DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA EN ELECTRÓNICA, REDES DE LA INFORMACIÓN Y COMUNICACIÓN DE DATOS

PROYECTO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN ELECTRÓNICA

AUTOR: ERIKA ELIZABETH VELOZ VILLAVICENCIO

TEMA: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE UNA EMPRESA ASEGURADORA

DIRECTOR: ING. DANILO CORRAL DE WITT

CODIRECTOR: ING. CARLOS ROMERO

SANGOLQUÍ, 2015

CERTIFICACIÓN

Certificamos que el presente proyecto de grado titulado: PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE UNA EMPRESA ASEGURADORA, ha sido desarrollado en su totalidad por la señorita ERIKA ELIZABETH VELOZ VILLAVICENCIO, bajo nuestra dirección.

Atentamente,

Ing. Danilo Corral De Witt

DIRECTOR

Ing. Carlos Romero Gallardo

CODIRECTOR

DECLARACIÓN DE RESPONSABILIDAD

ERIKA ELIZABETH VELOZ VILLAVICENCIO

DECLARO QUE:

El proyecto denominado "PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE UNA EMPRESA ASEGURADORA", ha sido desarrollado en base a una investigación exhaustiva, respetando los derechos intelectuales de terceros, conforme a las fuentes que se incorporan en la bibliografía.

Consecuentemente este trabajo es de mi entera autoría.

En virtud a esta declaración, me responsabilizo del contenido, veracidad y alcance del proyecto de grado en mención.

Sangolquí, marzo 2015.

Erika Elizabeth Veloz Villavicencio

AUTORIZACIÓN

ERIKA ELIZABETH VELOZ VILLAVICENCIO

Autorizo a la Universidad de las Fuerzas Armadas "ESPE" la publicación, en la biblioteca virtual de la institución el trabajo "PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA LA RED DE DATOS DE UNA EMPRESA ASEGURADORA", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, marzo 2015.

Erika Elizabeth Veloz Villavicencio

DEDICATORIA

A mis padres y abuelitos, por su incansable e ilimitado apoyo y amor incondicional a lo largo de toda mi vida estudiantil y compartir conmigo cada tristeza y alegría.

A mi hermana, por las sonrisas e innumerables momentos compartidos.

A todos, quienes han confiado en mí y me han motivado para concluir esta etapa de mi vida y me han incentivado para crecer y desarrollarme profesionalmente.

AGRADECIMIENTO

A Dios y a mi familia, quienes me han apoyado cada instante para que este sueño se convierta en realidad.

A mis tutores, quienes me ha guiado durante en el desarrollo del presente proyecto.

A la empresa aseguradora que me permitió desarrollar el proyecto, por la confianza y su colaboración durante la recolección de la información.

A mis amigos, quienes han compartidos los momentos más importantes de mi vida, me han hecho sonreír y me han acompañado durante todo el camino para conseguir mis metas.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El proyecto de tesis pretende establecer los principales lineamientos para diseñar y proponer un adecuado modelo de sistema de gestión de seguridad de información (SGSI) enfocado a la red de datos de una empresa de seguros ecuatoriana, la cual requiere garantizar que la tecnología de información actualmente en uso esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización. Se analizarán los procesos de seguridad actualmente empleados y se determinará si es necesario fortalecer las políticas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento. De acuerdo a la información obtenida y considerando los requerimientos de seguridad de la empresa, se propondrá la implementación del SGSI basado en la norma ISO 27001.

PALABRAS CLAVE:

- **AMENAZA A LA SEGURIDAD**
- **IMPACTO TECNOLÓGICO**
- **RIESGO**
- **VULNERABILIDAD**
- **SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN**

ABSTRACT

This thesis project pretends to establish the main lineaments to design and propose a suitable model of an information security management system, focused on a data network in an Ecuadorian insurance company. The aim of the project is to guarantee that the information technology currently used is according with the business strategy, as well as to verify that the actives of information have the protection level required according to the value and risk represented to the company. The security processes currently used in the company will be analyzed. Furthermore, the study will show if it is necessary to strengthen the security policies to guarantee the confidentiality, integrity and availability of information, as well as the systems involved in its treatment. According to the information obtained and considering the security requirements of the company, implementation of the information security management system based on the ISO 27001 will be proposed.

KEY WORDS:

- **MENACE TO SECURITY**
- **TECHNOLOGY IMPACT**
- **RISK**
- **VULNERABILITY**
- **INFORMATION SECURITY MANAGEMENT SYSTEM**

GLOSARIO

Amenaza: es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Impacto: consecuencia de la materialización de una amenaza.

Riesgo: combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas

Vulnerabilidad: posibilidad de ocurrencia de la materialización de una amenaza sobre un Activo.

Ataque: evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

SGSI (Sistema de Gestión de la Seguridad Informática): Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad de la información.

SI (Seguridad Informática): Se denomina seguridad informática al conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, se trata de un proceso en el cual participan personas.

PDCA (Plan, Do, Check, Act): El círculo PDCA o también conocido como ciclo de Deming, es una estrategia de mejora continua de la calidad en cuatro pasos: Planificar, hacer, verificar y actuar.

PRÓLOGO

Tomando en consideración la necesidad que la empresa ha manifestado en cuanto a perfilar un Sistema de Gestión Segura de Información (SGSI), enfocado a la red de datos de la empresa, el cual le permita administrar toda su información, garantizando los aspectos de confidencialidad, integridad, disponibilidad que debe cumplir; y tomando en cuenta que actualmente existen diferentes normas y estándares relacionados a la seguridad de información que pueden aplicarse; se pretende analizar e implementar un adecuado SGSI a partir del análisis de las mejores prácticas y metodologías existentes en la empresa.

Adicionalmente se pretende concientizar sobre los riesgos externos e internos a los que está expuesta la información y establecer políticas que disminuyan estos riesgos.

El proyecto de tesis pretende establecer los principales lineamientos para diseñar y proponer un adecuado modelo de sistema de gestión de seguridad de información (SGSI) enfocado a la red de datos en la empresa “SEGUROS EQUINOCCIAL S.A.”, la cual requiere garantizar que la tecnología de información actualmente en uso esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización.

Se recolectará información para determinar la situación actual de la empresa y a partir de sus lineamientos y políticas de seguridad se elaborará el plan de seguridad de la información para la red de datos se ajuste a sus necesidades y tenga perspectiva de crecimiento de la empresa.

OBJETIVOS

General:

Diseñar el plan estratégico de seguridad de la información en la red de datos de la empresa “SEGUROS EQUINOCCIAL S.A.”, partiendo del análisis de los procedimientos de seguridad que actualmente se siguen y la normativa existente, a fin mejorar la seguridad de las operaciones comerciales.

Específicos:

- Levantar los procesos de seguridad que utiliza la empresa.
- Analizar la situación actual de la seguridad con la que opera la empresa.
- Determinar las normas ISO (17799-27002) relativas al estándar de seguridad de la información aplicables al desarrollo del plan estratégico de seguridad.
- Diseñar los procedimientos de seguridad en base a la evaluación de riesgos y necesidades que presenta la empresa.
- Proponer el mejor plan estratégico de seguridad para que posteriormente la empresa lo implemente.

CAPÍTULO 1

MARCO TEÓRICO

1.1 Fundamentos de la Seguridad

La Organización Internacional para la Estandarización (ISO) define Seguridad de la Información (SI) como:

"La preservación de la confidencialidad, integridad y disponibilidad de la información; así como de los sistemas implicados en su tratamiento, dentro de una organización." (Alexander, 2006)

Otra definición que se ajusta al ámbito informático es: "la seguridad es la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles" (Subdirección General de Información, Documentación y Publicaciones, 2012)

La información es un recurso intangible y a la vez el activo más importante de una entidad, y tiene un sentido particular de acuerdo a la manera y a quien la procese y tiene las siguientes características:

- Crítica: Es indispensable para garantizar la continuidad operativa
- Valiosa: Es un activo con valor en sí misma
- Sensitiva: Debe ser conocida por las personas que la procesan y sólo por ellas

1.2 Importancia de la Seguridad de la Información

En una empresa, es trascendental tener presente que la revisión y la mejora continua del sistema son muy importantes para garantizar la disponibilidad, integridad y confidencialidad de la información.

La información es el activo más importante para todas las organizaciones y sin ella la empresa dejaría de funcionar y la seguridad, una cualidad intangible que permite protegerla.

La falta de seguridad puede deberse a dos factores:

- Desconocimiento de las posibles amenazas que pueden desencadenar un incidente en la entidad.

- Falta de conocimiento de las medidas de seguridad que existen para paliar las amenazas que pueden producir daños materiales o inmateriales en los activos (Seguridad Informática)

1.3 Sistema de Gestión de Seguridad de la Información

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

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Se entiende por información todo el conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

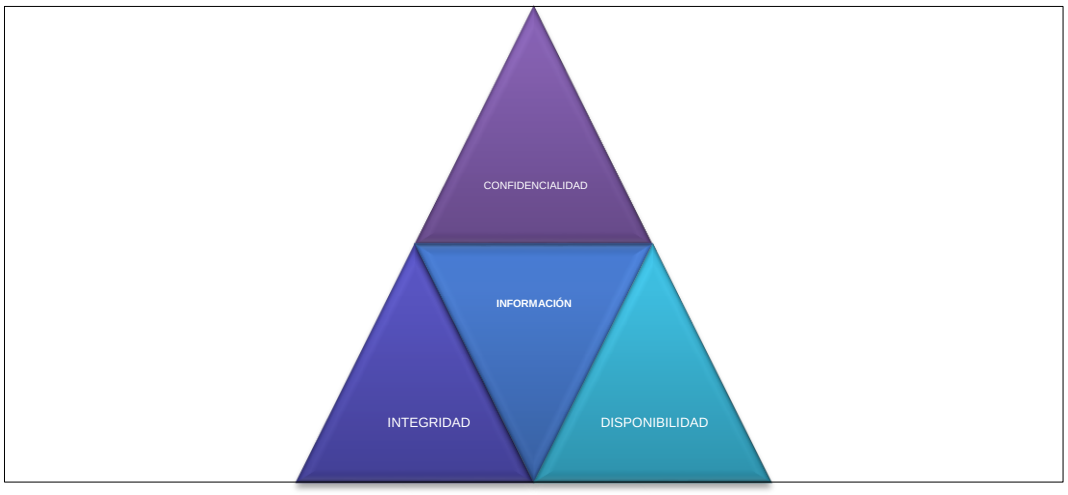


Figura 1 Triángulo de la seguridad informática

- La integridad de la información garantiza que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y estas modificaciones son registradas para posteriores controles.

- La disponibilidad de la información es la capacidad de estar siempre útil para ser procesada por personal autorizado. Lo que involucra que la misma se mantenga almacenada con el hardware y el software funcionando adecuadamente.

- La confidencialidad de la información es la necesidad de que la misma sea conocida únicamente por personal autorizado.

1.3.1 Implementación de un Sistema de Gestión de la Seguridad de la Información

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.

En la siguiente figura se muestra el ciclo de Deming aplicado al Sistema de Gestión de Seguridad de la información:

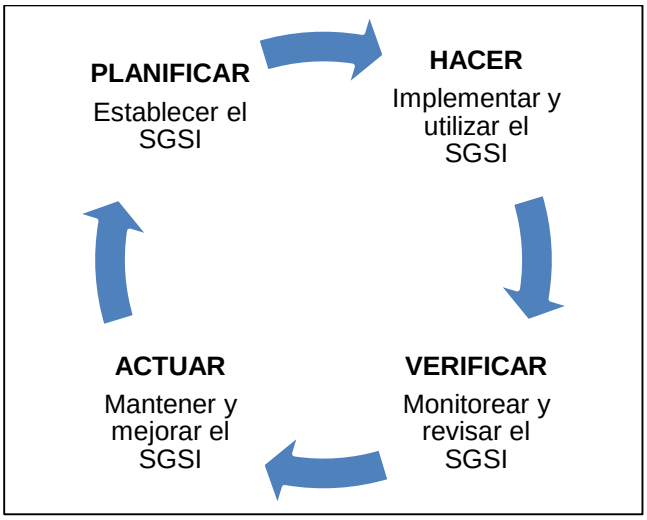


Figura 2 Ciclo de vida del SGSI

A continuación se revisarán las actividades a realizar dentro de cada etapa del ciclo de vida del SGSI:

PLANIFICAR

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.

- Definir una política de seguridad que incluya el marco general y los objetivos de seguridad de la información de la organización; considerando los requerimientos legales o contractuales relativos a la seguridad de la información; estén enfocados con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI; estableciendo los criterios con los que se va a evaluar el riesgo y esté aprobada por la dirección.

- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles

- Identificar los riesgos, lo que incluye identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios; identificar las amenazas que afectan a los activos; para lo cual a su vez se requiere identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas e identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- Analizar y evaluar los riesgos, al evaluar el impacto en el negocio de al producirse una falla de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información; y valorar de manera realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados; estimar los niveles de riesgo y determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

- Identificar y considerar las opciones de tratamiento de los riesgos para aplicar controles adecuados; aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos; evitar el riesgo, o transferir el riesgo a terceros.

- Definir una declaración de aplicabilidad que incluya los objetivos de control y controles seleccionados y los motivos para su elección; los objetivos de control y controles que actualmente ya están implantados; los objetivos de control y controles excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.
  (Alexander, 2006)

HACER

- Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.

- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.

- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

- Procurar programas de formación y concienciación en relación a la seguridad de la información 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.
  (Alexander, 2006)

VERIFICAR

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para detectar a tiempo los errores en los resultados generados por el procesamiento de la información; identificar brechas e incidentes de seguridad; ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación

a lo previsto; detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores; y determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- Revisar periódicamente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia y observaciones de todas las partes involucradas.

- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.

- Revisar regularmente en plazo de tiempo estipulado las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la empresa, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior como requerimientos legales, obligaciones contractuales, etc.

- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.

- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.

- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.
  (Alexander, 2006)

ACTUAR

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar las acciones preventivas y correctivas adecuadas y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.
  (Alexander, 2006)

1.4 De quién se debe proteger

Son diversas las amenazas que pueden atentar contra la seguridad de la información, las cuales se pueden clasificar en amenazas lógicas y físicas y en factores ambientales y humanos, los cuales se detallarán en el presente capítulo.

Lo que pretende el sistema de seguridad de la información es proteger de una amplia gama de amenazas, para asegurar la continuidad del negocio. Estas amenazas tienen como objetivo realizar acciones como: fraude informático, espionaje, sabotaje, vandalismo, etc., siendo las vulnerabilidades cada vez más comunes y sofisticadas, como virus informáticos, ataques de intrusión, hackers, accesos no deseados o denegación de servicios, entre otras. (García, La Seguridad de la Información. Nueva ventaja competitiva en la empresa, 2004)

1.5 Qué se debe proteger

Se debe tener claro qué activos de la empresa se desea proteger, de qué se los va a proteger y la manera de cómo se pretende realizarlo.

Los elementos que han de ser protegidos son:

- Datos: Es lo más valioso a proteger. Es la información lógica de la organización, resultado de la labor realizada.

