ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“DESARROLLO DE UN ESQUEMA DE SEGURIDAD DE INFORMACIÓN SIGUIENDO EL ESTÁNDAR ISO 27001-2013 APLICADO AL ÁREA DE SEGURIDAD DE LA INFORMACIÓN PARA UNA COOPERATIVA DE AHORRO Y CRÉDITO”

TRABAJO DE TITULACIÓN

PREVIA A LA OBTENCIÓN DEL TÍTULO DE:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

CARLOS FREDDY SALTOS PEÑA

ILSE LORENA YCAZA DÍAZ

GUAYAQUIL – ECUADOR

AÑO 2017

AGRADECIMIENTO

Agradezco a Dios por haberme dado la fuerza de seguir adelante cuando más lo necesitaba, por bendecirme con las cualidades necesarias para poder realizar este trabajo y por haberme guiado hacia el camino correcto para poder cumplir una de mis metas en la vida. A mi familia quien me ha apoyado siempre.

Ing. Carlos Freddy Saltos Peña

Agradezco a Dios por bendecirme para poder cumplir con este trabajo, a mis padres y hermana con quienes siempre cuento con su apoyo incondicional para poder lograr metas en mi vida.

Lsi. Ilse Lorena Ycaza Díaz

DEDICATORIA

El siguiente trabajo de tesis está dedicado especialmente a mis padres que gracias a sus escuerzos he logrado culminar mis estudios, a todas las personas cercanas que me apoyaron durante todo este proceso de desarrollo y superación.

Ing. Carlos Freddy Saltos Peña

Dedico esta a tesis a mi esposo e hija, ya que son la razón de que me esfuerce por el presente y el mañana, son mi principal motivación. Como en todos mis logros, en este han estado siempre presente, gracias por su apoyo incondicional.

Lsi. Ilse Lorena Ycaza Díaz

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenín Freire Cobo, MSIG.

DIRECTOR MSIG/MSIA

Ing. Jorge Enrique Olaya Tapia

DIRECTOR DEL PROYECTO DE TITULACIÓN

Ing. Róbert Andrade Troya

MIEMBRO DEL TRIBUNAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Trabajo de titulación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Ing. Carlos Freddy Saltos Peña

Lsi. Ilse Lorená Ycaza Díaz

RESUMEN

El presente proyecto de tesis consta de siete capítulos, los cuales inician con una descripción del problema actual de la Institución, la misma que no ha adoptado formalmente un estándar respecto a la seguridad de la información, sumado al cumplimiento normativo del organismo de control y a factores tales como incidentes y problemas que han afectado la imagen y a las finanzas de la institución.

En los capítulos siguientes se propone una solución, que está enfocada a dos procesos definidos por la institución, como son: monitoreo de la seguridad informática y la gestión de usuarios en los sistemas, basado en el estándar ISO 27001:2013, el cual es reconocido mundialmente y adoptado por instituciones financieras del medio local. Realizando los análisis respectivos, se detectarán los controles necesarios a implementar de la ISO 27002, asegurando de forma razonable la disponibilidad, confidencialidad, disponibilidad y vigencia de los activos de la información de los dos procesos definidos.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AD	**:**	Directorio activo
AUX	**:**	Equipamiento Auxiliar
AUX1	**:**	Equipos de aire acondicionado centro datos
AUX2	**:**	Equipos contra incendios del centro de datos
AUX3	**:**	Energía eléctrica
AUX4	**:**	Equipos de UPS de centro de datos
AUX5	**:**	Cableado
C	**:**	Confidencialidad
COM	**:**	Comunicaciones de redes
COM1	**:**	Red Telefónica
COM2	**:**	Red LAN
COM3	**:**	Red WAN
D	**:**	Disponibilidad
D1	**:**	Contrato de proveedores
D2	**:**	Documentación de procesos
ESPOL	**:**	Escuela Superior Politécnica del Litoral
HW	**:**	Hardware
HW1	**:**	Servidor
HW2	**:**	Computador de escritorio
HW3	**:**	Computador portátil

HW4	**:**	Impresoras
HW5	**:**	Equipos de red
HW6	**:**	Equipos de monitoreo
I	**:**	Integridad
ISO	**:**	Organización Internacional de Normalización
IVR	**:**	Sistema de voz interactivo
JB	**:**	Junta Bancaria
L1	**:**	Edificio
LAN	**:**	Red de área local
M	**:**	Soportes
M1	**:**	Cintas de respaldos
P1	**:**	Usuarios externos
P2	**:**	Usuarios internos
P3	**:**	Operadores de Monitoreo
P4	**:**	Operadores de Infraestructura
P5	**:**	Proveedores
PDCA	**:**	Planear, Hacer, Revisar y Actuar
PTR	**:**	Plan de tratamiento al riesgo
RHEL	**:**	Red Hat Enterprise Linux
S	**:**	Servicios
S1	**:**	Canal de Internet
S2	**:**	Repositorio de Archivos

S3	**:**	Web Institucional
S4	**:**	Correo electrónico
SBE	**:**	Superintendencia de Bancos del Ecuador
SEPS	**:**	Superintendencia de Economía Popular y Solidaria
SGSI	**:**	Sistema de Gestión de Seguridad de la Información
SOA	**:**	Declaración de Aplicabilidad
SW	**:**	Software
SW1	**:**	Aplicativo de Ofimática
SW2	**:**	Sistema de gestión de base de datos
SW3	**:**	Sistemas operativos
SW4	**:**	Sistema de gestión de respaldos
SW5	**:**	Sistema de monitoreo de seguridad informática
T	**:**	Trazabilidad
WAF	**:**	Firewall de aplicaciones web
WAN	**:**	Red de área amplia

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El presente trabajo, tiene como objetivo el desarrollo de un esquema de seguridad de la información para una cooperativa de ahorro y crédito en base a la Norma ISO 27001 para lograr cumplir con las normativas vigentes del organismo de control, en base a una adecuada gestión de la información, garantizando de forma razonable que los riesgos identificados sean tratados en base a procedimientos definidos y formalizados en la institución.

Para poder realizar este proyecto se consideró como bases, las guías que se indican en la Norma ISO 27001, acorde a la realidad de la institución. La aplicación de un SGSI, ayudará a la institución a mejorar sus procedimientos, procesos y cultura organizacional, lo cual finalmente se verá reflejado en la imagen de la institución ante sus clientes y público en general respecto al compromiso para el cumplimiento de sus obligaciones.

CAPÍTULO 1
GENERALIDADES

1.1 ANTECEDENTES

El presente proyecto tiene como objetivo el Desarrollo de un esquema de Seguridad de la Información para una Cooperativa de Ahorro y Crédito, considerando la Norma ISO 27001:2013, para obtener una gestión de la información adecuada y garantizar de forma razonable que el impacto de los riesgos identificados sean mínimos y estén respaldados en los procedimientos , en función de la normativa legal vigente del organismo de control, no se implementaran controles, estos quedarán dispuestos para que la institución los implemente en el tiempo que lo requieran.

La institución financiera, está legalmente constituida en el Ecuador desde 1992, regida por la SEPS (Superintendencia de Economía Popular y Solidaria) [10] y debe cumplir con carácter de obligatorio las resoluciones emitidas hasta el 2012 por la SBE (Superintendencia de Bancos del

Ecuador) [10] y de forma opcional las posteriores a esa fecha. La institución presta sus servicios financieros al público en general por medio de depósitos a la vista, certificado de depósitos, créditos de consumo, créditos comerciales, pago de servicios básicos, retiro por cajeros automáticos entre los principales.

La institución cuenta con 14 sucursales a nivel nacional y su matriz se encuentra radicada en la ciudad de Guayaquil, la cual cuenta con 40 empleados y su Oficina principal en Quito con 30 empleados.

1.2 DESCRIPCIÓN DEL PROBLEMA

Actualmente, la institución Financiera, no ha adoptado formalmente un estándar respecto a la seguridad de la información, sumado al cumplimiento normativo del organismo de control y a factores tales como incidentes y problemas que han afectado la imagen y a las finanzas de la institución, existe la necesidad de adoptar un estándar de seguridad basado en mejores prácticas reconocidas internacionalmente, por lo cual ha contratado recientemente a un Oficial de Seguridad de la Información y han definido inicialmente dos procesos para el desarrollo del proyecto de estabilización de la seguridad de la información , los cuales son: Administración del monitoreo de la seguridad informática y la Gestión de usuarios en los sistemas.

De una muestra de los problemas de seguridad detectados por la

institución, se evidenciaron los siguientes:

Gestión de usuarios en los sistemas:

- No existen políticas de cambios de claves., lo cual causa perdida de confidencialidad y disponibilidad del acceso a los sistemas por personal no autorizado.
- No existe control de acceso a estaciones de trabajo fuera del horario laborable, lo cual causa que se realicen trabajos críticos no autorizados fuera del horario establecido.
- No existe políticas de desvinculación de personal en los aplicativos, causando que en ocasiones usuarios de personal que ya no trabaja en la institución siga activo en los aplicativos.
- No existen políticas sobre el buen uso de las credenciales de acceso, lo cual ha provocado que entre empleados se presten las credenciales.
- La segregación de funciones en aplicativos críticos no está implementada, la misma persona puede ingresar y aprobar una transacción.
- No existen políticas de administración de los usuarios con accesos privilegiados, por lo cual personal de sistemas tiene acceso total a ciertos recursos de la información.
- No se ha identificado formalmente los activos de la información de la

institución basados en una metodología de riesgos.

Administración del monitoreo de la seguridad informática:

- No existen políticas de administración de la seguridad informática en la institución, lo cual causa que eventos que se presenten de forma aisladas o de manera poco frecuente no se consideren como potenciales amenazas en el corto plazo.
- Los eventos que se presentan y son resueltos, no se registran permanentemente de forma centralizada, causando un costo en recursos (tiempo, etc.) a la institución de volverse a presentar el evento para resolverlo.
- No existen procedimientos de manejo de incidentes, causando que esto se realice de forma empírica y a criterio propio del personal asignado.
- Existen herramientas de monitoreo que fueron adquiridas, pero no están operativas completamente por lo cual no están reportando el beneficio esperado.
- No existen políticas de mantenimiento y no se ha realizado revisiones periódicas de los controles como antivirus, soporte activo del fabricante del sistema operativo en las estaciones de trabajo y servidores.

Cumplimiento normativo:

- La institución, no tiene aplicado un estándar de seguridad de la información, la administración esta se realiza de la mejor forma considerada por el responsable de Seguridad, lo cual no necesariamente está alineada a un estándar reconocido, causando una contradicción con la normativa del organismo de control que indica que se debe administrar un sistema de seguridad de la información alineados a estándares internacionalmente reconocidos.

1.3 SOLUCIÓN PROPUESTA

La solución propuesta, está enfocada a dos procesos definidos por la institución, como son: monitoreo de la seguridad informática y la gestión de usuarios en los sistemas, en función del tiempo dispuesto para la propuesta, considerando el cumplimiento prioritario de la norma del organismo de control, la reducción de incidentes y problemas de seguridad, basado en el estándar ISO 27001:2013, el cual es reconocido mundialmente y adoptado por instituciones financieras del medio local. Esto se realizará por medio de la propuesta de implementación de controles de la ISO 27002, asegurando de forma razonable la disponibilidad, confidencialidad, disponibilidad y vigencia de los activos de la información de los dos procesos definidos.

La solución, se basará en el siguiente esquema general:

- Especificación del alcance.
- Análisis de la situación actual de la seguridad informática en la gestión de usuarios y en el monitoreo de la seguridad informática.
- Esquema documental.
- Análisis de riesgos.
- Propuesta de proyectos.

Los beneficios directos esperados de la solución propuesta son:

1. Mejora de la imagen de la institución hacia sus clientes internos y externos.
2. Cambio de cultura organizacional orientada a la seguridad.
3. Reducción de tiempos en la solución de incidentes relacionados a la seguridad y a la gestión de usuarios.
4. Cumplimiento normativo.
5. Detección oportuna de eventos de seguridad.

1.4 OBJETIVO GENERAL

Diseñar un esquema de Seguridad de la Información para una Cooperativa de Ahorro y Crédito de acuerdo con los requisitos del negocio, normas, leyes y regulaciones para los procesos de monitoreo de la seguridad informática y la gestión de usuarios en los sistemas, en base al estándar ISO 27001.

1.5 OBJETIVOS ESPECÍFICOS

- Comprender el estándar ISO 27001 y los reglamentos normativos.
- Analizar la situación actual de la institución respecto a su estructura.
- Diseñar los procedimientos necesarios en función de los riesgos asociados a los procesos seleccionados.
- Desarrollar y proponer los planes de acción para mitigar los riesgos.
- Comparar los resultados de la adopción del estándar por el área delegada por el Directorio en la institución.

