sniffer se podrían capturar paquetes	Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				12.3.1		Establecer políticas de medidas criptográficas	Sistemas
	A4	V4	Falta de políticas	5.1.1	Uso del servicio para fines no institucionales	Utilización de recursos para fines diferentes al negocio	Elaboración de documento de políticas de seguridad de la información
				6.1.4		Implantación de procesos de autorización	Jefes Departamentales
				8.1.1		Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				8.1.3		Informar a los empleados sobre las condiciones contractuales	RRHH
				8.2.1		Informar sobre las responsabilidades de los empleados	RRHH
				8.2.2		Informar a los empleados sobre leyes y normativas	RRHH
				8.2.3		Informar a los empleados sobre los sanciones disciplinarias por incurrir en violaciones a las normativas	RRHH
				11.3.1		Informar a los usuarios sobre el uso adecuado de las contraseñas	Sistemas
				11.3.2		Informar a los usarios sobre la protección de equipos	Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Servicio email	A5	V5	Falta de acuerdos definidos con proveedores	10.2.1	Mayor costo en tiempo y en dinero para reponer servicio	Realizar acuerdos de niveles de servicio con proveedores	Jefes departamentales
				10.2.2		Revisión de los acuerdos de niveles de servicio	Jefes departamentales
Portal de Informacion	A1	V1	Falta de procedimientos para cambios	8.1.1	Modificación no autorizada del sitio	Procedimiento para la elección oportuna de los empleados, sus roles y responsabilidades	RRHH-Jefes Departamentales
				10.1.1		Documentar procedimientos de actualización	Sistemas
				10.1.2		Monitoreo de cambios en el portal	Sistemas
				11.1.1		Implementación de políticas de seguridad de acceso	Dirección-Sistemas
				11.2.2		Proveer procedimiento de revisión de privilegios de usuarios	Sistemas
				11.4.4		Proveer mecanismo de control sobre puertos que pueden permitir accesos no autorizados	Sistemas
				12.5.1		Establecer procedimientos formales de cambios en el portal	Sistemas
	A2	V2	Falta de recursos necesarios	6.2.3	Negación del servicio	Asegurar que en los acuerdos no existan problemas entre las organizaciones	Sistemas-SSAA
				10.2.3		Manejar los cambios en la provisión de servicios	Sistemas
	A3	V3	Fallas en los acuerdos de niveles de servicios	10.2.1	No disponibilidad del sitio	Realizar acuerdos de niveles de servicio con proveedores	Dirección-Sistemas
				10.2.2		Revisión de los acuerdos de niveles de servicio	Sistemas
	A4	V4	Falta de procedimientos aprobados	10.1.2	Publicación errónea de información	Documentar los cambios operacionales que se den	Sistemas
Imagen Empresa	A1	V1	Insuficiente seguridad de la información	5.1.1	Divulgación de datos de empadronados	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas
				6.1.4		Establecer procedimientos para la autorización de FPI	Sistemas
				8.1.3		Informar a los empleados sobre las condiciones contractuales	RRHH

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Paquete Software	A1	V1	Insuficiencia de recursos	10.3.1	No instalación de software	Planificar la capacidad de los diferentes sistemas y servicios	Sistemas-SSAA
				12.6.1		Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
	A2	V2	Falta de protección	10.4.1	Ataques de virus	Establecer controles de prevención y recuperación de código malicioso	Sistemas
				12.5.1		Establecer procedimientos formales de cambios en el SO	Sistemas
				12.5.2		Revisión y pruebas de cambio en SO antes de ejecutarlas	Sistemas
				12.6.1		Analizar SO respecto a sus vulnerabilidades técnicas	Sistemas
	A3	V3	Falta de control de actualización	10.4.1	Fuga de información	Establecer controles de prevención y recuperación de código malicioso	Sistemas
				12.5.1		Establecer procedimientos formales de cambios en el SO	Sistemas
				12.5.2		Revisión y pruebas de cambio en SO antes de ejeciutarlas	Sistemas
	A4	V4	Falta de copias de seguridad	10.5.1	Perdida de datos en la instalación	Implantación de política de respaldos de información	Sistemas-Jefes departamentales
	A5	V5	Falta de políticas de seguridad	5.1.1	Uso para fines personales	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas
				13.1.1		Implementar procedimientos de divulgación formal de debilidades de la seguridad de la información así como su respuesta	Dirección-Sistemas
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Sistemas Operativos	A1	V1	Capacidad insuficiente de recursos	10.3.1	Negación del servicio	Planificar la capacidad de los diferentes sistemas y servicios	Sistemas-SSAA
				12.6.1		Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
	A2	V2.1	Falta de capacitación del administrador	10.10.1	Errores en la configuración	Analizar y revisión de informes de auditorías	Sistemas
				11.2.1		Establecer procedimiento de registro de ingreso y salida de usuarios del área de SO	Dirección-Sistemas
	A2	V2.2	Incompleta documentación del sistema	12.5.1	Errores en la configuración	Establecer procedimientos formales de cambios en el SO	Sistemas
	A3	V3	Falta de protección actualizada	10.4.1	Ataques de virus	Establecer controles de prevención y recuperación de código malicioso	Sistemas
				12.5.1		Establecer procedimientos formales de cambios en el SO	Sistemas
				12.5.2		Revisión y pruebas de cambio en SO antes de ejecutarlas	Sistemas
				12.6.1		Monitoreo y reportes sobre vulnerabilidades técnicas de los SI	Sistemas
				12.5.4		Uso de paquetes de SO tal y cual lo entrego el proveedor	Sistemas
	A4	V4	Falta de copias de seguridad	10.5.1	Perdida de información al restaurar copias de seguridad	Implantación de política de respaldos de información	Sistemas-Jefes departamentales
				14.1.3		Diseñar e implantar plan de contingencia	Dirección / dueño de información
	A5	V5.1	Actualizaciones incorrectas	10.1.1	Mal funcionamiento del sistema	Documentar procedimientos de actualización	Sistemas
				10.1.2		Monitoreo de cambios en el SO	Sistemas
				12.5.1		Establecer procedimientos formales de cambios en el SO	Sistemas
				12.5.2		Revisión y pruebas de cambio en SO antes de ejecutarlas	Sistemas