- Software (Sw.): Es el conjunto de programas, instrucciones y reglas informáticas que hacen funcionar el hardware.

- Hardware (Hw.): Es el conjunto de componentes que integran la parte física de una computadora.

- Infraestructura: La infraestructura tecnológica agrupa y organiza el conjunto de elementos tecnológicos que integran un proyecto, soportan las operaciones de una organización o sustentan una operación. Una infraestructura define el éxito de una empresa en la medida de que su robustez, calidad y sostenibilidad se traduce en incremento de la inversión en TI. Por este motivo es crucial conocer

todos sus componentes o elementos a nivel de software y de hardware. Una infraestructura sólida permite a un software operar de manera eficiente y eficaz durante el tiempo previsto con niveles altos de servicios y prestaciones. El software es el activo más nuevo de las organizaciones cuyo valor se obtiene por la importancia de su uso, eficiencia, procesado de datos y capacidad de facilitar operaciones.

- Know How: Es el conjunto de bienes inmateriales mediante el cual, la empresa obtiene exclusividad para utilizar y mantener la propiedad industrial sobre un proceso u objeto. Por lo tanto se convierte en un elemento valioso ya que se usa como una gran ventaja competitiva al hacer el producto único.

Se debe contar con un inventario de todos los activos importantes de la compañía que incluya toda la información necesaria acerca del activo como: el tipo de activo, lugar de ubicación, valor comercial y todo dato relevante para la empresa.

Además, cada activo debe tener un propietario que se haga responsable de su cuidado y mantenimiento.

1.6 Tipos de desastres

Es importante proteger los activos de posibles daños físicos que pudieran afectar a la entidad.

Las catástrofes se pueden dividir en dos grandes grupos:

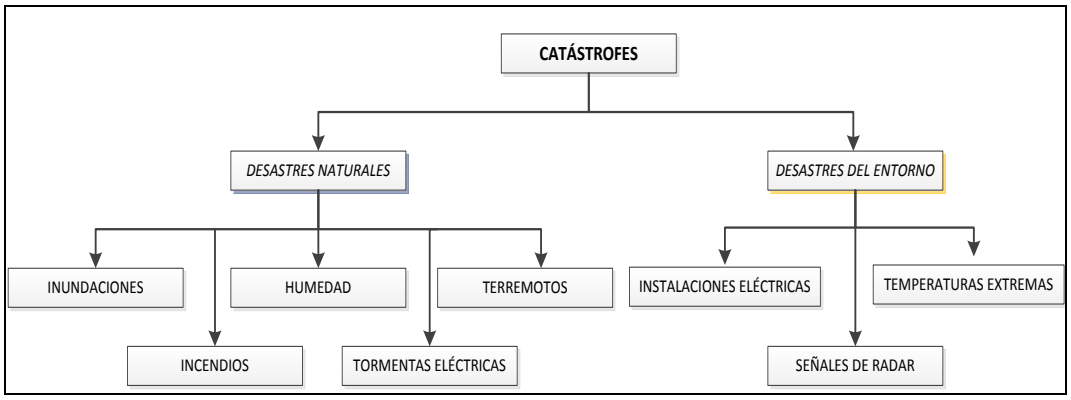


Figura 3 Clasificación de las catástrofes (Huerta, 2000)

1.6.1 Desastres Naturales

La posibilidad de controlar la naturaleza es casi nula, aunque muchas catástrofes naturales son predecibles y algunas se pueden evitar en mayor o menor medida.

- Inundaciones: Pueden ocurrir por causas naturales o provocadas por ejemplo para sofocar un incendio. Se pueden prevenir, instalando mecanismos de detección que apaguen los sistemas si se detecta agua y corten la corriente. Además, es necesario considerar posibles de sistemas de evacuación de agua en el caso de que se produzca la inundación.

- Humedad: En entornos normales, niveles aceptables de humedad son necesarios para evitar la electricidad estática pero demasiada humedad puede estropear los recursos de la empresa. Para controlar la humedad basta con instalar alarmas que monitoreen los niveles anormales de humedad.

- Tormentas eléctricas: Acompañan fuertes tormentas, tempestades, etc. y pueden estropear los activos de la organización. Para evitar daños se debe considerar colocar pararrayos y demás mecanismos

necesarios en el caso que se produjese cualquier condición climatológica adversa.

- Terremotos: Fenómenos sísmicos que según su intensidad pueden llegar a destruir edificios e inclusive vidas humanas. Para prevenirlos, se deben construir edificios antisísmicos, fijar los equipos y alejar los objetos de las ventanas.

- Incendios: El origen del fuego puede darse por causas como: un cortocircuito en las instalaciones eléctricas o el uso inadecuado de materiales combustibles. Para combatirlos de manera efectiva, conviene instalar detectores de incendios y de humo, extintores y realizar revisiones periódicas de éstos.

1.6.2 Desastres de Entorno

- Señales de Radar: Las señales de radar pueden afectar al procesamiento electrónico de la información si alcanza, al menos, los 5 voltios/metro. (Huerta, 2000)

- Instalaciones eléctricas: Las subidas y/o caídas de tensión entorpecen el funcionamiento de los componentes electrónicos, se podrían producir inclusive cortes de electricidad. Además, está presente el riesgo de corte de cables, deterioro o interferencias, por lo que más favorable es acoplar los cables a la estructura del edificio, instalar tomas de tierra, colocar filtros si hay presencia de ruido eléctrico y colocar estabilizadores de tensión.

- Temperaturas extremas: Ya sea el exceso de frío o calor, esta condición daña gravemente los equipos. Se debe tener en cuenta la sugerencia del fabricante y mantener a los equipos en el rango de temperatura recomendado. Para lo cual, se debe instalar sistemas

de aire acondicionado y calefacción, y asegurar la correcta ubicación y ventilación de los equipos

1.7 Amenazas a la seguridad

Existen innumerables amenazas a la seguridad las cuales se puede clasificar en amenazas humanas y ataques a equipos y redes.

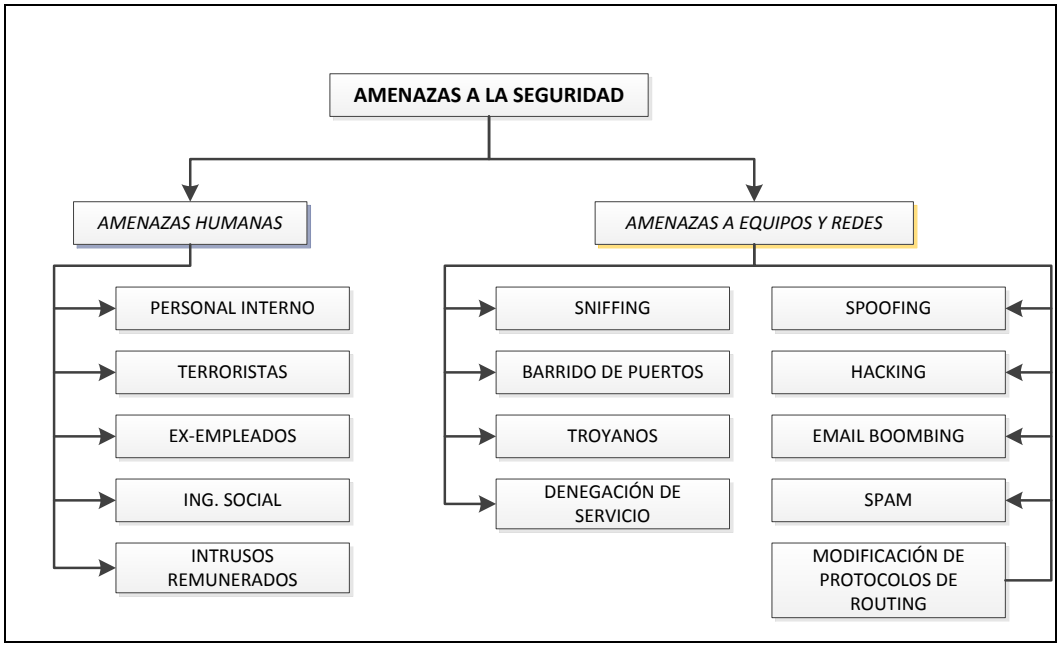


Figura 4 Clasificación de amenazas a la seguridad
(Ardita, 2011)

1.7.1 Amenazas Humanas

Entre las principales amenazas humanas se tiene:

- Personal Interno: Personal del propio sistema informático, muy pocas veces es considerado como posible atacante, ya que estas personas cuentan con la confianza de los líderes del área, en

mayor parte los ataques producidos por este grupo son causa de accidentes, desconocimiento o inexistencia de normas básicas de seguridad, sin embargo también puede ser intencional.

- Ex empleados: Este grupo puede estar interesado en violar la seguridad de la empresa, sobre todo aquellos que han sido despedidos y no han quedado conformes; o bien aquellos que han renunciado para pasar a trabajar a una empresa de la competencia.

- Terroristas: Se considera terrorista a cualquier persona que ataca el sistema para causar daño de cualquier índole en él. Por ejemplo ataques de modificación de datos de clientes, páginas web y bases de datos.

- Intrusos Remunerados: Este es el grupo de atacantes más peligroso. Puede incluir piratas informáticos con grandes conocimientos y experiencia, pagados por una tercera parte para robar secretos (códigos fuente de programas, base de datos de clientes, información confidencial de usuarios finales, etc.) o simplemente dañar la imagen de la entidad atacada.

- Ingeniería Social: Con éste término se define el conjunto de técnicas psicológicas y habilidades sociales, utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros, valiéndose de herramientas o inclusive a través de las relaciones interpersonales y la investigación de repositorios de información pública. Son ataques que aprovechan la buena voluntad de los usuarios de los sistemas atacados, ya que los atacantes influyen en las personas para que ellos hagan cosas que en circunstancias normales, no harían.

No existe una limitación en cuanto al tipo de información y tampoco en la utilización posterior de la información obtenida.

1.7.2 Amenazas y ataques a Equipos y Redes

Existen innumerables tipos de amenazas y ataques a equipos y redes, a continuación se señala las más relevantes:

- Sniffing: Consiste en capturar cualquier paquete que circule por la red. Se puede realizar sniffing por software o por hardware. En este último caso, se conecta un dispositivo a un cable de red para capturar los paquetes que viajen a través del cable (esta práctica recibe el nombre de wiretapping).

  Generalmente el sniffing se realiza por software. Un programa captura la información de la red almacenándola, en un archivo al que accede el atacante. Las tramas que circulan por delante de la máquina en la que se encuentra instalado el sniffer son captadas aunque la información no vaya dirigida a dicha máquina. Un sniffer se queda “escuchando” para captar contraseñas, números de tarjeta de crédito, direcciones de correo electrónico o cualquier otra información ya que, en ocasiones, estos datos no viajan cifrados.

- Barrido de Puertos: El escaneo de puertos es una técnica utilizada por hackers y administradores para auditar máquinas y redes con el fin de conocer cuales puertos están abiertos o cerrados, los servicios que son ofrecidos, chequear la existencia de firewall, así como verificaciones sobre el funcionamiento del mismo e información adicional. Existen diversas técnicas de escaneo de máquinas y redes, entre los más comunes escaneos a los puertos TCP y UDP.

- Troyanos: Un caballo de troya o troyano es un programa que bajo una apariencia inofensiva y útil para el usuario se inserta en un computador, y permite que usuarios externos accedan a la información contenida o controlen de forma remota el equipo. Los troyanos son creados para obtener información privilegiada de la máquina anfitriona. No necesariamente provocan daños en la computadora infectada y, a diferencia de los virus y los gusanos, los troyanos no se reproducen.

  Generalmente los caballos de Troya son utilizados para espiar, instalando en la máquina anfitriona un software de acceso remoto para observar las actividades que realiza el usuario del computador. Estos troyanos reciben el nombre de programa espía o spyware. Si lo que se pretende es capturar secuencias insertadas en el teclado para conseguir contraseñas reciben el nombre de keylogger. También existen troyanos que pueden abrir puertas traseras al computador para que un tercero realice las acciones maliciosas que persiga.

Los troyanos se componen de dos programas: uno que envía las acciones que deben realizarse en la computadora anfitriona llamado cliente, y otro programa que recibe las acciones del cliente y las realice desde el computador infectado denominado servidor.

Los troyanos actuales constituyen una gran amenaza para los usuarios debido a que pasan bastante desapercibidos. Esto se debe a que el programa servidor no consume apenas recursos. Cuando se arranca el equipo, el caballo de Troya se ejecuta automáticamente y reside en memoria.

- Denegación de Servicio: Es un tipo de ataque cuyo fundamental objetivo es negar el acceso del atacado a un recurso determinado o a sus propios recursos. Algunos ejemplos de este tipo de ataque son:

  - Tentativas de “floodear” (inundar) una red, evitando de esta manera el tráfico legítimo de datos en la misma;
  - Tentativas de interrumpir las conexiones entre dos máquinas evitando, de esta manera, el acceso a un servicio;
  - Tentativas de evitar que una determinada persona tenga acceso a un servicio.

- Spoofing: Suplanta la identidad de una máquina o usuario legítimo para realizar acciones sobre un sistema. Por ejemplo, el intruso puede conseguir el nombre y contraseña del usuario autorizado y enviar falsos correos electrónicos en nombre de la víctima.

  Cuando el ataque se realiza desde una dirección IP falsa se conoce como IP spoofing. El atacante consigue que el receptor de los mensajes crea que recibe tramas del emisor legítimo. El intruso simula la identidad de otra máquina para conseguir acceso a recursos de un sistema con el nombre o la dirección IP del equipo suplantado. Un ataque IP spoofing puede utilizarse para producir ataques de denegación de servicio. Si se suplanta la dirección IP del emisor y se envían mensajes a distintas máquinas, éstas enviarán sus respuestas a la dirección IP de la víctima, provocando una denegación de servicio.

- Hacking: Significa encontrar las debilidades de un sistema y explotarlo. Un hacker es una persona que descubre las debilidades en un equipo y lo explota. Los hackers pueden estar

motivados por una multitud de razones, tales como beneficios, acciones de protesta, o un desafío. La subcultura que se ha desarrollado en torno a los piratas informáticos se refiere a menudo como una comunidad informática clandestina, pero que ahora es una comunidad abierta.

- Modificación de protocolos de routing: Cuando un intruso ha conseguido ingresar en los equipos activos de la red, puede modificar los protocolos de ruteo de manera que lo beneficie, y aunque es una técnica poco habitual y compleja puede ser utilizada. Para combatirla se puede utilizar protocolos de ruteo con encriptación

- Email bombing y spamming: El email bombing consiste en enviar repetidas veces un mensaje idéntico a una misma dirección, saturando el mailbox del destinatario. El spamming es una variante del e-mail bombing, se refiere a enviar un email publicitario enviado a gran cantidad de usuarios sin solicitarlo.

1.8 Seguridad física

1.8.1 Seguridad física relacionada con el Entorno

- Perímetro físico de seguridad y controles de acceso: La protección física se lleva a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de la empresa y de las instalaciones de procesamiento de información.