1.6 METODOLOGÍA

La propuesta metodológica se basa en los siguientes pasos, considerando el ciclo PDCA el cual se describe a continuación:

Planear: Establecer políticas, objetivos y procesos relevantes para manejar el riesgo y optimizar la seguridad de la información con entregables en concordancia con la políticas y objetivos generales de la organización.

Hacer: Implementar y operar las políticas, controles, procesos y procedimientos SGSI.

Chequear: Evaluar y de ser el caso, cuantificar el desempeño del proceso basado en la comparación de la política, objetivos y experiencias prácticas del sistema de gestión y reportar los resultados hallados a la

gerencia responsable quien se encargará de la medidas orientadas a subsanar las observaciones.

Actuar: Realizar acciones basadas en la corrección y prevención, de los resultados de la auditoría interna SGSI, adicionando la evaluación de la Gerencia responsable con el objetivo de lograr el mejoramiento continuo del Sistema De Gestión.

Esta actividad se realizará en un plazo estimado de 3 meses, de acuerdo al siguiente detalle:

1 Formalización del Proyecto

Se realiza la propuesta del proyecto para la obtención de la aprobación del proyecto por parte de la Institución.

2 Equipo de trabajo

Previa aprobación de la institución, se delegará de forma permanente al proyecto a un sólo empleado del área de Plataforma Tecnológica, de ser el caso se solicitará la participación de otros funcionarios.

3 Análisis de la organización

Se ejecutará un análisis de brecha, basado en la situación actual de la Institución con los requisitos de ISO 27002 [11]. De ser necesario, se establecerán otras medidas de seguridad adicionales que puedan surgir

durante el proceso de análisis, se revisarán todos los dominios relacionados a los procesos definidos: Administración del monitoreo de la seguridad informática y la Gestión de usuarios en los sistemas.

4 Evaluación del análisis diferencial

Se realizará la evaluación del análisis de la organización para obtener el plan de acción correspondiente a minimizar los riesgos que serán tratados.

PLAN DE TRABAJO

El esquema de trabajo que se detalla, es el que permitirá un adecuado desarrollo del proyecto con el alcance de los dos procesos definidos, el cual considera los siguientes puntos:

- Adecuación de un lugar de trabajo.
- Estudio de la norma ISO 27001:2013
- Inicio de las actividades.
- Especificación y aprobación del alcance del proyecto.
- Análisis de brecha actual de la institución.
- Determinación de los requerimientos del SGSI.
- Tipificación, análisis y valoración de las vulnerabilidades.
- Elaborar planificación de respuestas antes los riesgos PTR.
- Factibilidad de aplicación de los controles seleccionados.

- Selección y evaluación de los objetivos de control.
- Costeo referencial para la implementación del diseño.

CAPÍTULO 2
MARCO TEÓRICO

2.1 CONCEPTOS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

2.1.1 Introducción

La seguridad de la información en forma general dentro de las organizaciones es presentada y asistida como un problema con enfoque tecnológico, por lo cual no se está considerando a la seguridad de la información como parte integral y transversal dentro de la organización. Es preciso definir un conjunto de medidas preventivas y reactivas en la organización y en los sistemas tecnológicos con el objetivo del resguardar y proteger la información para conservar la confidencialidad, disponibilidad e integridad de los datos. *(Ver Figura 2.1)*

Figura 2.1.- Seguridad de la Información tratada en capas

Fuente: Elaborado por (BINARIA, 2012)

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

2.1.2 Definición De Seguridad De La Información

La información que transita en una organización es el activo más relevante que pueda disponer, por lo cual tiene un valor alto para la institución y en función de aquello, se desarrollarán diferentes procesos para asegurar la razonabilidad de una protección

adecuada.

Los objetivos de la seguridad de la información son:

Proteger de forma razonable a la institución de amenazas, minimizando el impacto y maximizando el retorno de la inversión realizada.

La información puede adoptar diversos tipos, como son: física (escrita, impresa), transmitida por correo o por medios electrónicos o hablada, independientemente del medio, deberá protegerse adecuadamente.

La seguridad de la información, radica en la conservación de la confidencialidad, integridad y disponibilidad de este recurso y su vigencia.

2.2 GESTIÓN DE RIESGOS

La gestión del riesgo es una parte básica de la norma ISO 27001, considerando que posteriormente a la revisión y evaluación de los riesgos los controles se seleccionarán, por lo que es necesario, conocer, medir y evaluar los riesgos, así como hacer de esta una actividad continua en una etapa futura para asegurar que se tiene implantando una eficaz seguridad de información basada en la norma.

2.2.1 Definición Riesgo

Se define al riesgo como el daño potencial que puede afectar a un activo de la información por eventos que pueden involucrar a procesos, personas o tecnologías de la información. Es común utilizarlo como sinónimo de probabilidad, pero en el asesoramiento profesional de riesgo, esta combina la probabilidad de que ocurra un evento negativo con el impacto o daño que pueda causar.

2.2.2 Fuentes Riesgo

Las fuentes de riesgos son variadas y pueden tener un impacto en la organización, estas fuentes son conocidas como amenazas y tiene el potencial de causar un incidente deseado o no deseado, provocando daños en un sistema, a la organización y en general a los activos. Estas fuentes pueden ser por ejemplo de origen natural o causadas por negligencia o impericias como resultado de acciones maliciosas.

2.2.3 Análisis Del Riesgo

Para implantar un Sistema de Gestión de Seguridad de Información sustentando en la norma ISO 27000, la organización necesita de forma inicial determinar el alcance del estándar en la organización, en base a este insumo identificar los distintos activos de información.

Una vez identificados los activos de información, se realiza un análisis y evaluación del riesgo e identificar los controles que mitiguen el riesgo.

Es importante clarificar la definición de Activos de Información. Según el ISO 17799:2005, (Código de Práctica para la Gestión de Seguridad de la Información) un activo de información es: *"algo a lo que una organización directamente le asigna un valor y por lo tanto la organización debe proteger".* Los activos de información, son clasificados en las siguientes categorías:

- Activos de información (datos, manuales de usuario, etc.)
- Documentos de papel (contratos)
- Activos de Software (aplicación, software de sistemas, etc.)
- Activos Físicos (computadoras, medios magnéticos, etc.)
- Personal (clientes, personal)
- Imagen de la compañía y reputación
- Servicios (comunicaciones, etc.)

Los activos de información son muy amplios. Se requiere conocer qué es un activo de información, para poder efectuar un correcto análisis y evaluación de riesgo.

El objetivo del análisis del riesgo es apreciar la magnitud del riesgo

que afecta a los activos de la información, por lo cual, se deben tomar decisiones en función de que riesgos la organización aceptará o no y qué controles podrán ser implantados para mitigar el riesgo asociado.

Para realizar el análisis de riesgos, existen muchos métodos, cada uno de ellos tiene sus propias características, así como sus ventajas y desventajas, por lo cual es necesario entender los diferentes métodos y sus características para seleccionar un método de análisis de riesgos que se ajuste a lo que persigue la organización.

Entre las cuales tenemos:

- ISO 13335-1:2004. Tecnología de la información - Técnicas de seguridad - Gestión de la seguridad de la tecnología de la información y las comunicaciones
- ISO73 Gestión del Riesgo
- ISO27005 Seguridad de la información y de las comunicaciones
- AS 4360 (Australia) set de Gestión de Riesgos
- NIST SO 800-30 (USA) Metodología de Gestión del Riesgo
- MAGERIT (España) Metodología y práctica para gestionar riesgos
- EBIOS (Francia) Método de análisis, evaluación y acción sobre riesgos relacionados con el sistema de información.
- OCTAVE (Cert) Metodología de Análisis de Riesgo

Se realizará una breve descripción de algunas metodologías de análisis de riesgos:

MAGERIT

Es una metodología de Gestión de Riesgos, la cual es promocionada por el Consejo Superior de Informática español. Define los procedimientos para guiar a la Administración en el establecimiento de un nivel de protección adecuado, en respuesta a su dependencia en las técnicas cambiantes electrónicas, informáticas.

Los objetivos principales de la metodología son:

- Analizar los riesgos que soporta un determinado sistema de información y el entorno asociado, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio.
- Recomendar las medidas apropiadas que deberán adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos asociados mediante una adecuada gestión de riesgos.

EBIOS (Francia)

EBIOS permite visualizar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI). Posibilita también la comunicación dentro de la institución y también con los asociados para contribuir al proceso de la gestión de los riesgos.

Adicionalmente se considera una herramienta de negociación y de arbitraje brindando las justificaciones necesarias para la toma de decisiones.

OCTAVE (Cert)

Permite que los equipos de trabajo del área operacional y de tecnologías de la información puedan trabajar juntos direccionando las necesidades de seguridad de la institución. El equipo utiliza el conocimiento del personal en la organización con el objeto de establecer el estado de brecha de seguridad, por medio de la verificación de los riesgos asociados los activos críticos en paralelo a las estrategias de seguridad.

OCTAVE es diferente de las valoraciones tecnológica, está enfocada en el riesgo organizacional y estratégico, riesgos operacionales balanceados, prácticas de seguridad y tecnología.

2.2.4 Proceso De Evaluación Del Riesgo

La *figura 2.2* indica la forma de evaluar al riesgo para permitir que una organización este alineada con los requerimientos del estándar ISO 27001.

Figura 2.2.- Proceso de Evaluación del Riesgo

Fuente: Creación Propia

Identificación y tasación de activos

Todos los activos identificados, deben estar valorados, asociados e informados a su propietario.

ISO/IEC 27001 (Código para el SGSI) realiza un catálogo de los activos de acuerdo al siguiente detalle:

1 Activos de información: las bases de datos, documentación de los aplicativos, manuales de usuario y técnicos, documentos de capacitación, procedimientos operativos de apoyo, planes de continuidad, documentos no digitalizados, todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI

2 Documentos físicos: documentos impresos, acuerdos

contractuales, lineamientos, procedimientos, u otros documentos importantes para el negocio.

3 Activos físicos: Equipos de redes y computación, magnéticos, ópticos y otros equipos técnicos.

4 Personas: Empleados, clientes y proveedores.

5 Imagen y reputación de la organización.

6 Servicios: Servicios de computación y otros servicios operativos.

Con el objeto de definir una protección adecuada sobre los activos, es relevante evaluar a estos activos en relación a su importancia dentro del negocio.

Identificación de requerimientos de seguridad

Con el objetivo de identificar los requisitos de seguridad de la organización, es recomendable basarse en tres pilares principales, que se describen a continuación:

a) El primer pilar, se basa en la valoración de los riesgos, con la identificación de las amenazas a los activos, se evalúa las vulnerabilidades y la probabilidad de su ocurrencia.

b) El segundo pilar, está basado en el conjunto de requisitos normativos, legales, que deberá satisfacer al organismo de control y los proveedores de servicios.

c) El tercer pilar, está formado por los principios y requerimientos

integrantes del de la información que se ha desarrollado para apoyar sus operaciones.

Identificación de amenazas y vulnerabilidades

Las vulnerabilidades son debilidades que están asociadas con los activos de la organización. Las debilidades pueden ser explotadas por las amenazas, causando incidentes no deseados, causando pérdidas, daño o deterioro a los activos.

Valoración de los riesgos de seguridad

El propósito de la evaluación del riesgo es el de identificar y evaluar los riesgos en forma consistente.

a) Consecuencias. - El impacto económico que probablemente resulte de una vulnerabilidad explotada, teniendo en cuenta las posibles consecuencias de pérdida de elementos de seguridad de la información y otros activos;

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

A continuación, se expondrán las escalas utilizadas para la valoración del riesgo, el umbral de tolerancia y el criterio para este

umbral, para lo cual en la valoración de riesgos se identificará y evaluará a los activos basados en las necesidades de la organización.

La organización deberá establecer un criterio para la determinación de los elementos de confidencialidad, integridad, disponibilidad y vigencia. *Ver Tabla 1, 2 y 3*

Tabla 1

Estándares para confidencialidad

Activos de información	Tipo	Descripción
1	Pública	Es posible acceder por terceras partes. Si su contenido fuera expuesto, la exposición de
2	Uso interno	Puede solo ser expuesta pero no disponible a terceras partes. Si su contenido fuera
3	Secreto	Debe ser sólo revelado y proporcionado a partes específicas y debidamente autorizadas.
4	Alta confidencialidad	Debe ser sólo expuesto y proporcionado a partes específicas.

Fuente: Creación Propia

Tabla 2

Estándares para Integridad

Activos de información (Integridad)	Tipo	Descripción
1	No necesaria	Para consulta. No tiene potenciales problemas
2	Necesaria	Si su contenido fuera vulnerado, no afectaría en gran parte a la institución.
3	Importante	Si la integridad se perdiera, hubiera un efecto fatal en las operaciones.