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Sistemas Operativos	A5	V5.2	Instalación de software no autorizado	10.1.1	Errores en la configuración	Documentar procedimientos de actualización	Sistemas
				10.4.1		Establecer controles de prevención y recuperación de código malicioso	Sistemas
	A6	V6	Falta de politicas de seguridad	5.1.1	Uso para fines personales	Elaboración de documento de políticas de seguridad de la información	Dirección-Sistemas
				13.1.1		Implementar procedimientos de divulgación formal de debilidades de la seguridad de la información asi como su respuesta	Dirección-Sistemas
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales
	A7	V7	Falta de control de acceso	11.1.1	Alteración no autorizada de la configuración	Implementación de políticas de seguridad de acceso	Dirección / dueño de información
				11.2.2		Proveer procedimiento de revisión de privilegios de usuarios	Sistemas
Medios y Soporte	A1	V1	Falta de control de acceso	9.2.3	Filtración de pcs externas a la institución	Proteger a los cables de red de accesos no autorizados	Sistemas-SSAA
				10.6.1		Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				11.4.2		Proveer mecanismo para no comprometer la seguridad cuando se conecten usuarios externos a la institución	Sistemas
				11.4.3		Proveer mecanismo de autenticación de nodos en la red	Sistemas
				11.4.4		Proveer mecanismo de control sobre puertos que pueden permitir accesos no autorizados	Sistemas
				11.4.6		Monitear la red para detectar potenciales brechas de seguridad	Sistemas
				13.2.1		Implementar responsabilidades y procedimientos para respuesta ágil a los incidentes	Dirección-Sistemas
				15.2.1		Verificación del cumplimiento de los procedimientos	Jefes Departamentales

Tabla 3.18 de Plan de Acción

						Plan de Acción	
ACTIVO	**ID AMENAZA**	**ID Vulnera**	**Vulnerabilidad**	**Control ISO 27001**	**Riesgo**	**Actividad**	**Responsable**
Medios y Soporte	A1	V1	Falta de control de acceso	9.2.3	Filtración de pcs externas a la institución	Proteger a los cables de red de accesos no autorizados	Sistemas-SSAA
	A2	V2	Falta de protección física	7.1.1	Robo de soportes	Elaboración y mantenimiento de inventario de equipos	SSAA
				7.1.2		Asignación de bienes a los empleados	SSAA
				7.1.3		Difusión d guias de utilización adecuadda de los recursos	Sistemas
				9.2.3		Proteger a los cables de red de accesos no autorizados	Sistemas-SSAA
				13.1.1		Implementar procedimientos de divulgación formal de debilidades de la segruidad de la información asi como su respuesta	Dirección-Sistemas
				13.2.1		Implementar responsabiliaddes y procedimientos para respusta ágil a los incidentes	Dirección-Sistemas
	A4	V4	Falta de red segura	10.6.1	Intercepción de información viaja en texto plano	Proveer mecanismo para evitar la negación del servicio	Sistemas
				10.6.2		Proveer mecanismo para mantener la confidencialidad de los datos	Sistemas
				12.3.1		Establecer politicas de medidas criptogrpaficas	Sistemas
	A5	V5	Falta de monitoreo de la red	10.10.2	Creación de brechas de seguridad	Monitoero apopiadao de los servicios para detectar brechas de seguridad	Sistemas
				10.10.4		Registrar lo detectado por los administradores y operadores de servicios	Sistemas
				10.10.5		Monitoreo de fallas registadas de los servicios	Sistemas

Tabla 3.18 de Plan de Acción

Para un mayor detalle de las actividades para minimizar los riesgos por favor referirse al anexo A, en cual esta descrito por control las actividades.

CAPITULO IV: IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1. MANUAL DE PROCEDIMIENTOS PARA LA IMPLEMENTACIÓN DEL SGSI

A continuación se describe sugerencias sobre el contenido del manual de procedimientos para implementar el SGSI en la Institución, respecto a 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 del Organismo 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 la Institución Metropolitana de Salud 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 Institución, (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 institución. 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 Dilit-Inec y el uso adecuado de los mismos.