  La empresa utiliza perímetros de seguridad, es decir utiliza medios como paredes, puertas de acceso controlado o cualquier barrera, para proteger las áreas que contienen instalaciones de

procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información.

- Control de accesos públicos: Se debe asegurar que solo personal autorizado sea permitido para el acceso, para lo cual se pueden implementar controles como:

  - Control de Personas: este servicio es el encargado de colocar a personal de seguridad en lugares estratégicos para cumplir sus objetivos y controlar el acceso del personal. A toda persona ajena a la empresa debe solicitarse llenar sus datos personales, motivo de la visita, hora de ingreso y salida.
  - Uso de credenciales: este es un punto de control eficaz del ingreso y salida del personal a las distintas áreas y permite el acceso a las secciones de la empresa que realmente necesita el empleado para cumplir sus funciones.

- Protección contra amenazas externas y ambientales: La protección física también debe contemplar la posibilidad de daños por incendios, inundación, explosión, disturbio y otras formas de desastres naturales o provocados, la elaboración de un plan de evacuación que salvaguarde en primer lugar la vida de los usuarios y en segundo lugar permita tener continuidad en el negocio es indispensable.

1.8.2 Seguridad física relacionada con equipos

La seguridad de los equipos garantiza la continuidad del negocio mediante la protección de los activos de la organización, por lo cual se debe tener en cuenta:

- Instalación y protección: Los equipos deben ser protegidos para reducir el riesgo de amenazas de entorno, así como oportunidades de acceso no autorizado.

- Utilidades adicionales: Verificar que los insumos de electricidad, agua, ventilación sean apropiadas para que el equipo funcione sin inconvenientes.

- Seguridad del cableado: Se debe garantizar la protección contra intercepciones tanto el cableado eléctrico como el cableado de datos.

- Mantenimiento de equipos: La realización un mantenimiento preventivo de acuerdo a las recomendaciones, intervalos y especificaciones del fabricante, garantiza mantener o incrementar la vida útil del equipo.

- Seguridad fuera de la organización: Considerar que los equipos que deban salir de la empresa no contengan información sensitiva y de ser así, sean manipulados por personal autorizado y lleguen a su destino de una manera rápida y segura.

- Reutilización o eliminación: Todos los elementos que contengan dispositivos de almacenamiento deben ser revisados antes de la eliminación para garantizar que la información que contienen no se pierda o sea utilizada de manera incorrecta.

1.9 Seguridad lógica

Consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo." (National Institute for Standars and Technology).

Los objetivos que se plantean para la seguridad lógica son:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no corresponden.
- Asegurar que se estén utilizando los archivos indicados en el procedimiento correcto.
- Que la información transmitida sea recibida solo por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

1.9.1 Seguridad lógica en los sistemas

Es importante mantener la seguridad lógica sobre los sistemas y establecer criterios de aceptación, actualizaciones, control de nuevas versiones, y llevar a cabo pruebas adecuadas del sistema antes de su implementación.

Ampliando las consideraciones anteriores se tiene:

- Actualizaciones de software: El cambio constante obliga a mejorar el software e incrementar controles en el mismo, por lo que mantener actualizadas las versiones de software comercial y desarrollado es importante como mecanismo de defensa ante intrusos, se debe tener en consideración que el software comercial tiene licencias que se deben renovar para no caer en incumplimiento y ser un blanco de ataques.

- Protección contra código malicioso: El objetivo de este control es proteger la integridad del software y de la información, también se debe tomar en cuenta las precauciones para prevenir y detectar la introducción de software malicioso y de ser detectado tomar las medidas para combatirlo.

- Copias de seguridad: Una práctica para asegurar que la información estará disponible es crear copias de respaldo de archivos y aplicaciones importantes, la mayoría de protocolos para copias de respaldo especifican que al menos una de las copias de los datos debe conservarse en un sitio alterno. Existen varias estrategias para realizar las copias de seguridad y dependerá de las necesidades de la empresa elegir la que mejor cubra sus necesidades. Entre los más comunes tipos de respaldo se tiene:

- Respaldo Completo, realiza la copia de seguridad completa del sistema.
- Respaldo Incremental, realiza una copia de los archivos que se hayan modificado desde la última copia de seguridad.
- Respaldo Diferencial, ofrece un espejo que refleja el estado del sistema a partir de la última copia y una historia de copias diferentes.

1.9.2 Seguridad lógica en las comunicaciones

Dentro de la seguridad lógica de comunicaciones se consideran los siguientes puntos:

- Seguridad en el acceso a través de redes: Es importante dar acceso a la información y a los servicios, únicamente a los usuarios que la necesiten para sus labores diarias y a su vez limitar y controlar continuamente el uso de los sistemas y aplicaciones por parte de los usuarios, para evitar que estos eludan las medidas de seguridad o incorporar controles que restrinjan las capacidades de conexión de los usuarios.

- Identificación de equipos: Es importante tener una documentación sobre la identificación de todos los equipos que soportan la red de la empresa para facilitar la ubicación de los dispositivos y el análisis de la red.

- Cifrado: Es un mecanismo de seguridad que puede proveer confidencialidad a los datos o al flujo de tráfico, la criptografía encierra principios y métodos para la transformación matemática de los datos para esconder los contenidos de información, previniendo la alteración o uso no autorizado. El cifrado garantiza que la

información es secreta para individuos, entidades o procesos no autorizados.

1.9.3 Control de accesos

Los mecanismos para el control de acceso pueden ser usados para cuidar recursos físicos, recursos lógicos o recursos digitales. El mecanismo de control de acceso se utiliza para autenticar las capacidades de una entidad para acceder a un recurso dado y se puede llevar a cabo en el origen o en un punto intermedio. A continuación se analizará algunos métodos aplicables para el control de accesos:

- Identificación y autentificación: Se denomina identificación al momento en que el usuario se da a conocer en el aplicativo o sistema, y autentificación a la verificación que realiza el sistema obre esta identificación. Existen 4 técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas de manera individual o combinada:

    - Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso, una clave criptográfica, un número de identificación personal o PIN, etc.
    - Algo que la persona posee: por ejemplo una tarjeta magnética
    - Algo que el individuo es y lo que lo identifica unívocamente: por ejemplo las huellas digitales o la voz
    - Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura

Es conveniente que los usuarios sean identificados y autenticados solamente una vez, y puedan acceder a partir de ahí a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas

locales como en sistemas a los que deba acceder en forma remota. La seguridad informática se basa, en gran medida en la administración efectiva de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

- Roles: El acceso a la información también puede controlarse a través de la función o rol del usuario que requiere dicho acceso. Permitiendo el acceso únicamente a la información requerida para cumplir su trabajo.

- Limitación de Servicios: Este tipo de controles se refieren a las prohibiciones que dependen de parámetros propios de las aplicaciones o que sean predefinidos por el administrador del sistema.

- Ubicación y horario: El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. El control en los horarios permite limitar el acceso de los usuarios a determinadas horas del día o determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

1.10 Riesgos

Un riesgo es descrito como la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.

1.10.1 Análisis del riesgo

Para implementar un Sistema de Gestión de Seguridad de Información según la familia ISO 27000, la organización requiere determinar el alcance del estándar en la empresa, y en base a este alcance identificar todos los activos de la información. Posteriormente se realizará un análisis del riesgo para identificar qué activos están bajo riesgo y la magnitud del riesgo que los afecta. "Se deben tomar decisiones en relación a que riesgos la organización aceptará y qué controles serán implantados para mitigar el riesgo" (Alberts, 2003)

1.10.2 Proceso de evaluación de riesgos

Los riesgos se pueden evaluar de diferentes maneras, sin embargo se debe comenzar por la identificación de requerimientos de seguridad. Para identificar estos requisitos de la organización es aconsejable basarse en tres fuentes principales:

- Valoración de riesgos de la organización: donde se identifican las amenazas a los activos, se evalúa las vulnerabilidades y la probabilidad de ocurrencia.

- Requisitos legales: donde se revisan estatutos, regulaciones y contratos que debe cumplir la organización.

- Tratamiento de la información: sección donde se revisan los principios del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones.

Siendo el propósito de la evaluación del riesgo el identificar y evaluar los riesgos, se debe tomar en cuenta:

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

- Probabilidad: la probabilidad realista de que ocurra dicho fallo gracias a las amenazas y vulnerabilidades existentes, así como de los controles implantados.

Los resultados de esta evaluación ayudarán a dirigir y determinar una adecuada acción y prioridades para gestionar los riesgos de seguridad de la información y la implantación de los controles adecuados para protegerse contra dichos riesgos.

1.10.3 Opciones para el tratamiento del riesgo

Cuando los riesgos han sido identificados y evaluados, se debe considerar la acción más apropiada para tratar estos riesgos, lo que se conoce como un Plan de Tratamiento de Riesgos (PRT). El objetivo principal es describir de forma clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles aceptables, los recursos que se asignarán para realizar las actualizaciones, las responsabilidades asociadas y las prioridades en la ejecución de las actualizaciones.

Para el tratamiento del riesgo existen cuatro estrategias:

- Reducción del riesgo: en esta opción se debe implementar los controles apropiados para disminuir los riesgos a niveles de aceptación previamente identificados por la empresa, para lo cual se debe trabajar previamente en la identificación de requerimientos de seguridad, vulnerabilidades y amenazas.

- Aceptación del riesgo: si se detecta una situación en la que no se pueden encontrar controles y tampoco es viable diseñarlos o a su vez el costo para establecer el control es mayor que las consecuencias del riesgo, la decisión de aceptar el riesgo es la más acertada y se podría trabajar en opciones para disminuirlo.

- Transferencia del riesgo: se cuenta con la opción de transferir el riesgo por ejemplo delegando a terceras partes el manejo de activos procesos críticos, a una empresa que esté preparada para asumir dicha responsabilidad

- Evitar el riego: esta opción describe cualquier acción donde las actividades del negocio se modifican para evitar la ocurrencia del riesgo

1.11 Legislación informática y tecnologías en las redes de datos

1.11.1 Normativa ISO (17799-27002)

De forma general 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 implementación, vocabulario y mejora continua. (ISO 27000)

La clasificación de esta familia es muy amplia, entre las normas que se aplicarán en el desarrollo del presente proyecto se encuentran:

- 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 27000)

- 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. (ISO 27000)

- ISO 27002

  Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuando a seguridad de la información. (ISO 27000)

A continuación se realiza un análisis de la Norma ISO 27001 que será la base del presente proyecto:

BENEFICIOS DE LA NORMA ISO 27001

Entre los beneficios que se obtienen por la implementación del conjunto de normas ISO 27001 en una organización se encuentran:

- Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

- Reducción del riesgo de pérdida, robo o corrupción de la información.
- Los clientes tienen acceso a la información a través de 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 áreas a mejorar.
- Continuidad de las operaciones necesarias de negocio luego de ocurrir imprevistos de gravedad.
- Proporciona confianza y reglas claras a las personas de la organización.
- Seguridad garantizada en base a la gestión de procesos, reemplazando a la compra sistemática de productos y tecnologías.

ALCANCES DE LAS NORMAS ISO 27001

La norma ISO 27001 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 las partes interesadas incluyendo a los clientes de una empresa.

Es conveniente para varios tipos de uso empresarial, incluyendo lo siguiente:

- Formulación de exigencias y objetivos para la seguridad.
- Asegurar la gestión más rentable de los riesgos.
- Asegurar el cumplimiento legal.
- Desarrollar un proceso para la puesta en práctica la gestión de controles para asegurar el conocimiento de los objetivos de seguridad específicos de una empresa.
- Identificación y clarificación de los procesos existentes en la gestión de la seguridad de la información.
- Puede ser usado por la dirección para determinar los estados de las actividades de la gestión de la seguridad de la información.
- Como herramienta de auditores internos y externos para determinar el grado de cumplimiento con la política, directivas y normas adoptadas por una empresa.
- Para proporcionar información relevante sobre seguridad de la información a clientes.

OBJETIVO DE LA NORMA ISO 27001

Al aplicar la norma ISO 27001 se pretende:

- Aumentar el valor de un servicio "seguro". Esta filosofía supone implementar un SGSI para potenciar un servicio que ya incorpora funciones de seguridad.

- 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 agregado a los mismos.

- Reforzar los servicios y procesos internos. Se pretende fortalecer de esta manera determinados servicios y procesos internos, en los que una mejora en la seguridad pueda suponer una ventaja para la organización.

- Potenciar la gestión interna. Considerando que dentro de una organización existen múltiples sistemas de gestión centrados en diferentes aspectos como pueden ser redes de datos, aplicaciones, trato con el usuario final, la seguridad debe ser aplicada de manera afín a cada una de estas áreas ya que no hay una fórmula global.

1.11.2 Políticas y Gestión de la Seguridad

Una política de seguridad informática, establece el canal formal de actuación del personal, en relación con los recursos y servicios informáticos, importantes de la organización. No se trata de una descripción técnica de mecanismos de seguridad, ni de una expresión legal que involucre sanciones a conductas de los empleados. Es más bien una descripción de los que se desea proteger y la importancia de ello.

Para empezar es importante resaltar que una política de seguridad tiene un ciclo de vida completo mientras está vigente. Este ciclo de vida se puede dividir en cuatro fases:

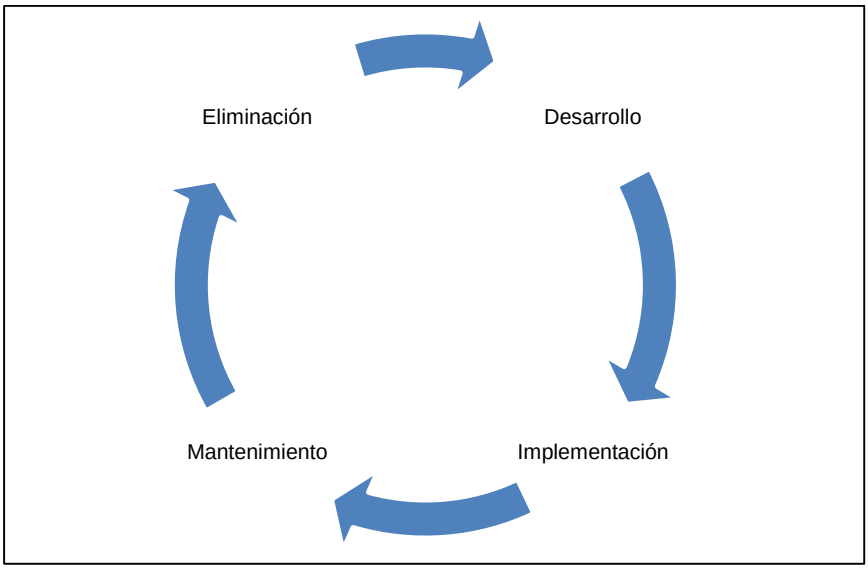


Figura 5 Ciclo de vida de una política
(ISO 27000)

- Fase de desarrollo: Durante esta fase la política es creada, revisada y aprobada.
- Fase de implementación: En esta fase la política es comunidad y acatada.
- Fase de mantenimiento: Donde los usuarios están conscientes de la importancia de la política y su cumplimiento es monitoreado y de ser necesario se actualiza.
- Fase de eliminación: Si la política a no es requerida se retira.