Fuente: Creación Propia

Tabla 3

Estándares para disponibilidad

Activos de información	Clase	Descripción
1	Bajo	Si la información llegara a estar no disponible, no hubiera efectos en las operaciones
2	Mediano	Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones. Sin embargo, métodos alternativos pudieran ser usados para las operaciones, o los procesos podrían ser demorados hasta que la información esté disponible.
3	Alto	Si la información no estuviera disponible cuando sea necesitada en cualquier momento, hubiera un fatal efecto en las operaciones.

Fuente: Creación Propia

La frecuencia de ocurrencia de las amenazas debe ser evaluada, a partir de la lista de amenazas determinada, estas deben ser revisadas en función de la experiencia de operaciones y datos estadísticos que han sido recolectados.

La frecuencia de ocurrencia de las amenazas es comúnmente dividida en tres categorías: “Baja”,” Media”,” Alta”. *Ver tabla 4 y 5.*

Tabla 4
Criterios para determinar las categorías de las amenazas
Amenazas

Probabilidad	Categoría	Descripción
1	Bajo	Hay una baja probabilidad, la frecuencia de ocurrencia
2	Medio	Existe una determinada probabilidad, la frecuencia
3	Alto	Hay una alta probabilidad, su frecuencia de ocurrencia

Fuente: Creación Propia

Tabla 5
Criterios para determinar las categorías de las vulnerabilidades
Vulnerabilidades

Probabilidad de	Categoría	Descripción
1	Bajo	Existen controles de seguridad muy débiles o no se tiene ningún control de seguridad, de tal manera que esta vulnerabilidad es susceptible de ser explotada sin mucho esfuerzo.
2	Medio	Existe un moderado control de seguridad
3	Alto	Si en el activo se tiene los controles de seguridad adecuados, de tal manera que sea

Fuente: Creación Propia

2.2.5 Selección De Opciones Para El Tratamiento Del Riesgo

Después de la identificación de los riesgos, la organización deberá evaluar la acción más idónea para tratar los riesgos, lo cual se conoce como el Plan de Tratamiento de Riesgos (PTR), que es un documento importante para el SGSI.

El objetivo básico es describir de forma clara las actualizaciones que se van a realizar para disminuir los riesgos a niveles tolerables para la organización, qué recursos van a asignarse para la realización de cada una de estas actualizaciones, las responsabilidades asociadas y las prioridades en la ejecución de las actualizaciones.

Para el tratamiento del riesgo existen cuatro estrategias identificadas:

Reducción del riesgo

Se deben implementar controles para disminuir a niveles aceptables (previamente identificados por la organización) el riesgo.

Aceptación del riesgo

Es posible que se presenten situaciones en la cual no se pueden disponer de controles sea por el costo de implantar el control represente un valor mayor que las consecuencias del riesgo si se

llegase a materializar.

En esta situación, la razonabilidad de la decisión se basa en la aceptación del riesgo y sus consecuencias o adoptar las opciones de “transferencia del riesgo” o la de “evitar el riesgo”.

Transferencia del riesgo

Es una opción generalmente adoptada por la organización, cuando es complicado, técnicamente como económicamente llevar al riesgo a un nivel aceptable, en estas circunstancias podría ser económicamente factible, transferir el riesgo a un tercero, como una empresa aseguradora.

Se debe considerar que, aunque se cuente con seguros externos, siempre existe un elemento de riesgo residual, como las condiciones que las aseguradoras tienen por exclusiones, por lo cual, al delegar los servicios a terceros, el riesgo residual no se delega, es responsabilidad de la empresa.

Evitar el riesgo

Describe cualquier acción donde las actividades del negocio o las formas de conducir la gestión del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras habituales para implementar esta opción son:

- Evitar realizar ciertas actividades asociadas al riesgo.
- Transferir activos de información de un área riesgosa a otra.
- Evitar procesar determinado tipo de información si no se consigue la protección adecuada.

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

Selección de controles para reducir los riesgos a un nivel aceptable

Como alternativa de tratamiento, al realizar el análisis de la evaluación del riesgo, se puede seleccionar los controles necesarios para neutralizar las posibles vulnerabilidades.

La selección de los controles deberá ser basada en los resultados de la evaluación del riesgo, las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida.

Cuando se seleccionan controles para la implementación, es necesario seleccionar ciertos controles, tales como:

- Uso de los controles.
- Transparencia del usuario.
- Ayuda otorgada a los usuarios para desempeñar su función.

- Relativa fuerza de controles.
- Tipos de funciones desempeñadas.

2.3 CONTROLES DE UN SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

La descripción de cada uno de los controles enmarcados dentro de la ISO 27002 y en los dominios se describe en forma general en el capítulo II.

2.4 ESTRUCTURA DEL SISTEMA DE GESTIÓN

Un Sistema de Gestión es una herramienta dispuesta para la Gerencia con el objeto de dirigir y controlar un determinado conjunto de responsabilidades. La organización tiene la posibilidad de implantar un número variable de estos Sistemas de Gestión para mejorar a la organización.

2.4.1 Objetivo

El objetivo de los diferentes estándares de Gestión de ISO es conducir a Sistemas de Gestión completos, que encierren todos los aspectos necesarios para la organización. Basándose en el ciclo PDCA *y* el proceso de mejora continua. *(Ver Figura 2.3).*

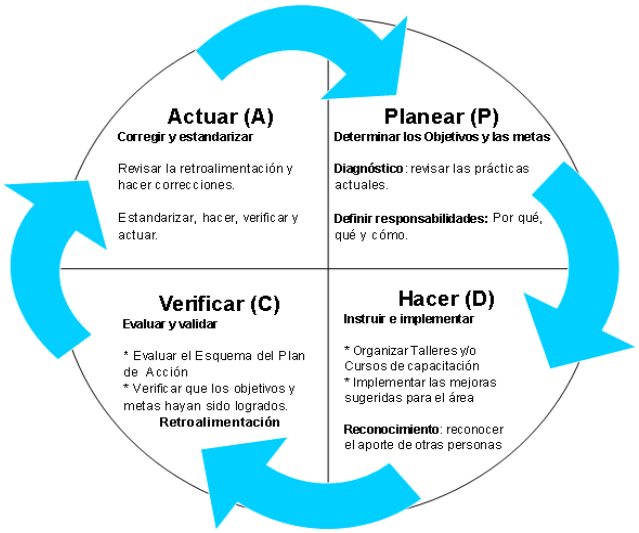


Figura 2.3.- Gráfico del PDCA

Fuente: (Orué, 2015) [9]

2.4.2 Operatividad de los sistemas de gestión

Los Sistemas de Gestión finalmente son adaptados a la organización para poder operar a la realidad de la organización, por lo cual tiene las siguientes características:

- Operar de manera eficaz
- Los resultados cubren las expectativas de los interesados.
- Énfasis en las acciones para prevenir eventos que puedan interrumpir las operaciones de la organización.

2.5 NORMAS ISO 27001:2013

2.5.1 Definición De Las Normas ISO 27001:2013

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO). El objetivo de la norma es definir la manera correcta en que la seguridad de la información debe de ser gestionada en la institución. La actualización más reciente de esta norma fue publicada en el año 2013. Nombrada como ISO/IEC 27001:2013 [7].

La norma ISO 27001[7] puede ser implementada en todo tipo de organización. Fue desarrollada por los mejores especialistas en el tema, proporciona metodologías que muestran de manera correcta cómo debe de ser implementada la gestión de la seguridad de la información en una organización. La implementación de esta norma en la empresa, permite que la misma sea certificada, confirmando que la seguridad de la información ha sido implementada en la institución.

ISO [7] es la norma principal y reconocida mundialmente para la seguridad de la información, la figura 2.4 detalla los dominios de la norma ISO 27001.

Figura 2.4 .- Dominios de la Norma Iso 27001

Fuente: (Info, 2013) [7]

En la Tabla 6 se describen en forma general, los 14 dominios del estándar ISO 27001:

Tabla 6

Dominio del estándar ISO 27001
Política de Seguridad
Organización de la información
Seguridad de Recursos Humanos
Gestión de Activos
Control de acceso
Criptografía
Seguridad Física y ambiental
Seguridad en las operaciones

Tabla 6

Dominio del estándar ISO 27001
Transferencia de la información
Adquisición de Sistemas, desarrollo y mantenimiento.
Relación con Proveedores
Gestión de incidentes de seguridad
Continuidad del negocio
Cumplimiento con requerimientos legales y contractuales

Fuente: Creación Propia

a) Política de seguridad

La revisión de esta política debe de ser planificada y comunicada a las partes interesadas. Los cambios significativos deben de ser direccionados para cumplir con los objetivos de la seguridad de la información y obtener una eficacia continua.

Política de seguridad de la información.

Revisión de las políticas para la seguridad de la información.

b) Organización de la información

Se debe establecer una estructura de la seguridad de la información, de tal manera que satisfaga todos los requerimientos, es indispensable la participación de los representantes de las diferentes

áreas dentro de la organización para cubrir las distintas necesidades.

Se debe de establecer un marco de referencia de gestión para controlar la operación de la seguridad de la información dentro de la organización.

Se debe de definir y asignar al personal responsable de la seguridad de la información. Si se cuentan con deberes y áreas de responsabilidad que estén en conflicto, deben de ser separadas para reducir las posibilidades de modificación no autorizada o intencional.

Se debe de mantener comunicación con las autoridades pertinentes o asociaciones de profesionales especializados en seguridad en información.

En la gestión de proyectos sin importar el tipo de proyecto que este sea, se debe de tratar la seguridad de la información con la persona responsable.

c) Seguridad de recursos humanos

Se debe de asignar a los recursos de la organización, clasificar la información a la que se va a tener acceso.

Dar a cada recurso la protección adecuada de acuerdo a su

clasificación, esta clasificación se realiza en base a niveles de sensibilidad y criticidad de la información.

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

La alta gerencia debe de exigir a los empleados y contratistas externos que las políticas y procedimientos correspondientes a la seguridad informática deben de ser necesariamente aplicados en sus actividades diarias.

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

Establecer un proceso formal, debe de ser debidamente comunicado y documentado en la organización sobre las acciones que recaerán sobre el empleado que comete alguna violación correspondiente a la seguridad de la información.

Se debe de definir un procedimiento para el manejo adecuado para la terminación o cambio de empleo, debe de estar incluido el retiro de los derechos de acceso a la información y la entrega de los

equipos de la compañía, para dar finalizada las responsabilidades con la institución.

d) Gestión de activos

Se debe identificar todo activos que se encuentre asociado con la información o procesamiento de la información. Debe de estar inventariado. Los activos en el inventario deben de tener un propietario. Se deberá de documentar e implementar reglas para el uso de la información y el activo asociado a la misma.

Los empleados externos o al salir de la empresa debe de devolver los activos que se encuentren a su cargo a la organización

e) Control de accesos

Los usuarios de red requieren de autorización previa para permitir el acceso a la red y los servicios de red. Se debe de diseñar una política de control de acceso de usuarios, la misma que deberá de estar documentada.

Se debe de implementar controles para el acceso de los usuarios autorizados para evitar accesos no autorizados a los sistemas y servicios.

Los procedimientos deben de cubrir las etapas de acceso de los

usuarios, desde el registro inicial hasta la baja del registro del usuario, incluye también la revocación de permisos y derechos de acceso.

Todo usuario debe de ser responsable por la información que este bajo su responsabilidad y de toda información que cuente con su autenticación.

El control de acceso a los usuarios restringe acceso a la información en base al rol del usuario de esta manera se evitarían accesos no autorizados a sistemas y aplicaciones.

El acceso a la información y a las aplicaciones de la organización debe de estar restringidos en base a las políticas de control de acceso.

Cuando la política de control de acceso lo requiera, al acceder ya sea por sistema o aplicación, se debe de controlar mediante el proceso de ingreso seguro.

Los sistemas de gestión de contraseñas deben de asegurar la calidad de las contraseñas ingresadas (sean diferentes a las del historial, con una cantidad mínima de caracteres, y combinaciones de complejidad alta).

Restringir el uso de programas utilitarios que pueden tener la

capacidad de anular el sistema y controles de las aplicaciones.

Por seguridad de la información, todo acceso a código fuente debe de estar restringido, el código fuente debe de estar auditado y documentada cualquier cambio en el mismo por el personal responsable.

f) Criptografía

Se deben utilizar sistemas basados en técnicas de cifrado para proteger la información, considerando que los controles actuales no proporcionen la protección adecuada.

Se debe de implementar una política sobre el uso y tiempo de vida de las claves criptográficas durante el ciclo de vida.

g) Seguridad física y ambiental

Se deben de definir políticas y controles para la prevención del acceso físico no autorizado, para proteger información confidencial. El acceso a la información crítica debe de ser mediante controles de acceso apropiados.

h) Seguridad en las operaciones

Los procedimientos de operación deben de estar debidamente documentados. Estos deberán de estar a disposición todos los

usuarios que lo requirieran.

Todo cambio, instalación o sistema de procesamiento que afecten directamente a la seguridad de la información y al negocio, deben de ser controlados y autorizados a través de su respectiva gestión.