El propósito de este manual es establecer las directrices, los procedimientos y los requisitos para asegurar la protección apropiada de Dilit-Inec 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 Institución.

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 Institución 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 Institución 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 Institución 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 Institución. 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 la Institución.

b) Protección de los activos de la Institución, incluyendo:

Procedimientos para proteger los bienes de la Institución, 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 Institución 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 Seguridad Informática 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 superan 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:

• Asignarle una fecha de efectividad.

• Comunicárselo al depositario del recurso.

• Realizar los 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 Institución 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 del Organismo 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 Institución y, cuando sea necesario, los usuarios externos y los terceros que desempeñen funciones en la Institución, 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 Institución recibirá el material, indicándosele el comportamiento esperado en lo que respecta a la seguridad de la información,

antes de ser 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 Institución 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 Institución. 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 Institución 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 la institución, todos los contratos y acuerdos con terceros, pues es necesario garantizar la institución de consideraciones relativas a la seguridad de la información involucrada en la gestión de los productos o servicios prestados.

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 Institución. 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 la Institución 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 la institución 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 la institución, 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.

POLITICA 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 acceso 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 Institución 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 institución 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 institución.

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 institución 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 la institución, por el proveedor o por un tercero.

c) Evaluar el impacto que se produce si la institución 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 Institución 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 la institución 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 Dilit-Inec utilizó el antivirus McAfee.

GESTION DE INCIDENTES DE SEGURIDAD DE LA INFORMACION

Divulgación de eventos y de debilidades de la seguridad de la información Es importante que la institución 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 institución.

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 Dilit-Inec 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 incluida en los planes de seguridad de información globales de su organización.

GESTION 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 institución.

El plan de continuidad debe mantenerse actualizado y ser una parte integrada en los diversos procesos de los diferentes departamentos de la institución.

Objetivo

Este control es importante para cubrir los puntos críticos de la institución 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.

Alcance

Estos controles se aplican a los críticos de la Institución.

Aspectos de la gestión de continuidad del negocio

Al desarrollar el plan de la continuidad del negocio para la institución, 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 la institución, 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 conscientes 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 a asignarse a cada persona responsable de un proceso determinado, para el caso de la institución 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 institución.

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 Dili-Inec.

Derechos de propiedad intelectual

Es necesario para toda organización conocer las leyes para no tener problemas futuros debido al 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:

• Ley de Propiedad Intelectual N° 83, Registro Oficial 320 de 19 de Mayo de 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 la institución 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:

• Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Nº 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."

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 institución 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:

• Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos Nº 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.

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.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

El Sistema de Gestión de Seguridad de Información se define para cada Organización 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 SGSI 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 absoluta no existe, lo que se trata es de reducir el riesgo a niveles aceptables. La seguridad es una actividad continua y la aplicación de la propuesta para mejorar la seguridad requiere el soporte de todos los funcionarios.

Para implantar una adecuada gestión de seguridad de información en una institución, el primer paso es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución.

EL SGSI debe verse no como un objetivo en sí mismo, sino como un medio de apoyo a la consecución de los objetivos.
La institución cuenta con un inventario de activos de información, donde se evidencia la criticidad y los riesgos de los mismos.

La concientización de la compañía es un pilar fundamental de esta norma, por lo cual las organizaciones deben ingeniosamente buscar y adoptar mecanismos que permitan que se despierte un interés y compromiso por parte de todos los empleados. Existen mecanismos como bonos, viajes, cenas o reconocimientos públicos que siempre despiertan interés.

El eslabón más débil de la cadena son las personas, por lo tanto dentro del análisis y evaluación del riesgo del SGSI se debe dar el énfasis necesario para considerar este tipo de amenazas. Siempre aplicando en los perfiles el principio del mínimo conocimiento.

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.

Para determinar el alcance del SGSI se utilizó el método de las elipses 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, los cuales no estaban identificados.

La planificación es una parte crucial para una adecuada implementación del SGSI, 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.

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 27001.

5.2 RECOMENDACIONES

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.

Revisión de la propuesta de implementación de los controles acorde al momento en que se decida implementar.
Realizar análisis periódicos de los riesgos y monitorear continuamente la situación, pues la seguridad que se requiere proporcionar con un SGSI es permanente para lo cual es necesario de un proceso continuo, más no de acciones puntuales

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.

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.

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, normas de control interno de la contraloría, entre otras

Se recomienda la implementación de la norma 27001 porque a más de proteger a la empresa razonablemente, permite mejorar la imagen al exterior.

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.

GLOSARIO
TÉRMINOS Y DEFINICIONES

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 Sistema 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 savalguardias, 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.

ANEXO A

ACTIVIDADES A REALIZAR EN LOS CONTROLES SUGERIDOS

Política de Seguridad (5.1.1)

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 reportado y todas las evidencias necesarias serán recopiladas. Las personas que trabajan en Dilit-Inec 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, especifica la dirección de seguridad que va a seguir la empresa, se reducirá este problema si en la institución se emite políticas de seguridad y se da conocer a todo el personal.