Si no se toma en cuenta este ciclo se corre el riesgo de desarrollar políticas incompletas, redundantes, y no van a tener apoyo de las directivas ni de los usuarios.

Para que las políticas de seguridad sean definidas adecuadamente se debe considerar entre otros, los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica. Es una invitación de la organización a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como, un motor de intercambio y desarrollo en el ámbito de sus negocios. Invitación que debe concluir en una posición.

- Objetivos de la política y descripción clara de los elementos involucrados en su definición.

- Responsabilidades por cada uno de los servicios y recursos informáticos a todos los niveles de la organización.

- Requerimientos mínimos para configuración de la seguridad de los sistemas que cobija el alcance de la política.

- Definición de violaciones y de las consecuencias del no cumplimiento de la política.

- Responsabilidades de los usuarios con respecto a la información a la que tienen acceso.

Existen varias razones por las cuales es recomendable establecer políticas en una organización, por ejemplo:

- Para cumplir regulaciones legales o técnicas.

- Como guía para el comportamiento profesional y personal.

- Permite encontrar las mejores prácticas en el trabajo.

- Permite asociar la filosofía de una organización (lo abstracto) al trabajo (lo concreto).

1.12 Empresas aseguradoras

Las empresas de seguros son aquellas cuya actividad económica consiste en producir el servicio de seguridad cubriendo determinados riesgos económicos a empresas y a personas particulares en función de sus necesidades.

Actualmente, las entidades aseguradoras muestran un especial interés en mejorar la atención al cliente y en ofrecer servicios de calidad.

En los últimos años, el incremento de la participación en las nuevas tecnologías como: Internet, Telecomunicaciones, Soluciones Móviles, etc., han hecho que la presión competitiva en el sector asegurador sea cada vez mayor. La tecnología ofrece a las entidades la oportunidad de ahorrar costos, y aumentar la rentabilidad de sus operaciones e incentivan la fidelidad de sus clientes, facilitando la puesta en marcha de nuevos canales más eficientes y rentables.

La empresa que será beneficiada mediante este proyecto, comenzó en Quito a inicios del año 1970. En el transcurso de los años, amplió sus operaciones hacia nuevos segmentos de personas ampliando los campos de seguros.

La aseguradora ha ocupado un importante sitial dentro del mercado de seguros ecuatoriano por los montos de su producción, por su solidez patrimonial y el importante volumen de activos de la empresa, y se encuentra en importantes ciudades como Quito, Guayaquil, Cuenca, Manta, Ambato, Ibarra, Riobamba y Loja.

A partir de 1997, inició una nueva era en la que se aplicaron muchos y variados conceptos de planificación estratégica, creación de valor y mejoramiento de servicio. La firma pasó por tres etapas de crecimiento. La primera fue especializar su servicio; centró su trabajo en el sector privado ecuatoriano. En la segunda fase de crecimiento, que duró cinco años, buscó la consolidación de las dos áreas privadas, local e internacional. En la actualidad representa a 11 firmas internacionales. La tercera fase de crecimiento es el negocio individual, en el cual el objetivo es liderar el mercado. (Seguros Equinoccial)

El desarrollo de tecnología va de la mano con su plan de crecimiento y la seguridad de la información es parte esencial para continuar la evolución de los servicios que ofrece.

CAPÍTULO 2

MODELO DE SEGURIDAD ACTUAL DE LA EMPRESA

2.1 Antecedentes Generales

En esta sección se describirá de manera general la estructura de la empresa y a detalle la infraestructura utilizada, lo que permitirá realizar el análisis de la situación actual de la red en cuanto a seguridad e identificar los riesgos que la comprometen.

2.1.1 Organigrama General de la Empresa

La empresa cuenta con el departamento de tecnología que abarca las siguientes áreas:

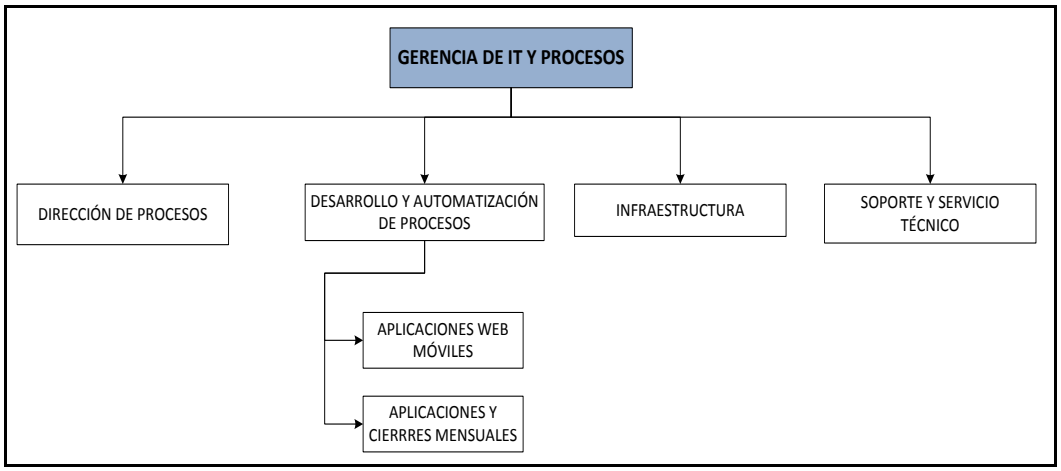


Figura 6 Gerencia de IT y procesos

El área de dirección de procesos tiene entre sus competencias el análisis de procesos, mejoramiento continuo, medición de procesos, auditoría de procesos y estadística de procesos. Cuenta con tres personas que desempeñan las actividades antes mencionadas.

El área de desarrollo y automatización de procesos se divide en dos áreas, el área de aplicaciones web móviles cuenta con cuatro programadores expertos en SLX Logix, FV y finanzas; el área de aplicaciones C/S y cierres mensuales, cuenta con cuatro programadores especialistas principalmente en SISE, BI y Datawarehouse.

El área de infraestructura está a cargo de preparación, pruebas, puesta en producción y monitoreo de redes, servidores, sistema de respaldos, telefonía IP y cuenta con dos colaboradores especializados.

El área de servicio y soporte técnico cuenta con cinco personas que realizan actividades de mesa de servicios mediante la asistencia telefónica y soporte en sitio para la solución de incidentes y atención de requerimientos solicitados por los usuarios.

2.1.2 Arquitectura de la red

La empresa aseguradora tiene un edificio principal, en el cual se encuentra su centro de operaciones y también el centro de datos. Adicionalmente cuenta con 10 agencias a nivel nacional en donde se ubican equipos que permiten la conectividad. La sucursal más importante por el número de usuarios soportados y el número de transacciones realizadas es la agencia de la ciudad de Guayaquil que tiene una pequeña sucursal asociada con la cual se comunica mediante una red LAN.

La aseguradora cuenta con dos proveedores que entregan el servicio de la red de datos mediante fibra óptica. En la siguiente tabla se puede observar el ancho de banda que tiene contratado cada agencia y el número de usuarios en cada una:

Tabla 1

Ancho de banda y número de usuarios por agencia

PROVEEDOR	AGENCIA	ANCHO DE BANDA	# USUARIOS
Proveedor 1	Edificio Principal UIO		270
	Agencia El Recreo	2 Mbps	15
	Agencia Manta	4 Mbps	12
	Sucursal Cuenca	10 Mbps	12
Proveedor 2	Sucursal Loja	2 Mbps	12
	Agencia Guayaquil	10 Mbps	80
	Edificio André	2 Mbps	45
	Agencia Ambato	2 Mbps	14
	Agencia Cámara Constitución Quito	2 Mbps	4
	Agencia Ibarra	2 Mbps	15
	CC Las Violetas	4 Mbps	17

El esquema de conexión de la matriz con las diferentes agencias a nivel nacional es el siguiente:

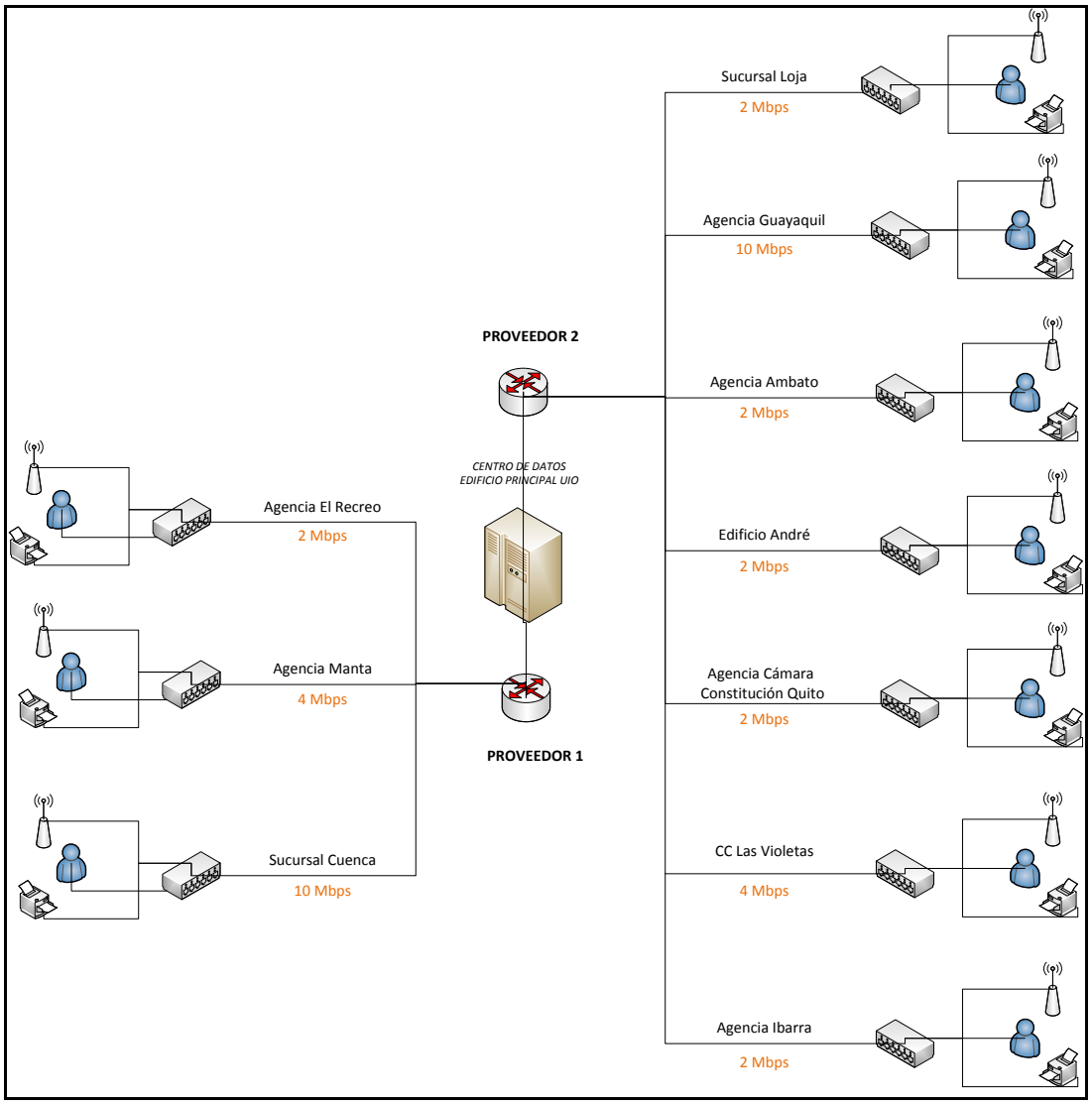


Figura 7 Conectividad entre agencias

El edificio principal cuenta con cinco pisos, por lo que la intranet está distribuida de la siguiente manera:

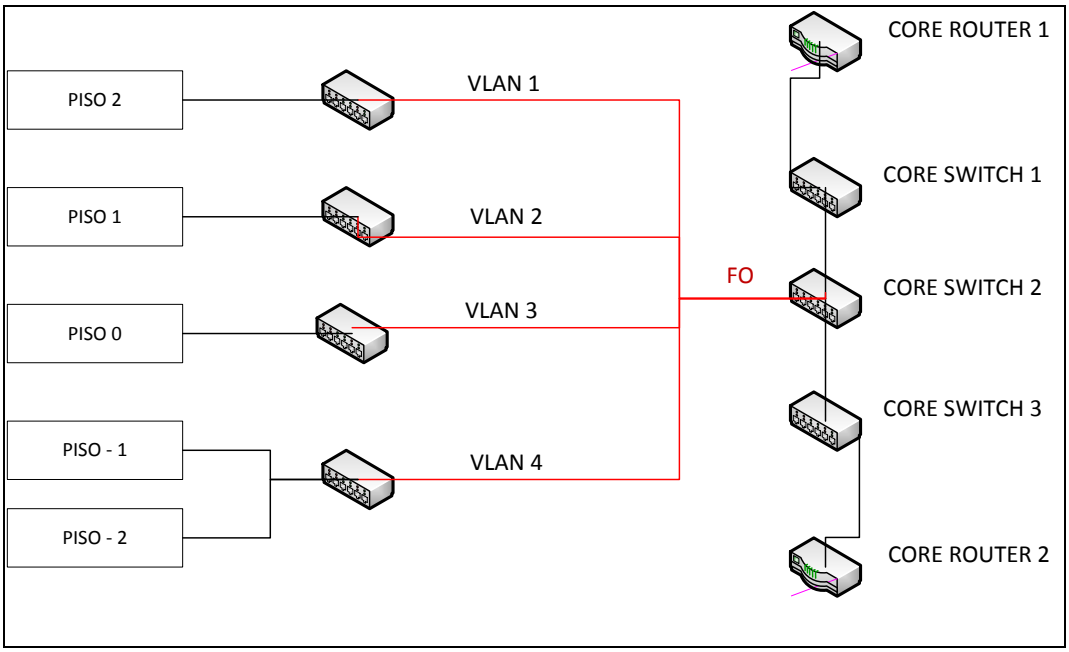


Figura 8 Distribución en el Edificio Principal

El cableado entre los equipos activos de piso a piso es de fibra óptica y la distribución hacia los usuarios se realiza mediante cableado estructurado, físicamente hablando es un cableado categoría 6a.