Para asegurar la capacidad futura de desempeño de la organización, se debe de realizar un análisis del uso de los recursos y una proyección de los requisitos.

Al implementar la arquitectura, se debe de establecer una separación de los ambientes de desarrollo, pruebas y operación. De esta manera no existirán cambios no autorizados en ambiente de producción, esto será debidamente monitoreado.

i) Transferencia de información

La seguridad de la información debe de mantenerse dentro de la organización no en cualquier entidad externa, para lo cual se debe de crear políticas y controles de transferencia formales para proteger la información por medio de instalación de tipo de comunicaciones. Deben de existir acuerdos de confidencialidad para la no divulgación de la información de la empresa.

j) Adquisición de sistemas, desarrollo y mantenimiento

Considerar los requisitos de seguridad, las disposiciones para contingencias, la infraestructura, aplicaciones de negocio; se deberá identificar durante la fase de requisitos del proyecto, previamente consensuado y debidamente formalizado como parte del proceso de un sistema de información.

Los requisitos deben de incluirse para mejoras o nuevos sistemas de información que se implementen en la empresa. La información debe de ser protegida en las redes públicas de actividades fraudulentas, de las divulgaciones o modificaciones que no han sido autorizadas. Se debe de controlar la alteración no autorizada de mensajes, divulgación no autorizada o duplicación y reproducción de mensajes no autorizados.

k) Relación con proveedores

Se debe de establecer una política de seguridad de la información para los riesgos asociados con el acceso a la información y a los activos de la organización. Cada proveedor debe de tener los requisitos de seguridad de información a los que pueda tener acceso.

Se debe de auditar la prestación de servicios de los proveedores. Los cambios e servicios, gestiones de mantenimiento y controles de seguridad deben de ser gestionados, analizando la evaluación de

riesgos que afecta a la seguridad de la información.

l) Gestión de los incidentes de seguridad

Se debe de reportar a las áreas pertinentes de forma periódica la gestión de los incidentes y cualquier evento sobre la seguridad de la información y fallas. Se debe de definir a los responsables de los procedimientos que involucran la seguridad de la información y detallar un reporte de eventos, debilidades, evaluación y respuesta a incidentes de seguridad de información.

m) Continuidad del negocio

Determinar los requisitos para la seguridad de la información para la planificación de la continuidad del negocio. Donde se planifique previamente los pasos a seguir ante un desastre.

Se debe de mantener procesos y controles para asegurar la continuidad del negocio ante un desastre.

Se debe de revisar los controles de seguridad del negocio asignados para verificar su validez y eficacia.

n) Cumplimiento con requerimientos legales y contractuales

El diseño y gestión de los sistemas de información, están sujeto a requisitos normativos y legales.

El objetivo del control, es evitar potenciales incumplimientos legales, reglamentarios y de todo requisito de seguridad.

El riesgo de la seguridad de la información en una compañía, representa una amenaza importante. Existe la posibilidad de perder información y afecte directamente a la compañía.

¿Cómo gestionar este riesgo?

En la seguridad de la información se tiene como riesgo la prevención de fraudes online, daños a sitios web, caídas en la red, robo de identidad, pérdida de los datos entre otros. Existen varios tipos de amenazas informáticas a las que una organización se encuentra expuesta hoy en día.

La gestión de riesgos es uno de los elementos clave en la prevención del fraude online, robo de identidad, daños a los sitios Web, la pérdida de los datos personales y muchos otros incidentes de seguridad de la información. Sin un marco de gestión de riesgos sólida, las organizaciones se exponen a muchos tipos de amenazas informáticas.

Como beneficios de la implementación de la norma:

- Mejora la gestión de los riesgos de seguridad de la información.
- Enfoca sistemáticamente la gestión de la información

confidencial.

- Brinda confianza a los clientes y proveedores de que la seguridad de la información se toma en serio en la organización.

2.5.2 Normativas De Referencia

La alta dirección debe de establecer una política de seguridad de la información que sea adecuada para el propósito de la organización. Deberá de incluir los objetivos y requisitos de la seguridad de la información.

La gerencia debe aprobar la política de seguridad de información y difundirla a toda la organización. Debe de estar disponible como información documentada para las partes interesadas.

La serie de normas ISO/IEC 27000 contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener Especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI), estas normas incluyen:

Normas de la Familia ISO 27000 [7]

- ISO 27000 – vocabulario estándar para el SGSI.
- ISO 27001 – especifica los requisitos para la implantación del SGSI.

- ISO 27002 – código de buenas prácticas para la gestión de seguridad de la información.
- ISO 27003 – directrices para la implementación del SGSI.
- ISO 27004 – métricas para la gestión de seguridad de la información.
- ISO 27005 – gestión de riesgos en seguridad de la información.
- ISO 27006 – requisitos para acreditación de organizaciones que proporcionan certificación de SGSI.
- ISO 27007 – Es una guía para auditar al SGSI.
- ISO 27011 – Guía de Gestión de seguridad de la Información específica para telecomunicaciones.
- ISO 27031 – Guía de continuidad de negocio basada en las tecnologías de la información y las comunicaciones.
- ISO 27032 – Marco seguro para el intercambio de información, el manejo de incidentes y la coordinación para hacer más seguro los procesos.
- ISO 27033 – Norma derivada de la norma de seguridad ISO/IEC 18028. Es una visión general de seguridad de la red y de los conceptos asociados.
- ISO 37034 – Es una guía de seguridad de aplicaciones.
- ISO 27799 – Es una guía para implementar ISO 27002 en la industria de la salud.

- ISO 27035 – actividades de: detección, reporte y evaluación de incidentes de seguridad y sus vulnerabilidades.

2.6 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

El SGSI (Sistema de Gestión de Seguridad de la Información) [6] es el concepto sobre el que se construye ISO 27001. El objetivo de un sistema de gestión de la seguridad de la información es, garantizar de forma razonable que los riesgos sean conocidos, asumidos, gestionados y tratados por la organización, de una forma sistemática, estructurada y adaptada a los posibles cambios que se produzcan en el entorno y en el uso de las tecnologías.

2.6.1 Requisitos De La Documentación Del SGSI

La implantación de un SGSI (Sistema de Gestión de Seguridad de la Información) basado en ISO implica la correcta elaboración y recopilación de la Documentación, la documentación se muestra gráficamente como una pirámide de 4 niveles (*Ver Figura* 2.5):

Figura 2.5 .- Estructura de Documentación

(BINARIA, 2012) [1]

Documentos del Nivel 1:

- Alcance del SGSI: Se debe incluir de forma clara las dependencias y de ser el caso las relaciones y límites existentes entre el alcance y las partes que no fueron consideradas.
- Política y objetivos de seguridad: Documento de contenido genérico el cual establece el compromiso de la alta Dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- Metodología de evaluación de riesgos: Se realizará la revisión de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impacto basados en los activos de información dentro del alcance.
- Informe de evaluación de riesgos: Estudio resultante de aplicar

la metodología de evaluación anteriormente mencionada.

- Plan de tratamiento del riesgo: Definición de las acciones para reducir, transferir o asumir los riesgos asociados a los activos e implementar los controles adecuados.

Documentos del Nivel 2:

Procedimientos: Documentos del nivel operativo que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información y describen cómo poder medir la efectividad de los controles implementados.

Documentos del Nivel 3:

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

Documentos del Nivel 4:

Registros: Documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los niveles anteriores que demuestran que se ha cumplido lo indicado.

2.6.2 Control De Documentos

Todos los documentos requeridos por el SGSI serán protegidos y controlados, considerando que un procedimiento documentado deberá establecer las acciones de administración necesarias para:

- Revisiones, actualizaciones y aprobaciones de documentos, asegurando que los cambios y las revisiones de documentos sean identificados.
- Asegurar que las últimas versiones de los documentos aplicables estén disponibles.
- Asegurar que los documentos permanezcan legibles y fácilmente identificables.
- Asegurar que los documentos estén disponibles para quien los necesite y sean transferidos, guardados y finalmente dispuestos acorde a los procedimientos aplicables a su clasificación.
- Asegurar que los documentos de origen externo sean identificados.
- Asegurar el control de la distribución de documentos.
- Prevenir el uso no deseado de documentos obsoletos y aplicar una clara identificación para poder acceder a ellos y que estén adecuadamente almacenados para cualquier propósito que la organización o los organismos de control necesiten.

2.6.3 Responsabilidades De Administración

La alta administración deberá estar comprometida con el SGSI, la cual se puede evidenciar por medio de sus acciones en los compromisos adquiridos para el establecimiento, implementación, operación, monitorización, mantenimiento y mejora del SGSI por medio de las tareas requeridas para proveer las herramientas y capacitación necesaria (Documento: Planificación, guías y programas de formación y preparación).

2.6.4 Implementación de un SGSI

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basado en la ISO 27001, se utilizará el ciclo continuo PDCA, el cual es comúnmente utilizado en los sistemas de gestión de la calidad, en la Figura 2.6 detalla el gráfico de PDCA.

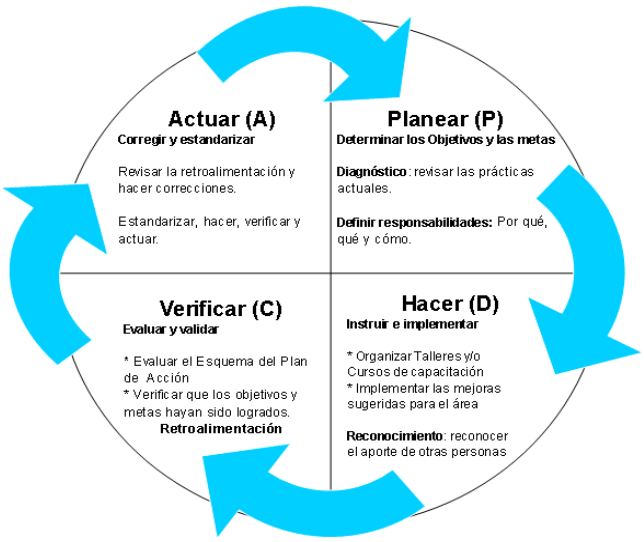


Figura 2.6.- Gráfico de PDCA

Fuente: (Orué, 2015) [9]

A continuación, se describen de forma general las actividades a seguir para la implementación del SGSI:

Plan (Establecer el SGSI)

- Definir el alcance del SGSI en términos del negocio.
- Definir una política de seguridad
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio que especifique los niveles de riesgo aceptables y los criterios de aceptación de los riesgos.
- Identificar los riesgos

- Analizar y evaluar los riesgos
- Identificar las acciones adoptadas para el tratamiento de los riesgos.
- Seleccionar los controles de la norma ISO 27002 que cumplan con los requerimientos identificados en la evaluación y tratamiento del riesgo.
- Definir una declaración de aplicabilidad

Do (Implementar y Utilizar el SGSI)

- Definir un plan de tratamiento de riesgos.
- Implantar el plan de tratamiento de riesgos.
- Implementar los controles.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables con el objeto de medir la eficacia de los controles seleccionados para mitigar los riesgos.
- Ejecutar programas de formación y comunicación en relación a la seguridad de la información dirigidos a todo el personal sin excepción.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida

detección y respuesta a los incidentes de seguridad.

Check (Monitorizar y revisar el SGSI)

- Ejecutar procedimientos de monitorización y revisión
- Revisar regularmente la efectividad del SGSI previamente planificado.
- Cuantificar la efectividad de los controles con el objeto de validar que cumplan los requisitos de seguridad establecidos.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Actualizar los planes de seguridad.
- Registrar acciones y eventos.

Act (Mantener y mejorar el SGSI)

- Implantar en el SGSI las mejoras identificadas, por medio de las acciones preventivas y correctivas adecuadas.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si aplica, la forma de proceder para aplicar las mejoras.

- Asegurarse que las mejoras introducidas alcanzan los objetivos definidos y enmarcados dentro del alcance del SGSI.

2.7 RESOLUCIÓN JB-2014-3066

El organismo de control ha definido mediante la Junta Bancaria el dos de septiembre del 2014 la resolución JB-2014-3066, la cual actualiza disposiciones emitidas en el titulo X “De la gestión integral y control de riesgo”, del libro I “Normas generales para la aplicación de la Ley General de Instituciones del Sistema Financiero”, de la Codificación de Resoluciones de la Superintendencia de Bancos [3] y de la Junta Bancaria, consta el capítulo V “De la gestión de riesgo operativo”.

La resolución actualiza determina las disposiciones relacionadas la seguridad de la información basada en riesgos. La norma contiene una serie de disposiciones específicas para la implementación de medidas de seguridad en los diferentes canales electrónicos, mediante los cuales brindan servicios financieros a sus clientes. Con el propósito de que las instituciones financieras incrementen las medidas de seguridad en los canales electrónicos, y mejoren la gestión de la tecnología de la información y comunicación. Se incluyen disposiciones específicas relativas a la continuidad de las operaciones del negocio, implementar las medidas de seguridad para mitigar los fraudes en cajeros automáticos y

determinar los causales de los mismos.