Asignación de responsabilidades sobre seguridad de la información (6.1.3)

Asegurar un entrenamiento adecuado de los empleados, mejorando la cultura de la seguridad de información en Dilit-Inec, 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 (6.1.4)

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 Dilit-Inec, para evitar el mal uso de los activos.

Responsabilidad sobre los activos. Inventario de activos (7.1.1)

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 institución.

Propiedad de los recursos (7.1.2)

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 institución.

Uso aceptable del uso de los recursos (7.1.3)

Para minimizar este riesgo se utilizan guías de utilización de los activos fuera de las premisas de la institución.

Seguridad en la definición del trabajo y los recursos.
Roles y responsabilidades (8.1.1)

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 (8.1.2)

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 (8.1.3)

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 (8.2.1)

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 (8.2.2)

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 institución, lo cual reducirá los errores de los empleados y también limitará los problemas que podría ocurrir y sus impactos.

Proceso disciplinario (8.2.3)

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 institución deben tener conocimiento de los riesgo que se toma al ejecutar código malicioso desconocido y que consecuencias puede traer esta acción, este debe ser un proceso disciplinario continuo.

Áreas seguras

Perímetro de seguridad física (9.1.1)

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 la institución:

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 (9.1.2)

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 (9.1.3)

Con este control se da una protección física adecuada a los activos de la institución, 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 (9.2.2)

Se evita la interrupción de los servicios que ofrecen los activos con la aplicación de estos controles

Mantenimiento de equipos (9.2.4)

Se minimiza este riesgo con un apropiado mantenimiento de los equipos de la Institución

Seguridad de equipos fuera de los locales de la organización (9.2.5)

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.

Procedimientos y responsabilidades de operación

Documentación de procedimientos operativos (10.1.1)

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 solos los procedimientos de operación permitidos y necesarios para la ejecución del Sistema Operativo.

Control de cambios operacionales (10.1.2)

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 (10.2.1)

Con este control se busca reducir las fallas en los acuerdos de niveles de servicio con partes externas, para lo cual la institución debe mantener un nivel apropiado de seguridad y chequea la implementación de los acuerdos.

Monitorización y revisión de los servicios de las terceras partes (10.2.2)

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 (10.3.1)

Con una adecuada planificación del sistema se evitará la degradación del servicio.

Aceptación del sistema (10.3.2)

Con una adecuada planificación del sistema se evitará la degradación del servicio.

Protección contra software malicioso.

Controles contra software malicioso (10.4.1)

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 reducirá la probabilidad de que este problema ocurra mediante la implementación de procedimientos apropiados para la protección contra SW malicioso.

Gestión interna de respaldo.

Recuperación de la información (10.5.1)

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 (10.6.1)

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 (10.6.2)

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.

Utilización de los medios de información.

Gestión de medios removibles (10.7.1)

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 (10.7.3)

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 (10.8.4)

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 (10.8.5)

Se trata de minimizar la transmisión de SW malicioso a través del uso de comunicaciones electrónicas.

Monitorización.

Registro de auditoria (10.10.1)

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 institución herramientas de administración de redes para realizar una adecuada monitorización y detectar a tiempo huecos de seguridad.

Monitorización del uso del sistema (10.10.2)

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 (10.10.4)

Una monitorización apropiada detectaría a tiempo brechas de seguridad y así

reducirá los impactos que puede causar estas brechas de seguridad

Registro de fallas (10.10.5)

Monitorización apropiada detectaría a tiempo brechas de seguridad y así reducirá los impactos que puede causar estas brechas de seguridad.

Requerimiento de negocios para control de acceso

Política de control de acceso (11.1.1)

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 (11.2.1)

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 (11.2.2)

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 (11.2.4)

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 (11.3.1)

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 (11.3.2)

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 (11.3.3)

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 (11.4.1)

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 (11.4.2)

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 institución.

Autenticación de nodos de la red (11.4.3)

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 (11.4.4)

Es necesario mantener un control sobre puertos que pueden ser una puerta de ingreso no autorizado a la información de la institución, por lo cual se deben definir los puertos necesarios y bloquear los demás

Control de conexión a las redes (11.4.6)

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 acceso al sistema operativo

Identificación y autenticación del usuario (11.5.2)

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 (11.6.2)

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.

Controles criptográficos

Política de uso de los controles criptográficos (12.3.1)

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 (12.5.1)

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 (12.5.2)

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 (12.5.3)

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 (12.5.4)

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 hackers o intrusos.

Gestión de vulnerabilidad técnica

Control de vulnerabilidades técnicas (12.6.1)

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.

Divulgación de eventos y de debilidades de la seguridad de la información

Divulgación de eventos de la seguridad de la información (13.1.1)

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 (13.2.1)

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.

Aspectos de la gestión de continuidad del negocio

Proceso de gestión de la continuidad del negocio (14.1.1)

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 (14.1.3)

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.

Cumplimiento con los requisitos legales

Derechos de propiedad intelectual (15.1.2)

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 (15.1.3)

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 (15.1.4)

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 (15.1.5)

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 (15.2.1)

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.