2.2 Análisis de la Información actual de la Empresa

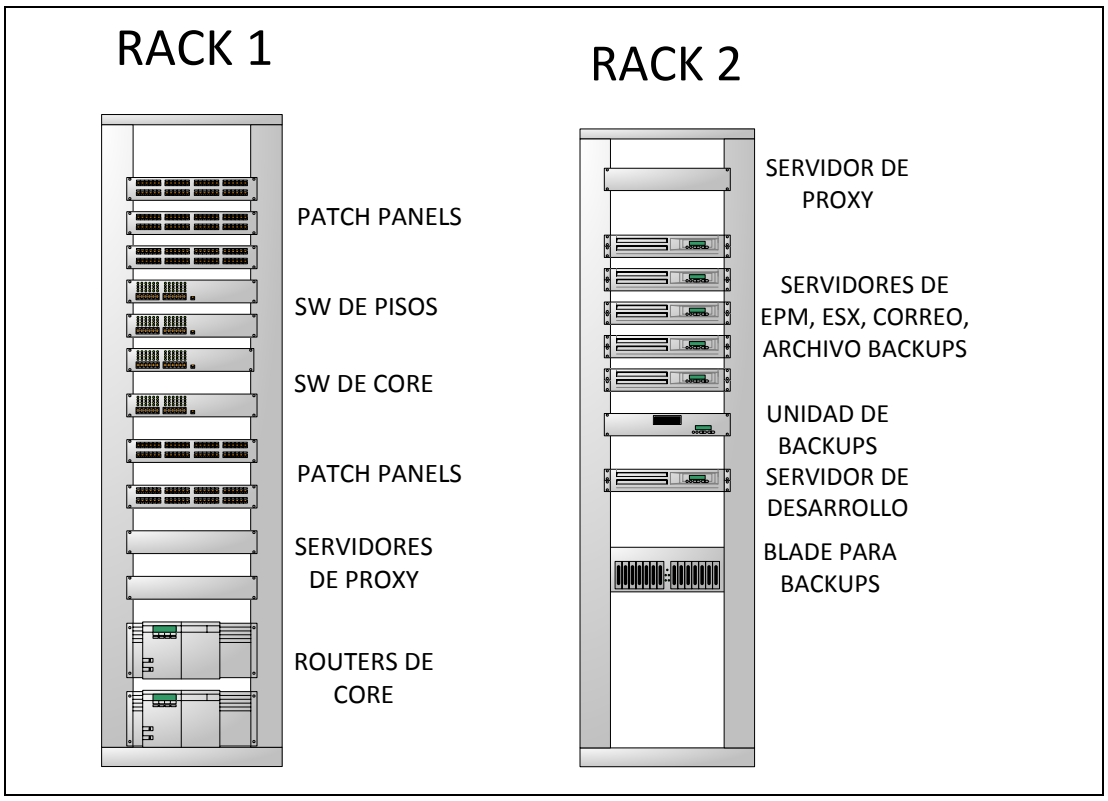
2.2.1 Seguridad de la infraestructura

El centro de datos ubicado en el Edificio Principal de la empresa, tiene una dimensión de 8 metros de largo y 4.5 metros de ancho. Está ubicado en el subsuelo.

El ingreso al centro datos está monitoreado por una cámara de seguridad, y el acceso es controlado por medio de tarjetas magnéticas, actualmente sólo dos personas encargadas del área de infraestructura tienen acceso.

Los equipos están distribuidos en cuatro armarios (racks), los cuales están monitoreados por cámaras de seguridad, que permiten ver cada cambio realizado por el personal que ingresa al centro de datos y además cuentan con un notificaciones automáticas enviadas al mail de los responsables de infraestructura cuando uno de los racks es abierto o cerrado para realizar alguna actividad.

En las siguientes figuras se puede observar la distribución de los equipos de cada rack:



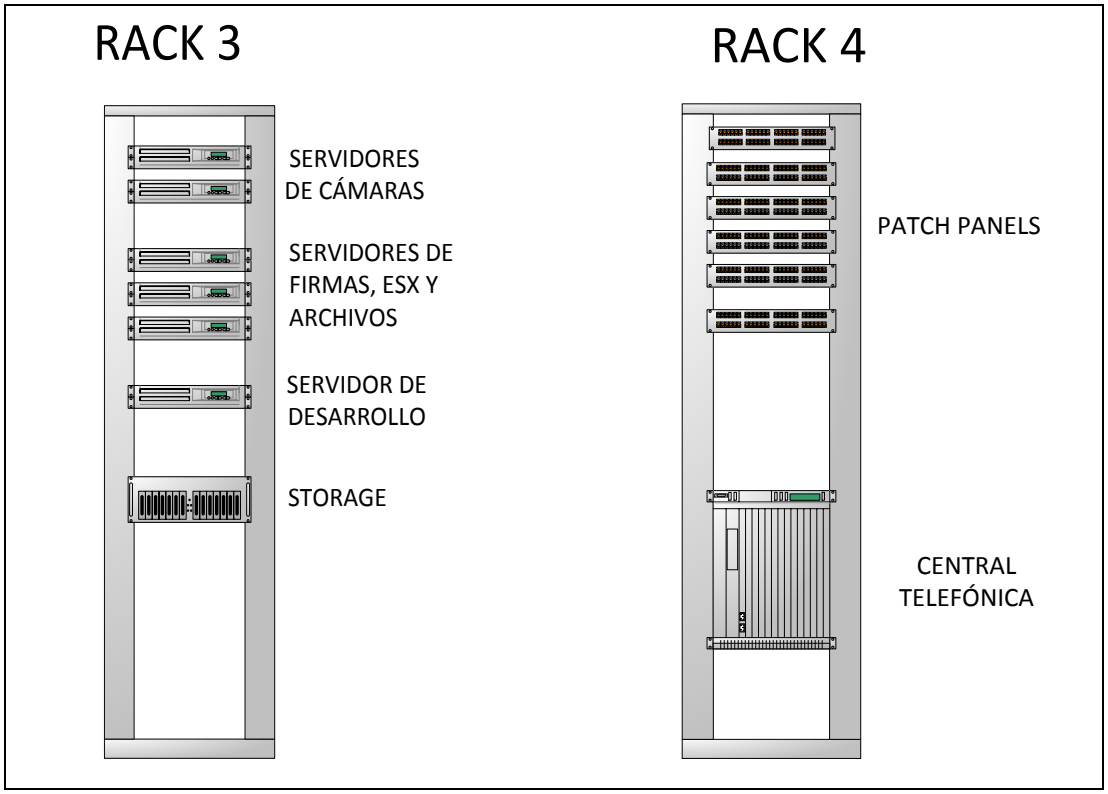


Figura 9 Distribución de equipos en los racks

La temperatura es monitoreada mediante un controlador de temperatura, el cual de ser necesario activa de manera alternada los dos aires acondicionados con los que está equipado el centro de datos. También se puede encontrar el UPS (Uninterrumptible Power System - Sistema de Energía Ininterrumpida) que permite proporcionar una fuente de energía con tensión estable y continua independientemente de las perturbaciones que puedan presentarse en la red eléctrica protegiendo de ésta manera a los equipos; y un tablero eléctrico que en caso de emergencia permitiría el apagado de todos los equipos en un corto período de tiempo.

En la siguiente figura se puede ver la distribución del centro de datos:

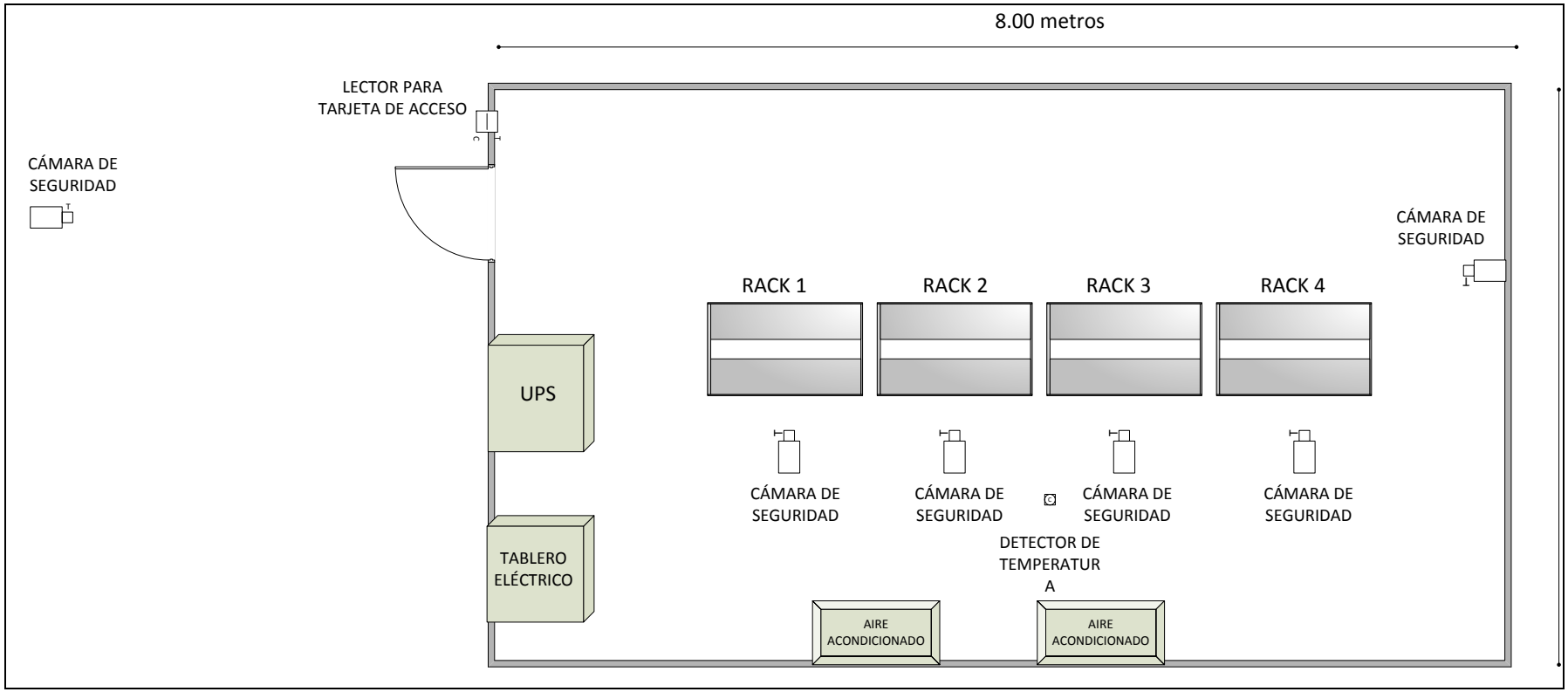


Figura 10. Distribución del centro de datos en el Edificio Principal

2.2.2 Autenticación

La autenticación es el proceso de verificación que realiza un sistema sobre la identificación de una identidad. La identificación de una persona está definida bajo los diferentes roles que desempeña en la empresa, lo que permite delimitar los accesos a la información, equipos y áreas requeridas para el desempeño de su trabajo.

La autenticación para el acceso a las áreas física se realiza mediante una tarjeta magnética y adicionalmente se cuenta con un registro escrito de las personas que han ingresado con una autorización temporal para realizar una actividad específica.

En cuanto al acceso a equipos de comunicaciones o servidores, se utiliza la autenticación de usuarios creados en los equipos tanto para realizar implementaciones o en caso extremo realizar un apagado del equipo.

Otro tipo de autenticación utilizada de manera recurrente por los usuarios es para acceder remotamente a la red de la empresa y trabajar remotamente, utilizando recursos propios de la organización; para conectarse a la red utilizan CITRIX, donde se solicita un usuario y contraseña. La contraseña a ingresar es la contraseña del dominio, propia para cada usuario y la cual es cambiada cada 30 días.

2.2.3 Administración y Control

En cuanto a la administración y control es necesario mencionar que existen controles para acceso interno, por ejemplo contraseñas que permiten el acceso al computador personal asignado a cada usuario, así como procesos de encriptación para el envío de información confidencial o restringida.

Las listas de control de acceso en equipos de comunicaciones permiten obtener un acceso diferenciado a información y servicios de acuerdo a la necesidad del usuario y bajo los roles establecidos para el cumplimiento de sus funciones.

Estos controles mencionados se complementan con los denominados controles de acceso externo como firewalls Linux donde se controla el acceso a la red privada y permitiendo que los usuarios se conecten previniendo la intromisión de virus o diversos tipos de ataques. Se tiene implementado el control de acceso a las aplicaciones mediante control de puertos

2.2.4 Operaciones y Roles

El control de acceso basado en roles es una función de seguridad para controlar el acceso de usuarios a tareas que normalmente están restringidas al no ser necesarias para cumplir determinadas funciones.

Los derechos o accesos a la información en caso de usuarios o accesos a la configuración y/o administración de equipos de red y servidores se implementan a través de privilegios y se los revisa recurrentemente en períodos semestrales.

En el área de infraestructura específicamente existen roles como de administración, monitoreo y programador entre los más utilizados.

CAPÍTULO 3

EVALUACIÓN DE LA INFORMACIÓN

En el presente capítulo se realizará una valoración y evaluación de las vulnerabilidades identificadas a partir del análisis de los factores de riesgo a los que se encuentra expuesta la red de datos de la empresa con el objetivo de plantear un modelo de seguridad que permita la reducción de los riesgos existentes.

3.1 Valoración de los niveles de seguridad existente en la infraestructura tecnológica

El análisis de riesgos y vulnerabilidades es un proceso que puede significar costoso y laborioso a la empresa. La información se recolectará mediante lo datos existentes, experiencias de los administradores de infraestructura y de ser necesario se realizaran pruebas específicas que permitan obtener el detalle requerido.

Para realizar un análisis de riesgos y vulnerabilidad se debe contar con la colaboración de algunas áreas de la empresa, desde los niveles técnicos-operativos hasta niveles gerenciales para cuantificar los riesgos adecuadamente.

El análisis de riesgo es recomendable ya que la operatividad de la empresa depende de los sistemas y redes de comunicación para cumplir su misión. Un adecuado análisis de riesgo permite la toma de decisiones por ejemplo para mejorar la infraestructura, realizar capacitaciones al personal, etc.

Se han identificado tres elementos:

- Activos: Elementos que forman parte del sistema de información.
- Amenazas: Son las posibilidades de ocurrencia de cualquier tipo de evento o acción que puede producir daño (material o inmaterial) sobre los elementos (activos, recursos) de un sistema.
- Protecciones: Elementos de defensa para prevenir que las amenazas causen daño. Las políticas de seguridad son parte de estas protecciones.

Con esos tres elementos se puede estimar:

- El impacto: efectos que los riesgos puedan ocasionarle a la empresa
- El riesgo: combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Se calcula de la siguiente manera:

$$Riesgo = Amenaza * Vulnerabilidad$$

Luego de realizar el análisis de riesgos se debe decidir qué hacer con cada uno y las posibles acciones que se pueden tomar son:

- Evitar el riesgo: Poner en práctica las acciones orientadas a prevenir su materialización.

- Reducir el riesgo: Implica tomar las medidas enfocadas a disminuir tanto la probabilidad de que ocurra (medidas de prevención), como el impacto que produzca (medidas de protección).

- Compartir o Transferir el riesgo: Reduce su efecto a través del traspaso de las pérdidas a otras organizaciones que están en posibilidades de enfrentarlos adecuadamente.

- Asumir un riesgo: Implica que el riesgo con su respectivo impacto serán tolerados por la empresa, generalmente son riesgos mínimos que existen luego de que han sido reducidos o transferidos.

3.1.1 Escala de valoración de riesgos

Para la valoración del riesgo se identificará y evaluará los activos basados en las necesidades de la empresa. La valoración se realizará a partir de los tres pilares principales en la seguridad de la información que son: confidencialidad, integridad y disponibilidad.