2.7.1 Estructura De La Resolución

La resolución actualiza determinadas disposiciones relacionadas la seguridad de la información basada en riesgos, correspondiente a la "Sección VII-Seguridad de la Información", de la cual se desprenden dos artículos específicos de la norma emitida por el organismo de control, las cuales se describen a continuación:

Artículo 21 indica: *"Con el objeto de gestionar la seguridad de la información para satisfacer las necesidades de la entidad y salvaguardar la información contra el uso, revelación y modificación no autorizados, así como daños y pérdidas, las instituciones controladas deben tener como referencia la serie de estándares ISO/IEC 27000 o la que la sustituya y deben al menos:"*

Artículo 22 indica: "Las instituciones deben establecer, implementar, ejecutar, monitorear, mantener y documentar un sistema de gestión de seguridad de la información que considere al menos lo siguiente:"

Cada artículo consta de ítems de cumplimiento, que se pueden observar el "Capítulo V.- De la gestión del riesgo operativo; título X.- De la gestión y administración de riesgos, del libro i.- Normas generales para las instituciones del sistema financiero"

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN

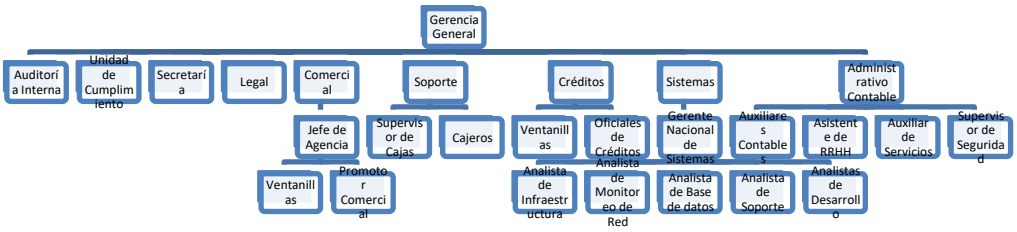
3.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

En esta sección se describirá la situación actual de las principales áreas relacionadas a los procesos de gestión de usuarios y del monitoreo de la seguridad informática.

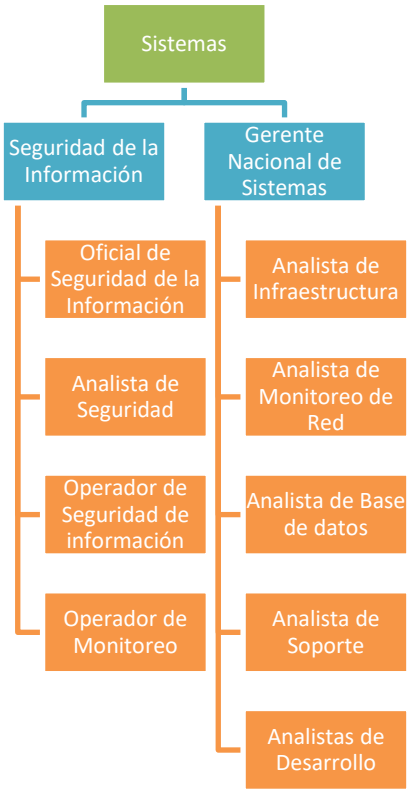
3.1.1 Estructura De La Resolución

La información de los roles e integrantes de las áreas de Sistemas y de Seguridad, ha sido proporcionada por el área de Recursos Humanos y las responsabilidades fueron emitidas por las gerencias de las áreas.

3.1.2 Organigrama General De La Empresa



3.1.3 Organigrama Del Departamento De Sistemas Y De Seguridad De La Información



3.2 ROLES Y RESPONSABILIDADES

En esta sección, se expondrán los roles y responsabilidades de los integrantes de los departamentos de Sistemas y de Seguridad de la Información, la cual será un insumo para el análisis de la situación actual de las dos áreas principales relacionadas a los procesos definidos en el alcance del proyecto.

3.2.1 Departamento De Sistemas

El área de Sistemas es gestionada por el Gerente Nacional de Sistemas y su estructura actual respecto a recurso humano es:

Analista de Infraestructura: Responsable de la administración de los recursos de infraestructura tecnológica del hardware y software a nivel de servidores y equipos centralizados, desempeñado por una persona

Analista de Monitoreo de red: Responsable del monitoreo y velar por el funcionamiento adecuado de la red local y de las agencias, desempeñado por una persona

Analista de Base de datos: Responsable de la administración de las bases de datos institucionales y de los respaldos, desempeñado por una persona.

Analista de Soporte: Responsable del soporte al usuario final, en hardware, software, uso adecuado del computador, desempeñado por tres personas.

Analista de Desarrollo: Responsable del soporte de los requerimientos del software desarrollado en casa y de la coordinación con empresas externas para las adecuaciones del software de terceros, desempeñado por cuatro personas.

3.2.2 Departamento de seguridad de la información

El área de seguridad informática es administrada actualmente por la Oficial de Seguridad de la Información, la cual posee actualmente la siguiente estructura en cuanto a su recurso humano:

Oficial de Seguridad de la Información: Responsable máximo en la planificación, desarrollo, control y gestión de las políticas y procedimientos con el objetivo de mejorar la seguridad de la información. Sus pilares principales son: la confidencialidad, integridad y disponibilidad de los datos.

Analista de Seguridad: Responsable de la gestión de permisos en el firewall, atención a requerimientos de seguridad en base de datos y complementa la gestión de usuarios, desempeñado por

una persona.

Operador de Seguridad de la Información: Responsable de creación, modificación, eliminación de usuarios y perfiles en todos los aplicativos de la institución, desempeñado por una persona.

Operador de monitoreo: Responsable del monitoreo de las herramientas de seguridad, desempeñado por una persona.

3.3 FLUJO DE PROCESOS

En esta sección se describe la interacción entre las áreas durante los procesos del alcance del proyecto, le empresa no ha establecido un flujo de procesos

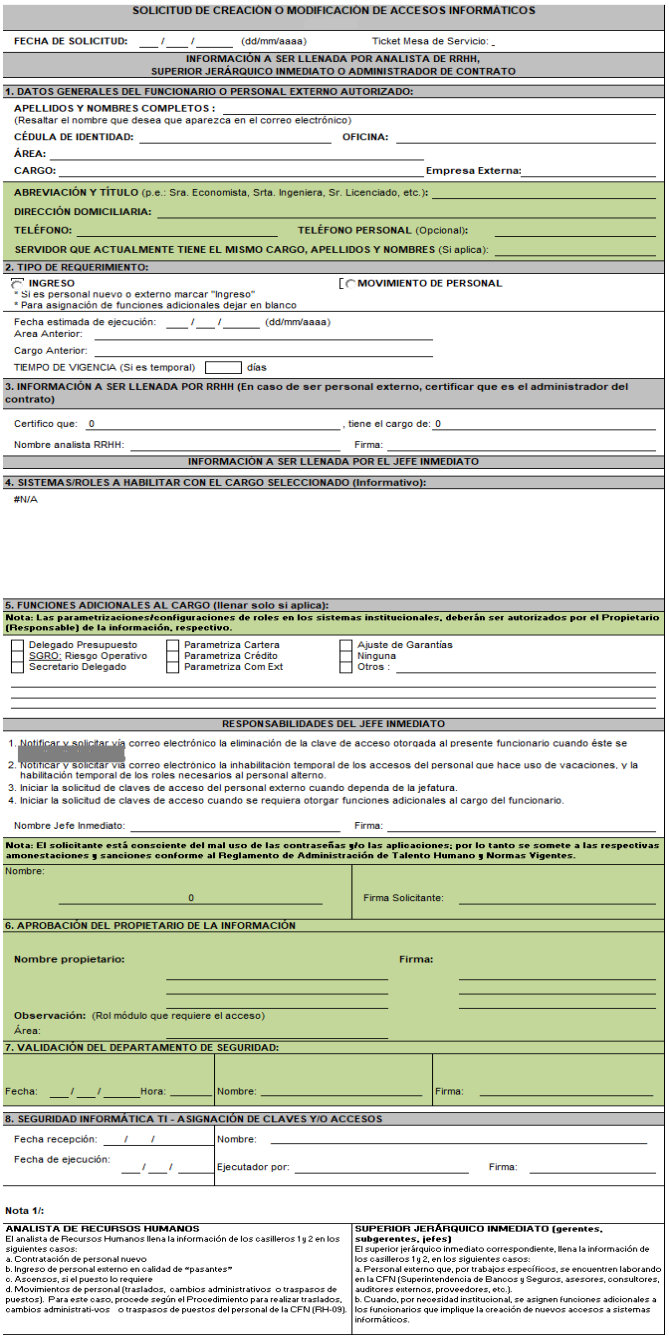
3.3.1 Gestión De Usuarios En Los Sistemas.

La creación/modificación/eliminación de usuarios en los aplicativos de la institución, inicia por medio de la llegada de un correo electrónico de autorización por parte del área de Recursos Humanos hacia el área de Seguridad de la Información, el correo se describe los datos para la creación del usuario, los aplicativos en los cuales se solicita acceso, el perfil, etc.

La modificación de perfiles, es autorizada por medio de correo

electrónico por un comité el cual está conformado por: el Contador General y Gerente Nacional de Operaciones para ser finalmente implementada por el área de Seguridad.

Realizada la creación, modificación, eliminación de los usuarios, el área de Seguridad de la Información, procede a remitir respuesta de lo realizado por correo electrónico al inmediato superior del usuario que fue creado. *(Ver Figura 3.1)*



SOLICITUD DE CREACIÓN O MODIFICACIÓN DE ACCESOS INFORMÁTICOS

FECHA DE SOLICITUD: ___ / ___ / _____ (dd/mm/aaaa) Ticket Mesa de Servicio: _

INFORMACIÓN A SER LLENADA POR ANALISTA DE RRHH, SUPERIOR JERÁRQUICO INMEDIATO O ADMINISTRADOR DE CONTRATO

1. DATOS GENERALES DEL FUNCIONARIO O PERSONAL EXTERNO AUTORIZADO:

APELLIDOS Y NOMBRES COMPLETOS :
(Resaltar el nombre que desea que aparezca en el correo electrónico)

CÉDULA DE IDENTIDAD: **OFICINA:**

ÁREA:

CARGO: **Empresa Externa:**

ABREVIACIÓN Y TÍTULO (p.e.: Sra. Economista, Srta. Ingeniera, Sr. Licenciado, etc.):

DIRECCIÓN DOMICILIARIA:

TELÉFONO: **TELÉFONO PERSONAL** (Opcional):

SERVIDOR QUE ACTUALMENTE TIENE EL MISMO CARGO, APELLIDOS Y NOMBRES (Si aplica):

2. TIPO DE REQUERIMIENTO:

INGRESO [**MOVIMIENTO DE PERSONAL**
* Si es personal nuevo o externo marcar "Ingreso"
* Para asignación de funciones adicionales dejar en blanco

Fecha estimada de ejecución: ___ / ___ / _____ (dd/mm/aaaa)
Area Anterior:

Cargo Anterior:

TIEMPO DE VIGENCIA (Si es temporal) [ ] días

3. INFORMACIÓN A SER LLENADA POR RRHH (En caso de ser personal externo, certificar que es el administrador del contrato)

Certifico que: 0 , tiene el cargo de: 0

Nombre analista RRHH: Firma:

INFORMACIÓN A SER LLENADA POR EL JEFE INMEDIATO

4. SISTEMAS/ROLES A HABILITAR CON EL CARGO SELECCIONADO (Informativo):

#N/A

5. FUNCIONES ADICIONALES AL CARGO (llenar solo si aplica):

Nota: Las parametrizaciones/configuraciones de roles en los sistemas institucionales, deberán ser autorizados por el Propietario (Responsable) de la información, respectivo.

[ ] Delegado Presupuesto
[ ] SGRO: Riesgo Operativo
[ ] Secretario Delegado
[ ] Parametriza Cartera
[ ] Parametriza Crédito
[ ] Parametriza Com Ext
[ ] Ajuste de Garantías
[ ] Ninguna
[ ] Otros :

RESPONSABILIDADES DEL JEFE INMEDIATO

1. Notificar y solicitar vía correo electrónico la eliminación de la clave de acceso otorgada al presente funcionario cuando éste se
2. Notificar y solicitar vía correo electrónico la inhabilitación temporal de los accesos del personal que hace uso de vacaciones, y la habilitación temporal de los roles necesarios al personal alterno.
3. Iniciar la solicitud de claves de acceso del personal externo cuando dependa de la jefatura.
4. Iniciar la solicitud de claves de acceso cuando se requiera otorgar funciones adicionales al cargo del funcionario.