ANEXO B

CONTROLES SELECCIONADOS DE LA NORMA ISO 27001 POR AMENAZA

Los controles seleccionados para las opciones que de acuerdo al plan de tratamiento del riesgo deben ser reducidas, son los que se adjunta en la siguiente lista:

HARDWARE PORTÁTIL:

Amenazas	***Vulnerabilidades***
Acceso no autorizado a la portátil	Falta de Protección por desatención de equipos

9.2. Seguridad de los equipos

9.2.5. Seguridad de equipos fuera de los locales de la organización

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

15.2. Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado

9.2. Seguridad de los equipos

9.2.2. Utilidades de apoyo

14.1. Aspectos de la gestión de continuidad del negocio

14.1.3. Desarrollo e implantación de planes de contingencia

14.1.5. Prueba, Mantenimiento y reevaluación de los planes

Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados

8.2. Durante el empleo

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

15.2. Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

Uso no previsto	Falta de las políticas

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

6.1. Organización interna

6.1.4. Proceso de autorización de recursos para el tratamiento de la información

8.1. Seguridad en la definición del trabajo y los recursos

8.1.1. Roles y responsabilidades

8.1.3. Términos y condiciones de la relación laboral

8.2. Durante el empleo

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

11.5. Control de acceso al sistema operativo

11.5.1. Procedimientos de conexión de terminales

Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal

8.2. Durante el empleo

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario

13.1. Divulgación de eventos y de debilidades de la seguridad de la información

13.1.1. Divulgación de eventos de la seguridad de la información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Degradación del hardware	Falta de mantenimiento adecuado

9.2. Seguridad de los equipos

9.2.4. Mantenimiento de equipos

No autorizada copia de software o información propietaria	Falta de políticas

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

15.1. Cumplimiento con los requisitos legales

15.1.2. Derechos de propiedad intelectual

15.1.4. Protección de los datos y de la privacidad de la información personal

Ataque destructivo	Falta de protección física

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

Robo	Falta de protección física

7.1. Responsabilidad sobre los activos

7.1.1. Inventario de activos

7.1.2. Propiedad de los recursos

7.1.3. Uso aceptable del uso de los recursos

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

11.3. Responsabilidades de los usuarios

11.3.2. Equipo informático de usuarios desatendido

PCs DE OFICINA

Amenazas	***Vulnerabilidades***
Acceso no autorizado al equipo	Falta de Protección por desatención de Equipos

9.2. Áreas seguras

9.2.5. Seguridad de equipos fuera de los locales de la organización

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

15.2. Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado

9.2. Seguridad de los equipos

9.2.2. Utilidades de apoyo

14.1. Aspectos de la gestión de continuidad del negocio

14.1.3. Desarrollo e implantación de planes de contingencia

14.1.5. Prueba, Mantenimiento y reevaluación de los planes

Incumplimiento con la legislación	Falta de conocimiento de protección de derechos de SW por parte de los empleados

8.2. Durante el empleo

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

15.2. Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

Uso no previsto	Falta de las políticas

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

6.1. Organización interna

6.1.4. Proceso de autorización de recursos para el tratamiento de la información

8.1. Seguridad en la definición del trabajo y los recursos

8.1.1. Roles y responsabilidades

8.1.3. Términos y condiciones de la relación laboral

8.2. Durante el empleo

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

11.5. Control de acceso al sistema operativo

11.5.5. Procedimientos de conexión de terminales

Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal

8.2. Durante el empleo

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario

13.1. Divulgación de eventos y de debilidades de la seguridad de la información

13.1.1. Divulgación de eventos de la seguridad de la información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Degradación del Hardware	Falta de mantenimiento adecuado

9.2. Seguridad de los equipos

9.2.4. Mantenimiento de equipos

Inautorizada copia de software o información propietaria	Falta de políticas

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

15.1. Cumplimiento con los requisitos legales

15.1.2. Derechos de propiedad intelectual

15.1.4. Protección de los datos y de la privacidad de la información personal

Ataque destructivo	Falta de protección física

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

Robo	Falta de protección física

7.1. Responsabilidad sobre los activos

7.1.1. Inventario de activos

7.1.2. Propiedad de los recursos

7.1.3. Uso aceptable del uso de los recursos

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

11.3. Responsabilidades de los usuarios

11.3.2. Equipo informático de usuarios desatendido

SERVIDORES

Amenazas	***Vulnerabilidades***
Negación de Servicio	Incapacidad de distinguir una petición real de una falsa

10.6. Gestión de la seguridad de red,

10.6.1. Controles de red

10.6.2. Seguridad de los servicios de red

11.4. Control de acceso a la red

11.4.1. Política de uso de los servicios de la red

11.4.2. Autenticación de usuarios para conexiones externas

11.4.3. Autenticación de nodos de la red

11.4.4. Protección a puertos de diagnóstico remoto

11.4.6. Control de conexión a las redes

12.6. Gestión de Vulnerabilidad Técnica

12.6.1. Control de Vulnerabilidades Técnicas

Corte de suministro eléctrico o Falla en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado

9.2. Seguridad de los equipos

9.2.2. Utilidades de apoyo

14.1. Aspectos de la gestión de continuidad del negocio

14.1.3. Desarrollo e implantación de planes de contingencia

14.1.5. Prueba, Mantenimiento y reevaluación de los planes

Acceso no autorizado a través de la red	Código malicioso desconocido

10.6. Gestión de la seguridad de red

10.6.1. Controles de red

10.6.2. Seguridad de los servicios de red

11.4. Control de acceso a la red

11.4.1. Política de uso de los servicios de la red

11.4.2. Autenticación de usuarios para conexiones externas

11.4.3. Autenticación de nodos de la red

11.4.4. Protección a puertos de diagnóstico remoto

11.4.6. Control de conexión a las redes

12.6. Gestión de Vulnerabilidad Técnica

12.6.1. Control de Vulnerabilidades Técnicas

Degradación o Falla del hardware	Falta de mantenimiento adecuado

9.2. Seguridad de los equipos

9.2.4. Mantenimiento de equipos

Manipulación de la configuración	Falta de control de acceso

9.1.1. Perímetro de seguridad física

9.1.3. Seguridad de oficinas, despachos y recursos

11.2. Gestión de acceso de usuarios

11.2.2. Gestión de privilegios

11.2.4. Revisión de derechos de acceso de los usuarios

11.5. Control de acceso al sistema operativo

11.5.2. Identificación y autenticación del usuario

Incumplimiento con controles de seguridad	Falta de conocimiento de seguridad por parte del personal

8.2. Durante el empleo

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario

13.1. Divulgación de eventos y de debilidades de la seguridad de la información

13.1.1. Divulgación de eventos de la seguridad de la información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Incapacidad de restauración	Falta de planes de continuidad del negocio

10.5 Gestión interna de respaldo.

10.5.1 Recuperación de la información

14.1. Aspectos de la gestión de continuidad del negocio

14.1.1. Proceso de gestión de la continuidad del negocio

14.1.3. Desarrollo e implantación de planes de contingencia

Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)

10.6 Gestión de la seguridad de red.

10.6.1 Controles de red

10.6.2 Seguridad de los servicios de red

11.4. Control de acceso a la red

11.4.2. Autenticación de usuarios para conexiones externas

11.4.4. Protección a puertos de diagnóstico remoto

11.5. Control de acceso al sistema operativo

11.5.2. Identificación y autenticación del usuario

12.6. Gestión de Vulnerabilidad Técnica

12.6.1. Control de Vulnerabilidades Técnicas

Brechas de seguridad no detectadas	Falta de monitoreo de los servidores

10.10 Monitorización. Objetivo: Detectar actividades no autorizadas.

10.10.2 Monitorización del uso del sistema

10.10.4 Registros del administrador y operador

10.10.5 Registro de fallas

11.4. Control de acceso a la red

11.4.2. Autenticación de usuarios para conexiones externas

11.4.4. Protección a puertos de diagnóstico remoto

Ataque destructivo	Falta de protección física

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

EQUIPOS DE OFICINA

Amenazas	***Vulnerabilidades***
Degradación o Falla de HW	Falta de Mantenimiento

9.2. Seguridad de los equipos

9.2.4. Mantenimiento de equipos

Uso no previsto	Falta de Políticas Falta de Control de Acceso

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

6.1. Organización interna

6.1.4. Proceso de autorización de recursos para el tratamiento de la información

8.1. Seguridad en la definición del trabajo y los recursos

8.1.1. Roles y responsabilidades

8.1.3. Términos y condiciones de la relación laboral

8.2. Durante el empleo

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

11.5. Control de acceso al sistema operativo

11.5.1. Procedimientos de conexión de terminales

SOPORTE ELECTRÓNICO

Amenazas	***Vulnerabilidades***
Robo	Falta de atención del personal

7.1. Responsabilidad sobre los activos

7.1.1. Inventario de activos

7.1.2. Propiedad de los recursos

7.1.3. Uso aceptable del uso de los recursos

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

11.3. Responsabilidades de los usuarios

11.3.2. Equipo informático de usuarios desatendido

Escape de información	Manipulación inadecuada de información

10.7. Utilización de los medios de información

10.7.1. Gestión de medios removibles

10.7.3. Procedimientos de manipulación de la información

11.3. Responsabilidades de los usuarios

11.3.3. Políticas de limpieza de pantalla y escritorio

DOCUMENTACIÓN Y REGISTROS

Amenazas	***Vulnerabilidades***
Pérdida de información	Errores de los empleados

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información

6.1. Organización interna

6.1.3. Asignación de responsabilidades sobre seguridad de la información

8.1 Seguridad en la definición del trabajo y los recursos.

8.1.1 Roles y responsabilidades

8.2 Durante el empleo.

8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Pérdida de información	Errores de los empleados

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información

6.1 Organización interna.

6.1.3 Asignación de responsabilidades sobre seguridad de la información

8.1 Seguridad en la definición del trabajo y los recursos.

8.1.1 Roles y responsabilidades

8.2 Durante el empleo.

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Pérdida de información — Almacenamiento no protegido

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física

9.1.3 Seguridad de oficinas, despachos y recursos

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Divulgación de información de clientes — Almacenamiento no protegido

9.1 Áreas seguras.