Los estándares de confidencialidad se calificarán de la siguiente manera:

Tabla 2

Valoración de confidencialidad

ACTIVOS DE INFORMACIÓN	CLASE	DESCRIPCIÓN
1	Pública	Información cuya divulgación no afecta a la empresa.
2	Interna	Información que circula al interior de una empresa y busca llevar un mensaje para mantener la coordinación entre distintas áreas.
3	Confidencial	Información sensible cuyo uso no autorizado afectaría a los intereses económicos y/o comerciales de la empresa.
4	Restringida	Información sensible cuyo uso no autorizado podría afectar a los intereses competitivos de la empresa.

Los estándares de integridad se considerarán de acuerdo a lo siguiente:

Tabla 3

Valoración de integridad

ACTIVOS DE INFORMACIÓN	CLASE	DESCRIPCIÓN
1	No necesaria	Usada para consultas, no hay problema en hacerla pública
2	Necesaria	Contenido clasificado, sólo ciertas áreas pueden acceder para evitar impacto al área operativa
3	Importante	De ser develada se afectaría directamente a las operaciones de la empresa

Los estándares de disponibilidad se revisarán de la siguiente manera:

Tabla 4

Valoración de disponibilidad

ACTIVOS DE INFORMACIÓN	CLASE	DESCRIPCIÓN
1	Bajo	Si la información no está disponible no existen efectos sobre las operaciones de la empresa
2	Media	Si la información no está disponible hubiera algún impacto sobre las operaciones, sin embargo existen mitigantes que pueden ser utilizados para que las operaciones y procesos no se vean afectados hasta que la información se encuentre disponible
3	Alta	Si la información no se encuentra disponible el impacto a las operaciones sería fatal

De igual manera es importante evaluar la frecuencia de ocurrencia de las amenazas y vulnerabilidades existentes; se puede realizar esta evaluación de acuerdo a la experiencia de operaciones y datos estadísticos si existieran.

A continuación se describen las categorías con las que serán analizadas:

Tabla 5
Valoración de amenazas

PROBABILIDAD DE OCURRENCIA	CATEGORÍA	DESCRIPCIÓN
1	Baja	Frecuencia de ocurrencia es una vez al año o menos
2	Media	Frecuencia de ocurrencia es una vez cada semestre o menos
3	Alta	Frecuencia de ocurrencia es una vez al mes o más

Tabla 6
Valoración de vulnerabilidades

PROBABILIDAD DE OCURRENCIA	CATEGORÍA	DESCRIPCIÓN
1	Baja	No se tiene controles o se tiene controles de seguridad muy débiles
2	Media	Controles moderados de seguridad
3	Alta	Se tienen controles de seguridad adecuados

3.2 Segmentación de la información para el análisis

3.2.1 Identificación de los Activos

Los activos tienen valor o son utilizados por la empresa y requieren protección para asegurar las operaciones del negocio y la continuidad de la empresa.

Establecida la escala de valoración, a continuación se describen los activos existentes que la empresa ha considerado necesarios para la continuidad del negocio y los cuales serán analizados para determinar los riesgos y su nivel de importancia:

Tabla 7

Activos identificados

N° ACTIVO	ACTIVO A PROTEGER
1	Servidores
2	Software de aplicación y Sistemas Operativos
3	Hardware de comunicaciones y servidores
4	Empleados
5	Servicio de comunicaciones
6	Cableado estructurado
7	Documentación y registros
8	Equipos de oficina
9	Energía eléctrica

La lista de activos no sólo se enfoca a los equipos de comunicación y redes en general, sino que a su vez incluye activos que están directa e indirectamente relacionados con la red de datos y su desempeño, clasificados mediante su nivel de importancia. El nivel de importancia se lo dará por la siguiente tabla de clasificación de activos, en la cual se

agruparán de manera que permitirá el enfoque hacia los equipos de mayor importancia en la red.

Tabla 8

Clasificación de activos de acuerdo a los niveles de afectación

OPERACIÓN	AFECTACIÓN
NORMAL	BAJA
DEGRADACIÓN	MEDIA
	IMPORTANTE
PARADA	ALTA
	MUY ALTA

El nivel de importancia fue analizado por personal del área de infraestructura de la empresa siendo **1** utilizado para calificar menor importancia y **5** para calificar mayor importancia, se describe en la siguiente tabla:

Tabla 9

Calificación de los activos de acuerdo al nivel de importancia

N° ACTIVO	ACTIVO A PROTEGER	IMPORTANCIA
1	Servidores	5
2	Software de aplicación y Sistemas Operativos	4
3	Hardware de comunicaciones y servidores	1
4	Empleados	3
5	Servicio de comunicaciones	5
6	Cableado estructurado	4
7	Documentación y registros	4
8	Equipos de oficina	2
9	Energía eléctrica	5

El nivel de importancia fue dado a cada activo bajo las siguientes consideraciones:

Servidores: Afectación muy alta ya que es donde se encuentra instalada la base de datos transaccional de la empresa.

Software y programas de aplicaciones: Afectación alta ya que el software principal “SISE Y SALES LOGIX” permite registrar de manera adecuada la transaccionalidad que maneja la empresa; las aplicaciones web permiten realizar transacciones en línea a los usuarios y acceso a los corredores de seguros asociados para revisar información sobre los datos de pólizas.

Hardware de comunicaciones y servidores: Afectación baja, ya que se cuenta con un stock mínimo que permitiría solventar cualquier incidente y seguir con la operatividad, de igual manera se cuenta con contratos de soporte de mantenimiento preventivo y correctivo.

Empleados: Afectación media ya que conocen el funcionamiento interno de la empresa sin embargo debe considerarse que registro de la información se encuentra en un repositorio de red, y es responsabilidad de cada empleado que la información que genere se encuentre en el repositorio asignado para que sea respaldada y disponible.

Servicio de comunicaciones y cableado estructurado: Afectación alta ya que se tiene un servicio a nivel nacional y los servicios e información se encuentran centralizados en la matriz, todas las sucursales toman registro, realizan consultas y transacciones a la matriz, por lo que necesitan que los equipos de comunicación operen adecuadamente.

Documentación y registros: Afectación alta ya que es importante mantener documentados procesos y configuraciones dado que se maneja una gran cantidad de servicios, servidores y aplicaciones de distribución de software.

Equipos de oficina: Tiene una afectación baja porque el computador es el medio por el cual se conectan a las aplicaciones ya publicadas (no instaladas localmente en el ordenador). El registro de la información se encuentra en un repositorio de red al cual los usuarios acceden de acuerdo a su perfil.

Energía eléctrica: Afectación muy alta ya que todos los equipos dependen del suministro constante para su operación normal.

De acuerdo a los niveles de afectación y para un registro visual de afectación se tiene la siguiente tabla:

Tabla 10

Calificación de los activos de acuerdo al nivel de afectación

N° ACTIVO	ACTIVO A PROTEGER	AFECTACIÓN
1	Servidores	5
2	Software de aplicación y Sistemas Operativos	4
3	Hardware de comunicaciones y servidores	1
4	Empleados	3
5	Servicio de comunicaciones	5
6	Cableado estructurado	4
7	Documentación y registros	4
8	Equipos de oficina	2
9	Energía eléctrica	5

3.2.2 Identificación de los factores de riesgo

De acuerdo a los estándares descritos en la sección 3.1.1 Escala de valoración de riesgos, y definidos los activos a proteger, siendo **1** utilizado para calificar bajo y **3** para calificar alto, se realiza la ponderación del riesgo para cada activo en la siguiente tabla:

Tabla 11

Valoración del riesgo

N° ACTIVO	ACTIVO	ELEMENTOS DE INFORMACIÓN	VALOR
1	Servidores	Confidencialidad	3
		Integridad	3
		Disponibilidad	3
2	Software de aplicación y Sistemas Operativos	Confidencialidad	1
		Integridad	2
		Disponibilidad	2
3	Hardware de comunicaciones y servidores	Confidencialidad	3
		Integridad	3
		Disponibilidad	2
4	Empleados	Confidencialidad	2
		Integridad	1
		Disponibilidad	2
5	Servicio de comunicaciones	Confidencialidad	2
		Integridad	2
		Disponibilidad	3
6	Cableado estructurado	Confidencialidad	1
		Integridad	3
		Disponibilidad	3
7	Documentación y registros	Confidencialidad	3
		Integridad	3
		Disponibilidad	2
8	Equipos de oficina	Confidencialidad	2
		Integridad	2
		Disponibilidad	2
9	Energía eléctrica	Confidencialidad	1
		Integridad	2
		Disponibilidad	3

La valoración se otorga de acuerdo a las siguientes razones:

Servidores

Confidencialidad: Solo personal específico debe acceder a la información de servidores debido a que manejan información de clientes y cartera.

Integridad: Es necesario que la información de servidores no sea modificada ni alterada sin autorización para que no se perjudique al negocio.

Disponibilidad: Es indispensable que los servidores estén accesibles al menos 100% en horas laborables para no afectar a clientes y empleados.

Software de aplicación y Sistemas Operativos

Confidencialidad: Es un software estándar el cual no es confidencial, cada área es responsable de su manejo.

Integridad: El software debe funcionar correctamente.
Disponibilidad: El software debe estar disponible durante horas laborables.

Hardware

Confidencialidad: La información almacenada debe ser vista únicamente por el personal autorizado.

Integridad: Es necesario la integridad de la información almacenada en especial cuando es la de clientes.

Disponibilidad: Para que los empleados puedan trabajar adecuadamente necesitan acceder a la información por medio de pcs o dispositivos móviles.

Empleados

Confidencialidad: Cierta información debe ser manejada al interior de la empresa por lo cual no debe ser divulgada.

Integridad: No hay aspectos de integridad relacionados con los empleados.

Disponibilidad: Los empleados deben estar disponibles para resolver posibles problemas que se presenten.

Servicio de comunicaciones

Confidencialidad: Se debe proteger para que los datos transferidos no sean interceptados.

Integridad: Se necesita que los servicios de comunicaciones se mantengan activos y funcionen adecuadamente.

Disponibilidad: Se necesita que los servicios de comunicaciones se mantengan activos y operativos con clientes, proveedores, etc.

Cableado estructurado

Confidencialidad: El cableado estructurado no requiere confidencialidad.

Integridad: El cableado estructurado debe funcionar adecuadamente ya que es parte de la red de la empresa.

Disponibilidad: Siempre debe estar disponible ya que al no estarlo puede causar la interrupción de las actividades propias de la empresa.

Documentación y registros

Confidencialidad: Debido a que la documentación maneja información de clientes, empleados y cartera, es necesario que pueda ser vista por personal autorizado para que no sea modificada.

Integridad: Es necesario que la documentación no sea alterada, ni se produzca pérdidas de la misma debido a que son el único respaldo físico de procedimientos, contactos, clientes, etc.

Disponibilidad: Se debe acceder a la información en cualquier momento que sea requerido.

Equipos de oficina

Confidencialidad: Elementos que contengan información del negocio necesitan confidencialidad.

Integridad: Si algún equipo de oficina como impresoras presenta alguna falla, se requiere que el área operativa pueda seguir trabajando.

Disponibilidad: Si bien algún equipo es necesario, se puede continuar la operación mientras no esté disponible.

Energía eléctrica

Confidencialidad: La entrada de la energía eléctrica no requiere confidencialidad.

Integridad: La entrada de la red eléctrica no debe sufrir manipulaciones.

Disponibilidad: Para que las operaciones de la empresa sean desarrolladas es importante que esté en funcionamiento la mayor parte del tiempo la red eléctrica y se considere una opción alterna en caso de falla.

3.2.3 Identificación de las vulnerabilidades

Al identificar las vulnerabilidades en la red de datos se debe considerar que se relacionan entre sí varios aspectos entorno a la seguridad y pueden ser originadas por distintos factores, en la siguiente tabla se encuentran el detalle de las amenazas, los activos afectados y el impacto de la afectación:

Tabla 12

Vulnerabilidades

CAUSA	DESASTRES NATURALES	DE ORIGEN INDUSTRIAL	ERRORES Y FALLOS NO INTENCIONADOS	ATAQUES INTENCIONADOS
Amenaza	-Fuego -Daños por agua -Terremotos	-Corte de suministro eléctrico -Degradación en el HW -Condiciones inadecuadas de temperatura y humedad	-Errores de usuarios -Errores de administración -Errores de configuración -Fuga de información -Modificación o degradación de información -Divulgación de información -Errores de actualización -Indisponibilidad del personal -Brechas de seguridad no detectadas -Ataques de virus, troyanos, etc.	-Instalación no autorizada o cambios de software -Brechas de seguridad no detectadas -Suplantación de identidad del usuario -Abuso de privilegios de acceso -Acceso no autorizado -Negación de servicio -Robo de información -Ingeniería social -Copia no autorizada de software o información -Ataques de virus, troyanos, etc.
Activo	-Activos Físicos -Servicios de comunicación -Documentación y Registros	-Activos físicos -Servicios de comunicación -Energía -Documentación y Registro	-Activos Físicos -Servicios de comunicación -Energía -Documentación y Registros -Software	-Activos Físicos -Servicios de comunicación -Energía -Documentación y Registros -Software

CONTINÚA

Afectación	-Disponibilidad y continuidad del servicio -Integridad	-Disponibilidad, confidencialidad e integridad de la información -Continuidad del servicio -Adecuado funcionamiento y procesamiento correcto de datos	-Disponibilidad del servicio -Confidencialidad, integridad de la información -Autenticidad de los usuarios -Autenticidad del origen de datos -Continuidad del servicio -Cumplimiento de regulaciones de seguridad	-Disponibilidad del servicio -Confidencialidad, integridad de la información -Autenticidad de los usuarios -Autenticidad del origen de datos -Continuidad del servicio -Cumplimiento de regulaciones de seguridad

3.3 Evaluación de riesgos

La evaluación de riesgos se basa en la medición del impacto y la frecuencia que se determinan en función a una clasificación del riesgo según su grado de afectación y estimación de periodicidad de ocurrencia dentro de un proceso. El enfoque cualitativo utiliza la autoevaluación a través del mapeo de procesos, evaluación del control actual y determinación de puntos de mejora a realizar.

3.3.1 Determinación de la probabilidad de ocurrencia

Para determinar la probabilidad de que una vulnerabilidad potencial se presente, se debe tomar en cuenta factores como la fuente de la amenaza y la naturaleza de la vulnerabilidad

La probabilidad de ocurrencia se puede clasificar de la siguiente manera:

Tabla 13

Probabilidad de ocurrencia

CLASIFICACIÓN	PROBABILIDAD DE OCURRENCIA	DESCRIPCIÓN
5	Esperado	Indica que los eventos derivados de un riesgo tecnológico se han presentado o se pueden presentar con un comportamiento muy a menudo durante un tiempo determinado, es decir, que la incidencia de los riesgos es muy común y constante
4	Muy probable	Indica que los riesgos identificados se han presentado o se puede presentar de manera común dentro de un proceso tecnológico
3	Probable	Indica que la incidencia del riesgo se ha presentado o se puede presentar con una repetición frecuente durante un tiempo determinado
2	Poco probable	Indica que los riesgos identificados se han presentado o se pueden presentar de forma ocasional
1	Remoto	La incidencia de riesgos es inusual que se presente o incluso nunca se había presentado una situación similar

3.3.2 Determinación de Impacto

Se denomina impacto a la medida del daño sobre el activo producido a causa de la materialización de una amenaza. Para determinar el impacto se toman en cuenta diferentes factores, en los cuales las características de la información pueden ser afectadas.