Nombre Jefe Inmediato: Firma:

Nota: El solicitante está consciente del mal uso de las contraseñas y/o las aplicaciones; por lo tanto se somete a las respectivas amonestaciones y sanciones conforme al Reglamento de Administración de Talento Humano y Normas Vigentes.

Nombre: 0 Firma Solicitante:

6. APROBACIÓN DEL PROPIETARIO DE LA INFORMACIÓN

Nombre propietario: **Firma:**

Observación: (Rol módulo que requiere el acceso)
Área:

7. VALIDACIÓN DEL DEPARTAMENTO DE SEGURIDAD:

Fecha: ___ / ___ / _____ Hora: _____ Nombre: Firma:

8. SEGURIDAD INFORMÁTICA TI - ASIGNACIÓN DE CLAVES Y/O ACCESOS

Fecha recepción: ___ / ___ / Nombre:

Fecha de ejecución: ___ / ___ / ____ Ejecutador por: Firma:

Nota 1/:

ANALISTA DE RECURSOS HUMANOS
El analista de Recursos Humanos llena la información de los casilleros 1 y 2 en los siguientes casos:
a. Contratación de personal nuevo
b. Ingreso de personal externo en calidad de "pasantes"
c. Ascensos, si el puesto lo requiere
d. Movimientos de personal (traslados, cambios administrativos o traspasos de puestos). Para este caso, procede según el Procedimiento para realizar traslados, cambios administrati-vos o traspasos de puestos del personal de la CFN (RH-09).

SUPERIOR JERÁRQUICO INMEDIATO (gerentes, subgerentes, jefes)
El superior jerárquico inmediato correspondiente, llena la información de los casilleros 1 y 2, en los siguientes casos:
a. Personal externo que, por trabajos específicos, se encuentren laborando en la CFN (Superintendencia de Bancos y Seguros, asesores, consultores, auditores externos, proveedores, etc.).
b. Cuando, por necesidad institucional, se asignen funciones adicionales a los funcionarios que implique la creación de nuevos accesos a sistemas informáticos.

Figura 3.17.- Formulario de Solicitud o Creación Accesos Informáticos

Fuente: Documento de la Institución

3.3.2 Gestión De Monitoreo De La Seguridad Informática

El monitoreo de la seguridad informática se está realizando por medio de la revisión de los logs del correlacionador de eventos CA Spectrum y de los reportes generados por la herramienta al ejecutar el monitoreo en el caso de detectarse alguna actividad sospechosa, reporta inmediatamente a la Oficial de Seguridad de la Información para su investigación, clasificación en amenaza real o falso positivo y su remediación. *(Ver Figura 3.2, 3.3 ,3.4 y 3.5)*

SPECTRUM

Reporte de Disponibilidad Mensual

Reporte de Disponibilidad Mensual de dispositivos de GC GRP Disponibilidad

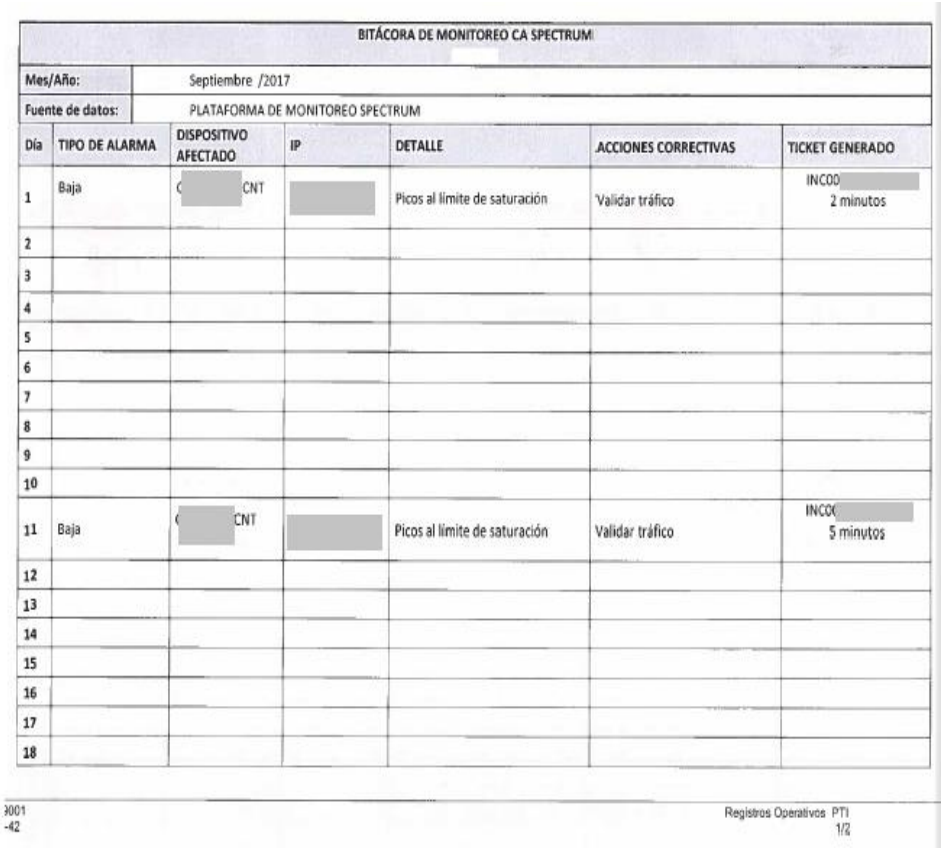
Report Period:	viernes 01 de septiembre de 2017 0:00:00 to domingo 01 de octubre de 2017 0:00:00
Global Collection Name:	Disponibilidad
Availability Target:	99,600%
Number of Managed Assets:	85
Actual Availability For Group:	99,818%
Types of Outages Contributing to Downtime:	Unplanned
Business Day Policy:	Business Day excluding Weekends
Business Day Hours:	8:00:00 to 17:00:00

Reporte de Disponibilidad Men

Name	Model Type	Total Downtime	Number of Outages	Availability
SRV01 LOCAL	Host_Device	0 Days + 01:58:30	2	98,955 %
MSRV01 LOCAL	Host_Device	0 Days + 01:57:40	2	98,962 %
CSRV01 LOCAL	Host_Device	0 Days + 01:56:19	2	98,974 %
SRV01 LOCAL	Host_Device	0 Days + 01:55:25	2	98,982 %
SRV01 LOCAL	Host_Device	0 Days + 01:52:50	2	99,005 %

Figura 3.2 .- Reporte de Disponibilidad Mensual de dispositivos CA Spectrum

Fuente: Informe Técnico de Infraestructura



BITÁCORA DE MONITOREO CA SPECTRUM

Mes/Año:	Septiembre /2017
Fuente de datos:	PLATAFORMA DE MONITOREO SPECTRUM

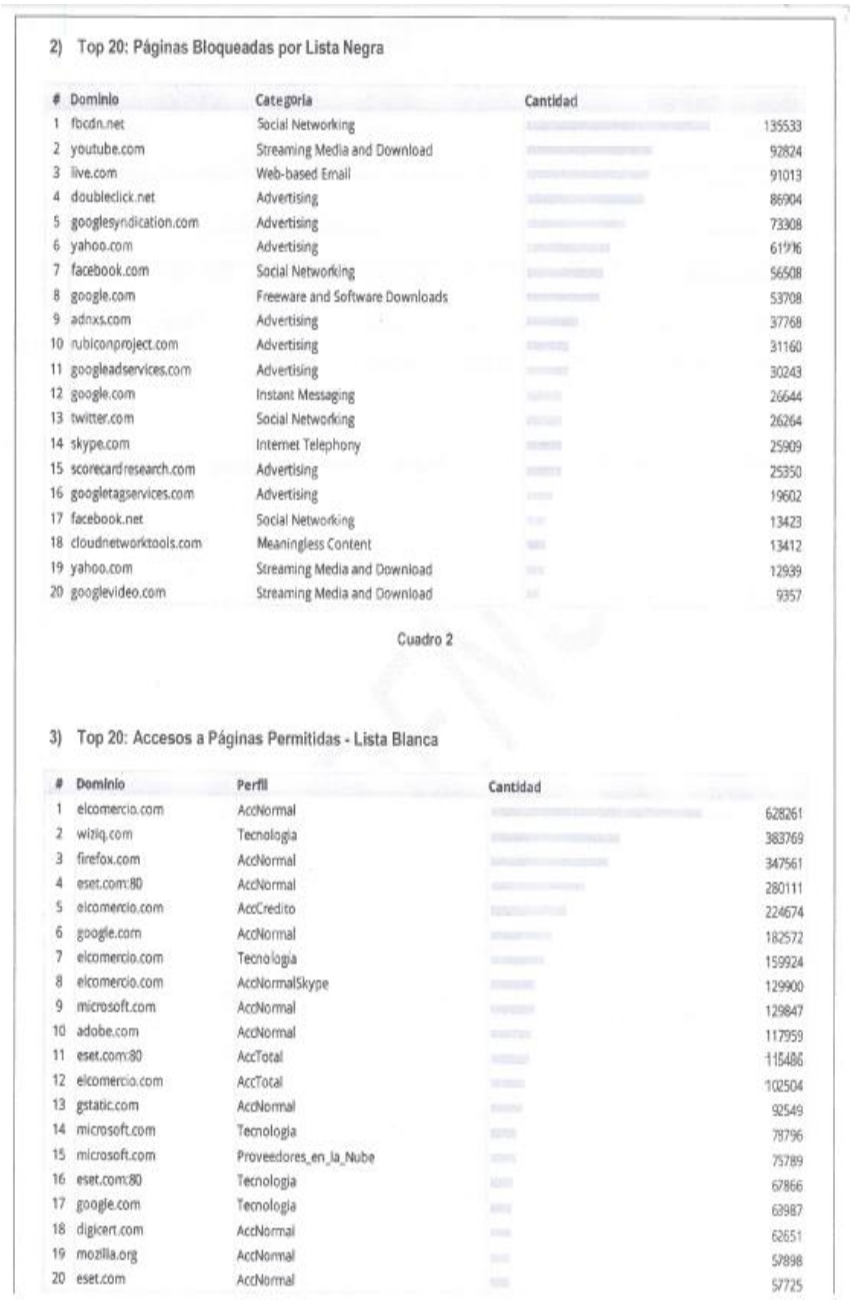
Día	TIPO DE ALARMA	DISPOSITIVO AFECTADO	IP	DETALLE	ACCIONES CORRECTIVAS	TICKET GENERADO
1	Baja	CNT		Picos al límite de saturación	Validar tráfico	INC00 2 minutos
2						
3						
4						
5						
6						
7						
8						
9						
10						
11	Baja	CNT		Picos al límite de saturación	Validar tráfico	INC0 5 minutos
12						
13						
14						
15						
16						
17						
18						

9001
-42

Registros Operativos PTI
1/2

Figura 3.3 .- Reporte de Disponibilidad Mensual de dispositivos CA Spectrum

Fuente: Informe Técnico de Infraestructura



2) Top 20: Páginas Bloqueadas por Lista Negra

#	Dominio	Categoria	Cantidad
1	fbcdn.net	Social Networking	135533
2	youtube.com	Streaming Media and Download	92824
3	live.com	Web-based Email	91013
4	doubleclick.net	Advertising	86904
5	googlesyndication.com	Advertising	73308
6	yahoo.com	Advertising	61916
7	facebook.com	Social Networking	56508
8	google.com	Freeware and Software Downloads	53708
9	adnxs.com	Advertising	37768
10	rubiconproject.com	Advertising	31160
11	googleadservices.com	Advertising	30243
12	google.com	Instant Messaging	26644
13	twitter.com	Social Networking	26264
14	skype.com	Internet Telephony	25909
15	scorecardresearch.com	Advertising	25350
16	googletagservices.com	Advertising	19602
17	facebook.net	Social Networking	13423
18	cloudnetworktools.com	Meaningless Content	13412
19	yahoo.com	Streaming Media and Download	12939
20	googlevideo.com	Streaming Media and Download	9357

Cuadro 2

3) Top 20: Accesos a Páginas Permitidas - Lista Blanca

#	Dominio	Perfil	Cantidad
1	elcomercio.com	AccNormal	628261
2	wiziq.com	Tecnologia	383769
3	firefox.com	AccNormal	347561
4	eset.com:80	AccNormal	280111
5	elcomercio.com	AccCredito	224674
6	google.com	AccNormal	182572
7	elcomercio.com	Tecnologia	159924
8	elcomercio.com	AccNormalSkype	129900
9	microsoft.com	AccNormal	129847
10	adobe.com	AccNormal	117959
11	eset.com:80	AccTotal	115486
12	elcomercio.com	AccTotal	102504
13	gstatic.com	AccNormal	92549
14	microsoft.com	Tecnologia	78796
15	microsoft.com	Proveedores_en_la_Nube	75789
16	eset.com:80	Tecnologia	67866
17	google.com	Tecnologia	63987
18	digicert.com	AccNormal	62651
19	mozilla.org	AccNormal	57898
20	eset.com	AccNormal	57725