9.1.1 Perímetro de seguridad física

9.1.3 Seguridad de oficinas, despachos y recursos

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

15.1. Cumplimiento con los requisitos legales

15.1.3. Salvaguarda de los registros de la organización

15.1.4. Protección de los datos y de la privacidad de la información personal

Ataque destructivo — Falta de protección física

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

9.1.4. Protección contra amenazas externas y ambientales

Incapacidad de restauración — Falta de planes de continuidad del negocio

10.5. Gestión interna de respaldo..

10.5.1. Recuperación de la información

14.1. Aspectos de la gestión de continuidad del negocio

14.1.3. Desarrollo e implantación de planes de contingencia

EMPLEADOS

Amenazas	***Vulnerabilidades***
Errores de los empleados y acciones Equivocadas	Falta de conocimiento y oportuno entrenamiento

8.1. Seguridad en la definición del trabajo y los recursos.

8.1.1. Roles y responsabilidades

8.1.2. Selección y política del personal

8.2. Durante el empleo..

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

ESTABLECIMIENTO

Amenazas	***Vulnerabilidades***
Acceso no autorizado	Falta de políticas

5.1. Política de seguridad de la información.

5.1.1. Documento de política de seguridad de la información

Acceso no autorizado	Falta de protección física

9.1 Áreas seguras.

9.1.2 Controles físicos de entradas

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

13.1. Divulgación de eventos y de debilidades de la seguridad de la información

13.1.2. Divulgación de debilidades de la seguridad

SERVICIO DE COMUNICACIONES

Amenazas	***Vulnerabilidades***
Degradación del servicio y equipos	Falta de mantenimiento adecuado

9.2. Seguridad de los equipos

9.2.4. Mantenimiento de equipos

Uso no previsto	Falta de políticas

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

6.1. Organización interna

6.1.4. Proceso de autorización de recursos para el tratamiento de la información

8.1. Seguridad en la definición del trabajo y los recursos

8.1.1. Roles y responsabilidades

8.1.3. Términos y condiciones de la relación laboral

8.2. Durante el empleo

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario

11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

15.1. Control de acceso al sistema operativo

15.1.5. Procedimientos de conexión de terminales

Ataque destructivo	Falta de protección física

9.1. Áreas seguras

9.1.1. Perímetro de seguridad física

9.1.2. Controles físicos de entradas

9.1.3. Seguridad de oficinas, despachos y recursos

9.1.4. Protección contra amenazas externas y ambientales

Fallas de servicios telefonía	Falta de acuerdos bien definidos con terceras partes

10.2 Gestión de servicios externos

10.2.1 Entrega del servicio

10.2.2 Monitorización y revisión de los servicios de las terceras partes

SERVICIO DE CORREO ELECTRÓNICO

Amenazas	***Vulnerabilidades***
Suplantación de la identidad del usuario	Falta de control de acceso

10.6 Gestión de la seguridad de red

10.6.1 Controles de red

10.6.2 Seguridad de los servicios de red

11.2. Gestión de acceso de usuarios

11.2.1. Registro de Usuarios

11.2.4. Revisión de derechos de acceso de los usuarios

Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)

10.6 Gestión de la seguridad de red.

10.6.1 Controles de red

10.6.2 Seguridad de los servicios de red

12.3. Controles criptográficos

12.3.1.Política de uso de los controles criptográficos

Uso no previsto	Falta de políticas

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

6.1. Organización interna

6.1.4. Proceso de autorización de recursos para el tratamiento de la información

8.1. Seguridad en la definición del trabajo y los recursos

8.1.1. Roles y responsabilidades

8.1.3. Términos y condiciones de la relación laboral

8.2. Durante el empleo

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario

11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

15.1. Control de acceso al sistema operativo

15.1.5. Procedimientos de conexión de terminales

Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes

10.2 Gestión de servicios externos

10.2.1 Entrega del servicio

10.2.2 Monitorización y revisión de los servicios de las terceras partes

PORTAL DE INFORMACIÓN DE LA INSTITUCIÓN

Amenazas	***Vulnerabilidades***
Modificación no autorizada del sitio Web	Falta de procedimientos para cambios