El impacto causado por una acción acertada de una amenaza puede ser clasificada de la siguiente manera:

Tabla 14

Clasificación del impacto

CLASIFICACIÓN	IMPACTO	DESCRIPCIÓN
5	Crítico	Riesgos extremadamente severos que conlleva a una pérdida altamente costosa que puede llevar a pérdida de ingresos o afectar totalmente el patrimonio de la empresa
4	Alto	Fuerte pérdida por eventos derivados de un riesgo severo que puede llegar a provocar interrupción de una parte de las operaciones de la empresa
3	Moderado	Pérdida producida de una posible contingencia produciendo inconvenientes significativos en la empresa
2	Bajo	Pérdida menor derivada de riesgos que pueden llegar a provocar algún inconveniente en la empresa
1	Menor	Pérdida mínima producida por riesgos que no afectan a la productividad de la empresa o pueden producir inconvenientes menores

3.3.3 Mapa de riesgos

De acuerdo a la categorización del riesgo por su impacto y frecuencia, se pueden representar los riesgos para identificar aquellos que son inherentes a la empresa

El mapa de riesgos es uno de los medios que permiten identificar factores de riesgos y cuantificación de probabilidad de ocurrencia a través de un consenso de grupos de trabajo y evaluaciones independientes, aprovechando la estadística disponible por incidencias o de lo contrario la experiencia de los responsables de cada área de apoyo y soporte. Cada cuadrante localizado en la gráfica permite visualizar el nivel de exposición que se tiene por cada uno de los riesgos.

Tabla 15

Mapa de riesgos

			Impacto				
			Menor	Bajo	Moderado	Alto	Crítico
			1	2	3	4	5
Probabilidad de ocurrencia	Esperando	5	Medio	Medio	Alto	Extremo	Extremo
	Muy Probable	4	Moderado	Medio	Medio	Alto	Extremo
	Probable	3	Moderado	Moderado	Medio	Alto	Alto
	Poco Probable	2	Bajo	Moderado	Medio	Medio	Alto
	Remoto	1	Bajo	Bajo	Moderado	Medio	Medio

A partir de lo anteriormente indicado, la siguiente tabla muestra la evaluación de los riesgos que afectan a los activos:

Tabla 16

Identificación de riesgos

N° ACTIVO	NOMBRE DEL ACTIVO	NIVEL DE IMPORTANCIA	FACTOR DE RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	RIESGO
1	Servidores	5	Acceso no autorizado	3	5	ALTO
			Corte de energía eléctrica	1	5	MEDIO
			Destrucción de un componente	2	3	MEDIO
			Error de configuración	4	4	ALTO
			Factores ambientales	2	2	MODERADO
			Límite de vida útil (EOL)	5	4	EXTREMO
			Equipos sin mantenimiento	3	3	MEDIO
			Modificación no autorizada de datos	2	5	ALTO
			Robo	1	5	MEDIO
			Virus no detectado	1	5	MEDIO
2	Software	4	Acceso no autorizado	2	4	MEDIO
			Aplicaciones sin licencia	2	3	MEDIO
			Error de configuración	4	4	ALTO
			Error en funciones de encriptación	3	4	ALTO

CONTINÚA

			Falla del sistema	2	4	MEDIO
			Falta de compatibilidad	2	4	MEDIO
			Pérdida de información	1	4	MEDIO
			Software desactualizado	3	3	MEDIO
			Virus no detectado	2	2	MODERADO
3	Hardware de comunicaciones y servidores	1	Corte de energía	2	5	ALTO
			Destrucción o mal funcionamiento de un componente	3	4	ALTO
			Factores ambientales	3	3	MEDIO
			Límite de vida útil (EOL)	5	4	EXTREMO
			Mantenimiento inadecuado	3	4	ALTO
			Robo	1	5	MEDIO
4	Empleados	3	Administración impropia del sistema	4	3	MEDIO
			Almacenamiento de contraseñas negligente	4	4	ALTO
			Mal uso de derechos de administrador	3	5	ALTO
			Destrucción de componentes de hardware	2	3	MEDIO
			Entrada sin autorización a	4	4	ALTO

CONTINÚA

			lugares restringidos	5	4	EXTREMO
			Ingeniería social			
5	Servicio de comunicaciones	5	Ancho de banda insuficiente	3	3	MEDIO
			Complejidad en el diseño de la red	3	2	MODERADO
			Errores de configuración y operación	2	3	MEDIO
			Denegación de servicio	2	4	MEDIO
			Falta de autenticación	3	3	MEDIO
			Límite de vida útil (EOL)	5	4	EXTREMO
			Falta de mantenimiento de los equipos	2	3	MEDIO
6	Cableado Estructurado	4	Longitud de cables de red excedida	4	2	MEDIO
			Daño de cables inadvertido	2	3	MEDIO
			Interferencias	3	3	MEDIO
			Factores ambientales	4	3	MEDIO
7	Documentación y registros	4	Acceso no autorizado a datos	2	5	ALTO
			Borrado, modificación o revelación desautorizada de datos	3	5	ALTO
			Copia no autorizada de un	2	4	MEDIO

CONTINÚA

			medio de datos			
			Descripción de archivos inadecuada	4	2	MEDIO
			Documentación insuficiente	4	3	MEDIO
			Medios de datos no están disponibles cuando son necesarios	2	4	MEDIO
			Virus, gusanos y caballos de troya no detectados	1	3	MODERADO
8	Equipos de oficina	2	Corte de energía	1	3	MODERADO
			Destrucción o mal funcionamiento de un componente	2	3	MEDIO
			Factores ambientales	4	2	MEDIO
			Límite de vida útil (EOL)	5	2	MEDIO
			Mantenimiento inadecuado	2	3	MEDIO
			Robo	3	2	MODERADO
9	Energía eléctrica	5	Cortocircuitos	2	4	MEDIO
			Factores ambientales	4	3	MEDIO

Al analizar la información de la matriz de riesgos se identifica que en todos los casos el Límite de vida útil (EOL), es un factor cuya probabilidad de ocurrencia es conocida el momento mismo de la adquisición del equipo y que el impacto de no considerar un cambio a tiempo o aplicar mitigantes que extiendan la vida útil del equipo pueden causar riesgos extremos que pueden afectar de manera importante a las aplicaciones, comunicaciones, e información que se maneja en estos equipos o por medio de los mismos.

Existen cinco activos impactados por un riesgo alto:

- Los servidores, al permitir un acceso no autorizado, tener errores de configuración y permitir la modificación no autorizada de datos; comprometen la confiabilidad de la información que es procesada.

- El Software, especialmente el desarrollado localmente es susceptible a tener errores de configuración que son detectados durante la ejecución de las aplicaciones y puede causar a su vez errores en funciones de encriptación que en ocasiones atentarían contra la confidencialidad de la información.

- El hardware de comunicaciones y servidores, es susceptible a corte de energía, por lo cual es importante verificar que estén conectados a UPS y se realicen pruebas de eléctricas controladas que permitan confirmar el adecuado funcionamiento de los equipos. El hardware puede sufrir daños si no se le provee un mantenimiento adecuado; se debe considerar que algunos componentes son sensibles y es una buena práctica tener en stock los principales repuestos como memorias, ventiladores, fuentes de poder y discos de similares características.

- Los empleados son un punto sensible, ya que al almacenar de manera negligente sus contraseñas pueden permitir el acceso a información sensible que puede ser utilizada de manera incorrecta o antiética. Más importante aún resaltar que los administradores de la infraestructura deben ser capacitados constantemente para evitar el mal uso de los privilegios que les han sido concedidos para realizar su trabajo. La entrada sin autorización a lugares restringidos debe ser controlada para evitar inconvenientes.

- Los documentos y registros deben ser almacenados de manera que no permitan el acceso no autorizado a la información, el cual puede conllevar también la eliminación, modificación o revelación desautorizada de datos.

Todos los activos se encuentran amenazados por riesgos medios y los siguientes activos por un riesgo moderado:

- Servidores
- Software
- Servicio de comunicaciones
- Documentación y registros
- Equipos de oficina

Al identificar el riesgo, se podrá trabajar en un SGSI que permita disminuir el nivel de riesgo, asumirlo y/o transferirlo.

CAPÍTULO 4

DISEÑO DEL PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN EN LA RED DE DATOS

Luego de realizar el análisis de riesgo se presenta el siguiente plan de seguridad de la información en la red de datos, el cual será evaluado por la empresa la cual determinará si es aplicable en todos los ámbitos y decidirá la mejor manera de implementarlo en el tiempo que considere necesario.

4.1 Requerimientos de seguridad presentados por la empresa

Los requerimientos de seguridad de la información se enfocaron en base a confidencialidad, disponibilidad e integridad:

- La información no debe ser vista por personal no autorizado.
- La información puede ser modificada por personal autorizado únicamente.
- La información debe estar disponible en cualquier momento.

4.1.1 Requerimientos de Software

Si se trabaja con un software comercial la confidencialidad no aplica, para el software propietario existe el requerimiento de confidencialidad.

- Las aplicaciones no deberían ser utilizadas por personal no autorizado.
- El software puede ser modificado únicamente por personal autorizado.
- El software de aplicaciones debe estar disponible durante la jornada laboral al menos.

4.1.2 Requerimientos de activos físicos

Para los activos físicos se debe enfocar los requerimientos de hardware, no en la información que se procesa, transmite o almacena.

- Los cambios en el hardware deben ser realizados únicamente por personal autorizado.
- El hardware debe ser accesible por personal autorizado.

4.1.3 Requerimientos de Servicios

Los servicios agrupan información, software y activos físicos, se deben especificar los requerimientos en base a los aspectos más importantes.

- Los servicios deben estar completos y consistentes.
- Los servicios deberían estar disponibles cuando se requiera.

4.2 Diseño del plan estratégico del Sistema de Gestión de Seguridad de Información (SGSI)

4.2.1 Política de Seguridad de la Información

Objetivo:

- Proteger los recursos de información de la empresa y los bienes tecnológicos utilizados para su procesamiento, ante las amenazas para asegurar que la información sea integra, confiable y se mantenga disponible.

Alcance:

- La política aplica en toda la empresa, a sus recursos y procesos, ya sean internos o externos y estén vinculados a la entidad a través de contratos con terceros.

- La finalidad es proporcionar instrucciones específicas de cómo mantener más seguros los activos físicos de la empresa. Como puntos focales asegurar la protección de equipos computacionales y sistemas de comunicaciones que son parte importante del manejo de la información.

4.2.2 Gestión de los activos de red

Objetivo:

- Garantizar que los activos de comunicaciones reciban un nivel de protección apropiado, y sean clasificados adecuadamente para señalar su sensibilidad y criticidad.

Responsabilidades sobre los activos:

- Los propietarios de la información serán los responsables de clasificarla de acuerdo a su criticidad, de documentar y mantener actualizada la clasificación efectuada.

- El jefe de infraestructura es el encargado de asegurar que la utilización de los recursos cumplan con los requisitos establecidos según la criticidad de la información.

- Se identificarán los activos asociados a cada sistema de información, sus propietarios y se completará un inventario el cual se debe revisar al menos una vez cada semestre (6 meses) y actualizar cada vez que se presente un cambio. El *Anexo A. Formato Inventario Activos Críticos* muestra el formato donde se llevará el registro de los activos.

4.2.3 Seguridad de los recursos humanos

Objetivos:

- Reducir los riesgos de error humano, el uso inadecuado de recursos e instalaciones y manejo no autorizado de la información.

- Indicar las responsabilidades en la etapa de contratación del personal y verificar su cumplimiento durante el desempeño como empleado de la empresa.

Responsabilidades:

- Garantizar que los usuarios estén al tanto de las amenazas que puedan presentarse en cuanto a seguridad de la información y se encuentren capacitados para cumplir la Política de Seguridad de la

empresa durante el desarrollo de sus tareas diarias. En el Anexo B.

- Boletines Informativos se describen consejos para que los usuarios se familiaricen con situaciones de la vida diaria.

- Establecer compromisos de confidencialidad con todo el personal, usuarios externos y proveedores ya sea que se encuentren dentro o fuera de las instalaciones.

- Determinar las herramientas y/o mecanismos para promover la comunicación de debilidades o amenazas existentes en materia de seguridad así como de incidentes ocurridos, con el objetivo de minimizar sus efectos y dar a conocer lecciones aprendidas.

Se elaboró un plan de concientización a los usuarios, el cual incluye charlas informativas y envío de boletines. El cronograma se encuentra detallado en el *Anexo C. Cronograma de capacitación en seguridad informática para usuarios.*

4.2.4 Seguridad Física y del entorno

Objetivos:

- Prevenir accesos no autorizados, daños en las instalaciones y acceso información de la empresa.

- Protección a los equipos que permiten el procesamiento de la información crítica de la empresa ubicándolo en áreas protegidas con controles de acceso y medidas de seguridad apropiados.

- Controlar los factores ambientales que podrían afectar el adecuado funcionamiento de los equipos que contienen la información de la empresa.

Para la empresa se realizaron y documentaron los siguientes puntos:

- Identificación del Edificio y Área. El centro de datos es donde se ubican los equipos que necesitan protección dentro de la sede principal. En las agencias y sucursales, se identificó que los equipos se encuentran expuestos, ya que no tienen una barrera que los separe del personal administrativo que labora en las instalaciones.

- Principales elementos a proteger. El levantamiento de información de activos críticos de la empresa están documentados en el *Anexo D. Inventario de equipos y aplicaciones críticas.*

- Medidas de protección física. En el *Anexo E. Controles de Acceso Físico*, se documentan procedimientos de control que permitirán resguardar mediante controles físicos las instalaciones y áreas sensitivas aplicables a la empresa de seguros.

4.2.5 Gestión de comunicaciones y operaciones

Objetivos:

- Garantizar el correcto funcionamiento de las instalaciones de procesamiento de información y comunicaciones.

- Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas.

Responsabilidades:

- El administrador de la red en colaboración con el encargado de la parte legal, debe revisar los contratos y acuerdos con terceros con el fin de garantizar la incorporación de consideraciones relativas a la seguridad de la información que involucra la parte de productos o servicios prestados.

- Establecer controles que impidan el acceso no autorizado a los sistemas de información.

La empresa tiene parcialmente documentados los procedimientos operativos, por lo que es necesario concluir con el levantamiento de información y realizar la documentación faltante. Se elaboró un cronograma con el detalle de las actividades por completar que se pueden encontrar en el *Anexo F. Cronograma Procedimientos Operativos*.

4.2.6 Política de control de acceso

Objetivos:

- Impedir acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

- Implementar o mejorar la seguridad en los accesos de usuarios por medio de técnicas de autenticación.

- Controlar de manera adecuada la seguridad de conexiones remotas a la empresa.