Figura 3.4 - Listado De Páginas bloqueadas

Fuente: Informe Técnico de Infraestructura

5) Top 30: Usuarios con Mayor Consumo de Ancho de Banda

#	Oirgen	Usuario	Grupo	Ancho de Banda	Trafico de Salida	Trafico de Entrada
1	10. 57	eg na	G	-Tecnologia		45.64 GB
2	10. 13	ach a	G	-Tecnologia		16.52 GB
3	10. 87	rbr	G	-Proveedored_en_la_Nube		16.24 GB
4	10. 151	rm	G	-AccPublicidad		11.33 GB
5	19. .66	erc	G	-AccNormal		10.88 GB
6	10. 122	gar z	G	-AccNormal		10.61 GB
7	10. 171	ece s	G	-Tecnologia		9.25 GB
8	10. 93	cgo	G	-Tecnologia		9.00 GB
9	10. 2	rp	G	-Tecnologia		8.73 GB
10	10. 15	xrl	G	-Tecnologia		8.25 GB
11	10. 216	jm	G	-AccPublicidad		6.64 GB
12	19. .55	sb	G	-AccNormal		6.24 GB
13	19. .57	fca	G	-AccTotsinCorreo		6.09 GB
14	10. 178	EP O	G	-AccNormal		5.43 GB
15	10. 102	fn	G	-AccTotal		5.31 GB
16	10. 188	jqu s	G	-Proveedored_en_la_Nube		5.28 GB
17	10. 202	fca	G	-Tecnologia		5.05 GB
18	10. 158	mc	G	-Proveedored_en_la_Nube		4.80 GB
19	10. 127	jlo	G	-Tecnologia		4.20 GB
20	10. 57	ag	G	-Tecnologia		4.15 GB
21	10. 66	jja	G	-Tecnologia		4.10 GB
22	10. 62	gja	G	-Tecnologia		4.10 GB
23	10. 251	epi	G	-AccPublicidad		3.77 GB
24	10. 198	ag	G	-Tecnologia		3.58 GB
25	10. 162	rat	G	-AccNormal		3.53 GB
26	10. 88	ag	G	-Tecnologia		3.48 GB
27	10. 131	jor	G	-Tecnologia		3.44 GB
28	10. 123	om z	G	-AccTransporte		3.37 GB
29	10. 167	mc	G	-Proveedored_en_la_Nube		3.26 GB
30	10. 71	mc	G	-Proveedored_en_la_Nube		3.24 GB

Cuadro 4

Figura 3.5 - Usuarios con mayor consumo de ancho de banda

Fuente: Informe Técnico de Infraestructura

3.4 ARQUITECTURA DE TECNOLOGÍA DE LA INSTITUCIÓN

3.4.1 Ubicación Física

La institución opera en un Edificio propio, ubicado en el norte de la ciudad de Guayaquil, con vigilancia las 24 horas del día.

El edificio posee cuatro pisos, distribuidos por áreas, tal como se describe a continuación: En la planta baja funcionan las áreas de Caja, en el primer piso se encuentra el área de Jurídico, Créditos, Administrativa, Cámara y de Recursos Humanos, en el segundo piso, se encuentra el área de Sistemas y de Seguridad de la Información, en el tercer piso se encuentra la Gerencia General.

Respecto a la disposición física de los servidores de la institución, estos se encuentran ubicados en el tercer piso del edificio, contiguo al área de Sistemas.

El cableado de red es estructurado categoría 5e, lo que facilita la administración física de la red, contando con un generador propia de energía eléctrica para estos equipos.

3.4.2 Estructura De La Red Lan

La red de la matriz, dispone de 12 servidores principales, 55 estaciones de trabajo de las cuales 4 son clones y 8 equipos de marcas, como se muestra en la Figura 3.6.

En el centro de datos, se dispone de:

- 4 Switch Cisco de 48 puertos, de los cuales actualmente se encuentran 18 puertos disponibles.
- 2 Switch Cisco de 16 puertos, de los cuales se encuentran 14

puertos en uso.

- En la planta baja se tiene:
- 1 Switch Cisco de 48 puertos, de los cuales 35 se encuentran utilizados.
- En el piso uno, se tiene:
- 1 Switch Cisco de 48 puertos, de los cuales 30 se encuentran utilizados.
- En el piso dos, se tiene:
- 2 Switch Cisco de 48 puertos, de los cuales 64 se encuentran utilizados.
- En el piso tres se tienen:
- 1 Switch Cisco de 48 puertos, de los cuales 14 puertos se encuentran utilizados.
- 1 Acces Point

La tasa de transmisión en la red es de 10 /100 Megabits por segundo.

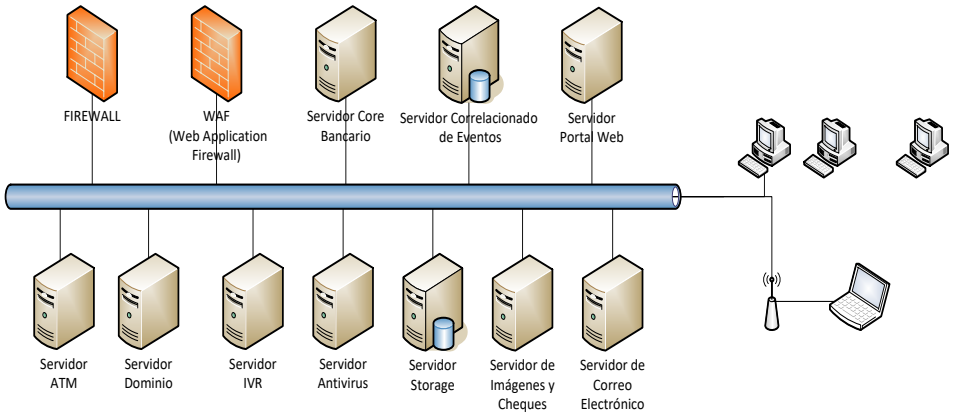


Figura 3.6 .- Diagrama Lan de la Red A1

Fuente: Creación Propia

3.4.3 Datos de los servidores/equipos principales

A continuación, se detallan los doce servidores principales con los que cuenta la matriz de la institución.

Correlacionado de eventos: Utiliza como base de datos el software Sql Server 2005 SE, levantado sobre un sistema operativo RHEL 4, usado principalmente por el área de Seguridad para el monitoreo.

WAF: Firewall de aplicaciones web, herramienta para prevención automática y de ser el caso manual de ataques web externos/internos, utilizada por el área de Seguridad.

Firewall: Cortafuegos interno/externo, herramienta para la administración de los filtros a nivel de puertos y de ips del tráfico de entrada/salida de la red local y de las agencias, utilizada por el área

de Seguridad.

Core Bancario: Equipo central en donde reside y opera el software base para la continuidad de las operaciones de la institución, está basado en la arquitectura de IBM, es utilizado por todos.

Storage: Equipo en el cual se encuentra disponibles los respaldos de las bases de datos e información de usuarios críticos, su sistema operativo es *Windows Server Storage 2003* utilizado por el área de sistemas y de seguridad.

Imágenes y Cheques: Equipo en el cual se encuentra el software para la gestión de cheques y su respaldo, el cual reside en un sistema operativo *Windows Server 2003 R2* y utiliza la base de datos *Sql Server 2005,* utilizado por el área de Cámara.

Portal Web: Equipo en el cual se encuentra el software para el aplicativo web institucional que utilizan los clientes para realizar sus transacciones, reside en un sistema operativo *Windows Server 2008 R2.*

Servidor ATM: Equipo en el cual se encuentra el software que gestiona las operaciones de los cajeros automáticos y se encuentra residente en el sistema operativo *Windows Server 2008 R2.*

Servidor de Correo Electrónico: Equipo en el cual se encuentra el

gestor de correo electrónico institucional basado en tecnología Microsoft Exchange y se encuentra residente en el sistema operativo Windows server 2008 r2.

Servidor Central de Llamada: Equipo IVR (interactive voice response) el cual es el gestor de llamadas telefónicas institucional cuando los clientes necesitan conocer los saldos de sus cuentas y se encuentra residente en el sistema operativo Windows server 2003 r2.

Servidor Antivirus: Equipo en el cual se encuentra la consola administradora del antivirus F-secure, y se encuentra residente en el sistema operativo Windows server 2003 r2.

Servidor de Dominio: Para el servicio de Dominio se utiliza el Directorio activo, bajo un sistema operativo Windows 2003 Server R2.

Respecto a las instalaciones de parches de seguridad en los servidores, no se dispone de un procedimiento aprobado respecto a las actualizaciones y mantenimiento del software utilizado en la institución.

3.4.3.1 Datos de las estaciones de trabajo

Las estaciones de trabajo disponen de sistema operativo Windows *Xp Sp3*, el antivirus *F-Secure* así como Microsoft *Office 2010 Profesional*, utilizan como navegador Web *Mozilla Firefox 34*,

tienen instalado además *Acrobat Reader*.

A continuación, se detallan las características de los equipos:

Tabla 7

Características de los Equipos de Cómputos de Desktops

Cpu	HP 6300 Pro sff	
Procesador	Intel Core 2 Duo	Core i5
Disco Duro	320 GB	500 GB
Memoria	3 GB	4 GB
Sistema Operativo	Windows XP Professional con Service Pack 3	

Fuente: Creación Propia

Tabla 8

Características de las computadoras portátiles HP Probook

CPU	5 portátiles HP Probook4430s	
Procesador	Core i5	2.5 Ghz
Disco Duro	500 GB	
Memoria	4 GB	
Sistema Operativo	Windows 7 Professional SP1	

Fuente: Creación Propia

Adicionalmente se encuentran disponibles en la red 15 impresoras. Actualmente no se dispone de alguna implementación ni de sistemas de gestión que permitan una administración de red. Es suma, no se cuenta con herramienta de software ni hardware que permita el monitoreo de la red y el análisis de vulnerabilidades.

3.4.3.2 Estructura de la red Wan

Se cuenta con tres enlaces: un enlace a Internet, otro enlace para datos (conectividad desde y hacia otras agencias con la matriz) y un enlace de comunicación con Banred para los cajeros automático y sus respectivos respaldos contratado con un proveedor externo (*Ver Figura* 3.7).

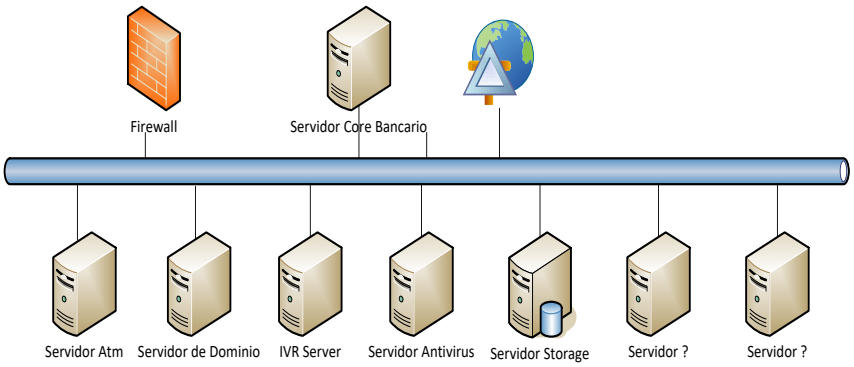


Figura 3.713 .- Diagrama Wan de la red (Imagen A.2)

Fuente: Creación Propia

3.5 SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADA

Para establecer una visión de la seguridad actual de la seguridad en la organización, se realizó un análisis para determinar los controles sean estos automáticos o manuales que están operativos en la institución.

3.5.1 Gestión De Usuarios En Los Sistemas

La gestión de usuarios tiene controles básicos manuales que se pudieron evidenciar, como son:

- Uso de un procedimiento basado en el expertise del Oficial de Seguridad de la Información, aunque no está formalizado.
- Se evidencio la presencia de un formulario para la solicitud de la creación/modificación de usuarios. (Ver Anexo 1).
- Existen varios departamentos que intervienen en el proceso.

3.5.2 Gestión De Monitoreo De La Seguridad Informática.

La gestión de monitoreo tiene controles básicos manuales que se pudieron evidenciar, tales como:

- Presencia de 6 herramientas relacionadas al monitoreo como son: Correlacionador de eventos, waf, firewall, core bancario (módulo de seguridad), consola antivirus y servidor de dominio.
- Todos los aplicativos tienen activos los logs de seguridad.

- Respaldos de logs en el storage.
- Uso de un procedimiento basado en el expertise del Oficial de Seguridad de la Información, aunque no está formalizado para el monitoreo.
- Monitoreo de parte del operador por 8 horas cada día laborable.