8.1 Seguridad en la definición del trabajo y los recursos.

8.1.1 Roles y responsabilidades

10.1 Procedimientos y responsabilidades de operación.

10.1.1 Documentación de procedimientos operativos

10.1.2 Control de cambios operacionales

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

11.2. Gestión de acceso de usuarios

11.2.2. Gestión de privilegios

11.4. Control de acceso a la red

11.4.4. Protección a puertos de diagnóstico remoto

12.5. Seguridad en los procesos de desarrollo y soporte

12.5.1. Procedimientos de control de cambios

Sitio Web no disponible — Fallas en los acuerdos de niveles de servicio

10.2 Gestión de servicios externos.

10.2.1 Entrega del servicio

10.2.2 Monitorización y revisión de los servicios de las terceras partes

SOFTWARE ESTÁNDAR

Amenazas	***Vulnerabilidades***
Uso no previsto	Falta de políticas de seguridad

5.1. Política de seguridad de la información

5.1.1. Documento de política de seguridad de la información

6.1. Organización interna

6.1.4. Proceso de autorización de recursos para el tratamiento de la información

8.1. Seguridad en la definición del trabajo y los recursos

8.1.1. Roles y responsabilidades

8.1.3. Términos y condiciones de la relación laboral

8.2. Durante el empleo

8.2.1. Responsabilidades de administración

8.2.2. Conocimiento, educación y entrenamiento de la seguridad de información

8.2.3. Proceso disciplinario 11.3. Responsabilidades de los usuarios

11.3.1. Uso de contraseñas

11.3.2. Equipo informático de usuarios desatendido

15.1. Control de acceso al sistema operativo

15.1.5. Procedimientos de conexión de terminales

Virus de Computación, Fuerza Bruta y ataques de diccionario — Falta de Protección (AV) actualizada

10.4 Protección contra software malicioso.

10.4.1 Controles contra software malicioso

12.5. Seguridad en los procesos de desarrollo y soporte

12.6. Gestión de Vulnerabilidad Técnica

12.6.1. Control de Vulnerabilidades Técnicas

12.5.4. Canales encubiertos y código troyano

Falta de capacidad de restauración — Falta de copias de backup continuas

10.5 Gestión interna de respaldo..

10.5.1 Recuperación de la información

14.1. Aspectos de la gestión de continuidad del negocio

14.1.3. Desarrollo e implantación de planes de contingencia

Pérdida de Servicio — Actualizaciones incorrectas

10.1 Procedimientos y responsabilidades de operación.

10.1.1 Documentación de procedimientos operativos

10.1.2 Control de cambios operacionales

12.5. Seguridad en los procesos de desarrollo y soporte

12.5.1. Procedimientos de control de cambios

12.5.2. Revisión técnica de los cambios en el Sistema Operativo

Pérdida de Servicio — Instalación de SW no autorizado

10.1 Procedimientos y responsabilidades de operación.

10.1.1 Documentación de procedimientos operativos

10.4 Protección contra software malicioso.

10.4.1 Controles contra software malicioso

12.5. Seguridad en los procesos de desarrollo y soporte

12.5.3. Restricciones en los cambios a los paquetes de SW

Controles de Seguridad no cumplidos — Falta de Políticas de Seguridad

5.1 Política de seguridad de la información.

5.1.1 Documento de política de seguridad de la información

13.1. Divulgación de eventos y de debilidades de la seguridad de la información

13.1.1. Divulgación de eventos de la seguridad de la información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

15.2. Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

Alteración no autorizado de la configuración — Falta de control de acceso

11.1. Requerimiento de negocios para control de acceso

11.1.1. Política de control de acceso

11.2. Gestión de acceso de usuarios

11.2.2. Gestión de privilegios

12.5. Seguridad en los procesos de desarrollo y soporte

12.5.3. Restricciones en los cambios a los paquetes de SW

MEDIOS Y SOPORTE

Amenazas	***Vulnerabilidades***
Acceso no autorizado a la información	Falta de control de acceso

9.2 Seguridad de los equipos.

9.2.3 Seguridad del cableado

10.6 Gestión de la seguridad de red.

10.6.1 Controles de red

10.6.2 Seguridad de los servicios de red

11.4. Control de acceso a la red

11.4.2. Autenticación de usuarios para conexiones externas

11.4.3. Autenticación de nodos de la red

11.4.4. Protección a puertos de diagnóstico remoto

11.4.6. Control de conexión a las redes

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

15.2. Revisiones de la política de seguridad y de la conformidad técnica

15.2.1. Conformidad con la política de seguridad

Robo	Falta de protección física

7.1 Responsabilidad sobre los activos.

7.1.1 Inventario de activos

7.1.2 Propiedad de los recursos

7.1.3 Uso aceptable del uso de los recursos

9.2 Seguridad de los equipos.

9.2.3 Seguridad del cableado

13.1. Divulgación de eventos y de debilidades de la seguridad de la información

13.1.1. Divulgación de eventos de la seguridad de la información

13.2. Administración de incidentes y mejoras de la seguridad de la información

13.2.1. Responsabilidades y procedimientos

Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)

10.6 Gestión de la seguridad de red.

10.6.1 Controles de red

10.6.2 Seguridad de los servicios de red

12.3. Controles criptográficos

12.3.1. Política de uso de los controles criptográficos

Brechas de seguridad no detectadas	Falta de monitoreo de la red

10.10 Monitorización.

10.10.2 Monitorización del uso del sistema

10.10.4 Registros del administrador y operador

10.10.5 Registro de fallas

BLIBIOGRAFÍA

http://www.tb-security.com

http://docquality.info.es

https://www.iso27000.es

https://www.isca.org

NIST; "ESPECIAL PUBLICATIONS", Internet. http://csrc.nist.gov/publications

Alexander Alberto Ph.D , Diseño de un Sistema de Gestión de Seguridad , Editorial Alfaomega, Colombia, 2007