- Mantener una bitácora de eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

Alcance:

- Se definirá una política de control de acceso para los usuarios internos y externos que tienen permisos para acceder a los sistemas de información, red y base de datos. De igual manera aplica al personal técnico que define, instala, administra y mantiene permisos de accesos a las conexiones de red y a quienes administran su seguridad.

Para mayor información revisar el *Anexo E. Controles de acceso físico*

4.2.7 Adquisición, desarrollo y mantenimiento de sistemas de información.

Objetivos:

- Definir y documentar los procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y la infraestructura en la cual se apoyan.
- Determinar los métodos de protección de la información crítica.

Alcance:

- Los controles aplican a los sistemas informáticos y sistemas operativos que operan en la empresa.

Se considerará:

- Revisión técnica de los cambios en el sistema operativo.

- Restricción del cambio de paquetes de software suministrados por proveedores sin previa autorización del responsable del área de infraestructura.

Las áreas de desarrollo y automatización de Procesos e Infraestructura trabajarán en conjunto para realizar el levantamiento de información y documentación de los procedimientos, restricciones y consideraciones que deben tener los sistemas informáticos que operan en la empresa. Posterior a lo cual se realizarán actualizaciones anuales de los manuales y procedimientos y se tendrán almacenados tanto de manera impresa en el archivo correspondiente como de manera digital, para que se encuentren accesibles y puedan ser utilizados.

4.2.8 Gestión de incidentes de seguridad de la información

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

- Al presentarse un incidente es importante tener un procedimiento a seguir para disminuir los errores que puedan cometerse, reducir el impacto y evitar que un nuevo ataque similar ocurra.

- Luego de cada incidente es necesario actualizar el procedimiento para mejorar la seguridad.

Administración de incidentes y mejoras de la seguridad de la información

- El mantener actualizada la información permitirá poner en práctica las lecciones aprendidas si el incidente se volviera a presentar.

- Un análisis de resultados posterior a los incidentes puede ayudar a concientizar al personal y advertirlo para reducir las vulnerabilidades que hicieron que se produzca.

La empresa es propietaria del software Sysaid para el registro de llamadas e incidentes. Se incentivará al registro de las soluciones conocidas por parte de cada técnico de soporte.

4.2.9 Gestión de continuidad del negocio

Objetivos:

- Analizar las consecuencias de la interrupción del servicio y tomar las medidas necesarias para la prevención de este hecho.
- Incrementar la efectividad de las operaciones de contingencia de la empresa mediante la detección del daño, restauración de los procesos críticos, y restauración normal de las operaciones.

Alcance:

- Aplica a los procesos críticos de la empresa y por consiguiente a los sistemas involucrados en la operación.

La empresa no tiene un plan de contingencias por lo que se detalla cómo elaborar un plan de continuidad del negocio en el *Anexo G. Lineamientos base para la elaboración de un Plan de Contingencias*. (Achiary, 2005)

4.2.10 Cumplimiento

Objetivos:

- Cumplir con las disposiciones legales a fin de evitar sanciones administrativas a la empresa y/o empleados.

- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la empresa.

Alcance:

- Aplica a todo el personal de la empresa.

4.3 Políticas de seguridad

Tomando en cuenta las necesidades de seguridad analizadas en la sección 3.3 de Evaluación de riesgos, y los requerimientos de seguridad presentados por la empresa, se recomienda la implementación de las siguientes políticas de seguridad:

4.3.1 Políticas de Acceso Físico

- Todos los empleados deben tener acceso solo a las áreas donde se encuentra la información necesaria que les permita desarrollar sus actividades.

- Solo el personal autorizado podrá ingresar a las instalaciones donde se almacena la información confidencial.

- Solo bajo vigilancia de personal autorizado y durante un período de tiempo justificado, personal externo (proveedores) pueden ingresar a las instalaciones donde se almacena la información confidencial.

4.3.2 Políticas de Seguridad de comunicaciones

- El encargado del área de comunicaciones deberá tener la documentación detallada con los diagramas actualizados de la red.

- Se deben definir medios alternativos de transmisión en caso de que alguna contingencia afecte el medio primario.

- Respecto a la utilización de la red, deben almacenarse los siguientes datos:
    - Ancho de banda utilizado
    - Tráfico generado por las aplicaciones
    - Recursos de los servidores que utilizan las aplicaciones
    - Intentos de violación a la red

- Los sistemas de comunicación sólo deben usarse para actividades de trabajo. El uso personal en forma ocasional será permisible siempre y cuando consuma una cantidad mínima de tiempo y recursos, y no interfiera con la productividad del empleado, para lo cual se gestionará con el supervisor el uso de los mismos.

- Todas las conexiones a internet de la empresa deben pasar a través de los servidores de proxy una vez que las haya filtrado el firewall.

- Deben documentarse servicios provistos a través de internet y definirse las responsabilidades de su administración.

- Si es necesario establecer una vía de comunicación con terceros se debe establecer los mecanismos de transmisión y responsabilidades con la entidad por escrito.

- Todos los equipos de la empresa deben tener instalado y ejecutar el antivirus de forma recurrente para detectar y controlar cualquier acción viral y debe ser un producto legal ya sea licenciado o software libre.

- El firewall de la empresa debe presentar una política de negación preestablecida, de tal manera que se prohíban todos los protocolos y servicios y luego habilitando únicamente los necesarios.

4.3.3 Políticas de Seguridad de las Aplicaciones

- No debe utilizarse software que provenga de fuentes no confiables, como por ejemplo software descargado de internet, a menos que haya sido autorizado su uso por el área de aplicaciones.

- Se debe llevar el registro de todas las transacciones realizadas en la base de datos, de manera que puedan revertirse en caso de surgir algún inconveniente.

- Se definirá un responsable de cada área de la empresa que sea el responsable de la información que se maneja. Será el encargado de realizar la clasificación de los datos y los controles de acceso necesarios en conjunto con el jefe del área de infraestructura.

- Se generará un procedimiento donde se especifique las aplicaciones que deben instalarse de acuerdo al perfil de cada usuario y la frecuencia con la que se actualizarán las aplicaciones.

- Antes de realizar un cambio en la configuración de los servidores se obtendrá un respaldo de la configuración existente, por si es necesario reversar el cambio.

- Se documentará el proceso de instalación, reparación y mantenimiento de los equipos, así como de los errores de hardware y software reportados.

- Antes de realizar alguna modificación en el sistema, deberá realizarse un análisis del impacto y presentar un plan a las áreas involucradas.

- Los cambios deben documentarse mediante un documento formal, donde se detallará el motivo y solicitud del cambio y se agregarán los requerimientos de seguridad necesarios, definidos por el responsable de la información y el jefe del área de infraestructura. El documento debe incluir:

    - Sistema afectado
    - Fecha para la modificación
    - Desarrollador que realizará el cambio
    - Solicitante del cambio
    - Descripción de la modificación a realizar
    - Autorización de los jefes de las áreas involucradas

4.3.4 Políticas de Almacenamiento y Respaldo de información

- La información debe ser almacenada y respaldada de forma que se garantice su disponibilidad.

- El área a la que pertenece la información, en conjunto con el personal de infraestructura definirá el proceso y el intervalo adecuado para respaldar la información.

4.3.5 Políticas de Confidencialidad de la información

- Cada área deberá clasificar el tipo la información que maneja principalmente bajo el criterio de información pública, interna, confidencial y restringida.

- El personal debe comprometerse a utilizar la información exclusivamente para fines empresariales, dentro de los procesos administrativos correspondientes.

4.3.6 Lineamientos para la adquisición de bienes informáticos

- Toda adquisición será analizada por el área de infraestructura, teniendo en consideración estudio técnico, precio, calidad, estándares y desarrollo tecnológico.

- Para la adquisición de hardware se revisará que el equipo a adquirir esté dentro del listado vigente otorgado por los proveedores.

- Los equipos adquiridos, de preferencia deben contar con asistencia técnica durante la instalación y una garantía de al menos un año.

- Para la adquisición de software base y utilitarios, deben adquirirse las últimas versiones liberadas, las cuales deben contar con su respectiva licencia, documentación y garantía.

4.3.7 Lineamientos para la información

- La información almacenada en medios magnéticos debe ser inventariada, incluyendo descripción y especificaciones de la misma.

- Los jefes de cada área serán responsables de la información de los departamentos a su cargo.

- La información almacenada en medios magnéticos, de carácter histórico, quedará documentada y estará resguardada en un lugar seguro y que cumpla con las condiciones requeridas para mantenerla disponible.

4.3.8 Plan de contingencias

El plan de contingencias debe considerar los siguientes puntos para continuar con las operaciones críticas del negocio:

- Tener respaldos de información fuera del sitio principal.
- Contar con un instructivo de operación para detección de fallas y procedimientos en caso de encontrarlas.
- Contar con un directorio del personal interno y externo de soporte para ubicarlos en caso necesario.
- Ejecutar pruebas controladas del plan de contingencias que permitan medir su efectividad.
- Actualización continua del plan, al suscitarse cambios en software, hardware o procedimientos que impacten las operaciones.

4.3.9 Responsabilidad de los empleados en el cumplimiento de la normativa para la seguridad de la información:

- Todas las personas que laboran dentro de la empresa, son responsables del cumplimiento de las políticas de seguridad.
- Los responsables de la información serán los encargados de definir los accesos a la misma y estarán involucrados en cambios a nivel de aplicativo que involucre el uso de la información.

4.4 Plan para la implementación del SGSI

La implantación de un sistema de Gestión de la Seguridad de la Información en una empresa es recomendable completarlo entre seis meses y un año.

Se recomienda que el proceso de implementación no supere el año, ya que una dilatación puede causar que el trabajo realizado al principio del proyecto quede obsoleto antes de llegar a su finalización.

Dentro de esta fase la formación e información continua al personal es una de las bases para que todos los directa o indirectamente involucrados en el SGSI tengan conocimiento de las responsabilidades que se les asignará y permitirá observar a nivel macro el objetivo a alcanzar.

Indudablemente se encontrará personas que colaborarán con el proceso de inmediato y a su vez se encontrará personal resistente al cambio, por lo cual es importante contar con el apoyo de los directores de departamento y la gerencia general quienes deben estar en capacidad de ampliar la información sobre los beneficios que traerá la implementación del SGSI y manejar adecuadamente las dudas y resistencia que pueda expresar el personal.

En esta etapa la documentación que se pueda generar será de gran utilidad, entre los principales documentos a elaborar o actualizar se encuentran:

- Política de seguridad: Con las líneas generales que la organización desea seguir en seguridad.

- Inventario de activos: Que incluya la descripción de los activos de información de la organización y su valoración para la misma.

- Análisis de riesgos: Con los valores de riesgo de cada uno de los activos.

- Procedimientos: Con la descripción de las tareas a realizar para la ejecución de los controles que lo necesiten o de las tareas de administración del SGSI.

- Registros. Son las evidencias de que se han realizado las tareas definidas para el SGSI. Son muy importantes de cara a poder medir la eficacia de las medidas implantadas así como a justificar las labores realizas frente a las auditorías del sistema (tanto internas como externas)

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

- Se realizó el levantamiento de información sobre la arquitectura de la red, la seguridad que tienen implementada para el manejo de la infraestructura, los roles y operaciones y el tipo de administración que la empresa utiliza.

- Se identificaron fortalezas en la seguridad física de los activos, sin embargo también se encontraron brechas de seguridad a nivel lógico y en la documentación que maneja el área de desarrollo e infraestructura, así como la falta de un proceso y prueba de contingencia que garantice la operatividad básica de sus sistemas en caso de un desastre.

- Se determinó que la norma ISO 27001 establece los requisitos de los sistemas de gestión de la seguridad de la información que la empresa requiere, por lo cual fue tomada como base para realizar el diseño; asegurando la selección de los controles de seguridad adecuados y proporcionados para proteger la información y dar la confianza a las partes interesadas.

- De acuerdo a los nueve activos físicos que se determinaron a proteger en conjunto con el personal de la empresa, se realizó el análisis de riesgo de cada uno y de acuerdo al nivel de afectación que representa para la empresa, se propone la implementación del SGSI.

- Se pone a consideración la implementación del plan del SGSI elaborado, tomando en consideración los requerimientos de seguridad presentados por la empresa. El SGSI está enfocado en los principales procesos donde se concentra la mayor parte de actividades relacionadas con la gestión de información y riesgos levantados en el transcurso del proyecto.

5.2 Recomendaciones

- Designar una persona responsable dentro de la empresa para que se ejecute la implementación del Sistema de Gestión de Seguridad de la información.

- Mantener actualizadas las normas, procedimientos y políticas de acuerdo a la dinámica en que se vayan incorporando nuevas estrategias para evitar el ataque contra sistemas y activos de información.

- Documentar todos los procesos operativos, detallando las interdependencias con otros sistemas, tareas de mantenimiento, tiempos de respuesta y procesos de recuperación de producirse algún incidente.

- Trabajar en la elaboración de un proceso de contingencias y designar un comité que se encargue de definir las funciones y responsabilidades de cada área involucrada ante algún desastre para garantizar la continuidad del negocio hasta que se regularice la operatividad.

BIBLIOGRAFÍA

Achiary, C. (Julio de 2005). Obtenido de Política Modelo: http://www.sgp.gov.ar/sitio/PSI_Modelo-v1_200507.pdf

Alberts, C. D. (2003). Managing Information Security Risks. En C. D. Alberts, *Managing Information Security Risks.* Boston.

Alexander, A. (2006). *Análisis del riesgo y el sistema de gestión de información: el enfoque ISO 27001:2005.* Lima.

Ardita, J. C. (2011). Cybercrimen y Manejo de Incidentes. *XII Congreso Interamericano de Seguridad de la información.* Uruguay. Obtenido de Cybercrimen y Manejo de Incidentes: http://www.cybsec.com/

Consejos de Seguridad. (s.f.). Obtenido de http://www.seguridad.unam.mx/usuario-casero/consejos/

García, J. M. (2004). La Seguridad de la Información - Nueva ventaja competitiva en la empresa. *Canales de mecánica y electricidad*, 22-25.

García, J. M. (2004). La Seguridad de la Información. Nueva ventaja competitiva en la empresa. *Canales de mecánica y electricidad*, 22-25.

Huerta, A. V. (2 de Octubre de 2000). *Segu.Info*. Obtenido de Seguridad de la información: http://www.segu-info.com.ar/fisica/

ISO 27000. (s.f.). *ISO 27000*. Obtenido de EL PORTAL DE ISO 27001: http://www.iso27000.es/

National Institute for Standars and Technology. (s.f.). *National Institute for Standars and Technology*. Obtenido de NIST: http://www.nist.gov/

Ramio, J. (2006). Seguridad Informática y Criptografía. En J. Ramio, *Seguridad Informática y Criptografía* (págs. 63-74). Madrid.

Seguridad Informática. (s.f.). Obtenido de Seguridad Informática: http://es.kioskea.net/contents/622-introduccion-a-la-seguridad-informatica

Seguros Equinoccial. (s.f.). *Seguros Equinoccial*. Obtenido de Seguros Equinoccial: http://www.segurosequinoccial.com/web/cms.php?c=616

Subdirección General de Información, Documentación y Publicaciones. (2012). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid España: Ministerio de Administraciones Públicas.