CAPITULO 4
ANÁLISIS Y DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

4.1 ESQUEMA DOCUMENTAL

4.1.1 Definición Del Alcance Del SGSI

El SGSI debe ser aplicado en todos los activos de información, en sus las plataformas tecnológicas y en sus procesos. El alcance del trabajo es identificar los controles de seguridad necesarios y si éstos se encuentran operando. Queda por parte de la institución realizar la implementación de los controles identificados.

4.1.2 Política De Seguridad De La Información

Es la normativa interna que debe conocer y cumplir todo el personal

involucrado directa o indirectamente por el alcance del Sistema de Gestión de Seguridad de la Información, el contenido de la política debe definir lineamientos globales que serán detallados en normas y políticas de segundo y tercer nivel descritos en el documento.

4.1.3 Procedimiento De Gestión De Usuarios En Los Sistemas

El procedimiento descrito, está basado en la operatividad empírica de la institución, la cual se describe a continuación: Cada usuario que tenga acceso a la red, requiere de una cuenta de usuario y contraseña. La cuenta de usuario permite las siguientes acciones: autentica la identidad de la persona que se conecta a la red, controla el acceso a los recursos del dominio, audita todas las acciones que son realizadas por la cuenta de usuario.

4.1.4 Procedimiento De Monitoreo De La Seguridad Informática

El procedimiento descrito, está basado en la operatividad empírica de la institución, la cual se describe a continuación: Cualquier sistema puede verse comprometido por un intruso, el sistema registra logs de auditoría constantemente.
El procedimiento de monitoreo radica en la identificación de cualquier evento imprevisto en el sistema. Entre menos tiempo haya pasado desde la identificación de intrusión, el daño será menor; es importante tener un monitoreo constante de los logs del sistema para

detectar cualquier intrusión a la seguridad de la información.

4.1.5 Declaración De Aplicabilidad

La Declaración de Aplicabilidad se desarrollará después del tratamiento que se darán a los riesgos, actividad posterior a la evaluación de riesgos.

El tratamiento tiene como objetivo la definición de las acciones a realizar para mitigar aquellos riesgos que han sido seleccionados por la institución para su implementación.

Definidas las opciones de tratamiento de los riesgos, la institución debe aplicar medidas de seguridad, es decir, desarrollando un SOA basado en el cumplimiento regulatorio (tabla 20), el documento donde se registran los controles de seguridad que son aplicables (necesarios) y si éstos se encuentran operando o todavía, lo cual se describirá a detalle en la sección 4.2.

4.2 IDENTIFICACIÓN, ANÁLISIS Y EVALUACIÓN DE RIESGOS

En esta sección se identificarán los activos de la institución y se realizará la valoración de estos activos y de los riesgos asociados en los procesos definidos en el alcance del proyecto.

4.2.1 Selección Del Método De Análisis De Riesgos

Se optó por: “Guías para la administración de seguridad de IT” (Furnell, 2005) [4] el cual provee un análisis detallado, considerando que este método ayuda a cumplir nuestro objetivo, el cual es seleccionar controles adecuados para minimizar los evento de riesgos, es suma se ajusta a los requerimientos de la norma ISO 27001.

4.2.2 Identificación De Activos.

Con el objeto de la identificación de los activos, se tomó como referencia los datos proporcionados por los dueños de los procesos, y para facilitar el análisis y gestión de riesgos se han dividido los activos en nueve categorías de información, a continuación, se detalla cada una de las 9 categorías (Véase Tabla 9):

Tabla 9

Categoría de Activos	
Tipo	Alcance
[S] Servicios	Servicios auxiliares que se necesitan para poder organizar las operaciones
[SW] Software	Aplicaciones informáticas
[D] Documentos	Soporte no electrónico que contiene datos

[HW] Hardware	Equipos físicos donde operan las aplicaciones y residen los datos
[M] Soportes	Los soportes de información que son dispositivos de almacenamientos de datos
[AUX] Equipamiento Auxiliar	El equipamiento auxiliar que complementa los medios informáticos
[COM] Comunicaciones Redes	Las redes de comunicaciones que permiten intercambiar información
[I] Instalaciones	Las instalaciones que acogen los equipos de sistemas
[P] Personal	Personas que operan todos los elementos anteriormente citados

Fuente: Creación Propia

Los activos relevantes que se obtuvieron del levantamiento y que serán los considerados para la valoración, fueron los siguientes (Véase Tabla 10):

Tabla 10

Listado de Activos Relevantes

Ítem	CODIGO	ACTIVO
1	AUX1	Equipos de aire acondicionado centro datos
2	AUX2	Equipos contra incendios del centro de datos
3	AUX3	Energía Eléctrica
4	AUX4	Equipos de UPS de centro de datos
5	AUX5	Cableado

Tabla 10

Listado de Activos Relevantes

6	COM1	Red Telefónica
7	COM2	Red LAN
8	COM3	Red WAN
9	D1	Contrato de proveedores
10	D2	Documentación de procesos
11	HW1	Servidor
12	HW2	Computador de escritorio
13	HW3	Computador portátil
14	HW4	Impresoras
15	HW5	Equipos de red
16	HW6	Equipos de monitoreo
17	L1	Edificio
18	M1	Cintas de respaldos
19	P1	Usuarios externos
20	P2	Usuarios internos
21	P3	Operadores de Monitoreo
22	P4	Operadores de Infraestructura
23	P5	Proveedores
24	S1	Canal de Internet
25	S2	Repositorio de Archivos
26	S3	Web Institucional
27	S4	Correo electrónico

Tabla 10

Listado de Activos Relevantes

28	SW1	Aplicativo de Ofimática
29	SW2	Sistema de gestión de base de datos
30	SW3	Sistemas operativos
31	SW4	Sistema de gestión de respaldos
32	SW5	Sistema de monitoreo de seguridad informática

Fuente: Creación Propia

4.2.3 Valoración De Activos.

Para la valoración de activos se utilizó la siguiente tabla simple que fue basada en una estimación monetaria del valor de los activos que es percibida por la institución *(Véase Tabla 11):*

Tabla 11

Valoración de Activos

	Valor	Código	Descripción
Valoración de los activos ($ miles)	mayor que 100	A	Alto
	entre 100 y 50	M	Medio
	menor que 50	B	Bajo

Fuente: Creación Propia

4.2.4 Dimensiones De La Seguridad.

Se hará la valoración de todos los activos que estén dentro del alcance del SGSI [8], indicando el impacto que puede sufrir el negocio con la pérdida de las siguientes dimensiones: confidencialidad, integridad, disponibilidad y trazabilidad.

La obtención de la valoración, fue realizada por el personal encargado de cada proceso, los cuales conocen la importancia de cada activo dentro de la institución. (Véase Tabla 12).

Tabla 12

Dimensiones de la valoración	
[C] Confidencialidad	La información no se pone a disposición de personas no autorizadas
[I] Integridad	Activo no ha sido alterado de forma no autorizada
[D] Disponibilidad	Activo está disponible para los procesos autorizados cuando lo requieran.
[T] Trazabilidad	Las acciones de una entidad puedan ser imputadas a dicha entidad

Fuente: Creación Propia

A continuación, se presenta la tabla de valoración de activos del

proceso (Véase Tabla 13):

Tabla 13

Activos del Proceso

Activos	Dimensión de Seguridad	Valor	Razón
Computador Portátil	Confidencialidad	3	La información debe estar disponible solo por el personal autorizado.
	Integridad	3	Es necesaria la integridad de la información, en especial la de clientes, informes de parametrizaciones de las herramientas de monitoreo.
	Disponibilidad	2	Para que los empleados puedan realizar sus labores, necesitan disponer de la información, sin embargo, existen documentos y servidores de respaldos.
	Trazabilidad	3	Los ubicación y pertenencia de los equipos necesita ser registrados en todo momento
Computador de Escritorio	Confidencialidad	3	La información debe estar disponible solo para el personal autorizado.

	Integridad	3	Es necesaria la integridad de la información almacenada, en especial la de clientes, informes de parametrizaciones de las herramientas de monitoreo.
	Disponibilidad	2	Para que los empleados puedan realizar sus labores, necesitan disponer de la información, sin embargo, existen documentos y servidores de respaldos.
	Trazabilidad	1	La ubicación y la pertenencia de los equipos por su naturaleza no necesitan ser registrados.
	Confidencialidad	4	Solo el personal autorizado debe acceder a la información de los servidores que almacenan información de clientes y parametrizaciones.
Servidores	Integridad	3	Se debe asegurar que la información de los servidores no sea modificada sin la debida autorización.
	Disponibilidad	3	Los servidores deben estar accesibles al menos todo la jornada laboral, para no afectar a los clientes Internos y externos.
	Trazabilidad	3	La ubicación y la pertenencia de los equipos necesitan ser

			registrados en todo momento.
Impresoras	Confidencialidad	4	Información del negocio operativa o de seguridad que se imprima o se fotocopie necesita ser confidencialidad.
	Integridad	2	Se necesitan estos equipos, pero si eventualmente falla se puede seguir trabajando.
	Disponibilidad	2	Si bien son necesarios los equipos, se puede trabajar, aunque no estén disponibles
	Trazabilidad	3	Es necesario conocer el origen y destino de las impresiones
Equipos de Red	Confidencialidad	4	La información que transita en estos equipos solo debe ser visualizada por los autorizados
	Integridad	3	Se necesita estos equipos, no sean manipuladas las configuraciones.
	Disponibilidad	3	La disponibilidad de estos equipos es alta de acuerdo al giro del negocio.
	Trazabilidad	?	Es necesario conocer el origen y destino del tráfico si estos equipos lo permiten.
Equipos de Monitoreo	Confidencialidad	4	La información de estos equipos debe ser accedida solo por personal debidamente autorizado

	Integridad	3	Es necesario asegurar que la información de los servidores no sea alterada ni modificada sin autorización.
	Disponibilidad	3	Es indispensable que los servidores estén accesibles y operando 24/7 para prevenir o detectar algún evento que afecte a la normalidad de las operaciones del negocio.
	Trazabilidad	?	Todo lo realizado en estos equipos debe ser trazable con el objeto de que sirvan como pistas o evidencias ante cualquier evento.
	Confidencialidad	3	Cuando se tenga información de negocio almacenada en estos equipos es necesaria su protección.
Cintas de Respaldo	Integridad	2	Es un medio temporal para almacenar Información
	Disponibilidad	1	No es requerido, cuando la información es Redundante
	Trazabilidad	3	Es importante conocer la cadena de custodia de los respaldos.
Contrato de Proveedores	Confidencialidad	3	En función de los acuerdos de servicios y confidencialidad, será útil tener esta información debidamente resguardada

	Integridad	2	Es necesario que la documentación no sea alterada, aunque si se produce perdida de la misma, se podría solicitar al proveedor una fiel copia del original.
	Disponibilidad	1	No es necesario acceder a la información en cualquier momento que sea requerido.
	Trazabilidad	1	La trazabilidad del documento es mínimamente requerida
	Confidencialidad	4	Es importante tener los procedimientos donde se
	Integridad	2	Es necesario que la documentación no sea alterada, aunque si se produce perdida de la misma, se podría solicitar una copia.
Procedimientos			
	Disponibilidad	3	Es importante tener la documentación de procesos críticos disponibles para cuando se requiera.
	Trazabilidad	1	La trazabilidad del documento es mínimamente requerida
	Confidencialidad	3	Determinada información debe ser gestionada al interior de la institución por lo cual no debe ser expuesta.
Usuarios Internos			
	Integridad	1	No aplicable a aspectos de integridad.
	Disponibilidad	2	Los empleados deben estar disponibles para resolver posibles

			problemas que se presenten
Usuarios Externos	Trazabilidad	1	No aplicable a aspectos de integridad.
	Confidencialidad	3	Determinada información debe ser gestionada al interior de la institución por lo cual no debe ser expuesta.
	Integridad	1	No hay aspectos de integridad relacionados con los empleados
	Disponibilidad	1	No depende de la institución
	Trazabilidad	2	Es necesario conocer desde donde estos usuarios realizaron sus accesos
	Confidencialidad	4	Cierta información debe ser manejada al interior de la institución por lo cual no debe ser divulgada.
Operadores de Monitoreo	Integridad	1	No hay aspectos de integridad relacionados con los empleados
	Disponibilidad	2	Los operadores deben encontrarse disponibles para cuando se requiera su presencia
	Trazabilidad	3	Es necesario conocer desde donde estos usuarios realizaron sus accesos
Operadores de Infraestructura	Confidencialidad	4	Cierta información debe ser manejada al interior de la institución por lo

			cual no debe ser divulgada.
	Integridad	1	No hay aspectos de integridad relacionados
	Disponibilidad	3	Los operadores deben encontrarse disponibles
	Trazabilidad	3	Es necesario conocer desde donde estos
	Confidencialidad	4	Cierta información debe ser manejada al interior de la institución por lo cual no debe ser divulgada.
Proveedores	Integridad	1	No hay aspectos de integridad relacionados con los empleados
	Disponibilidad	3	Los proveedores deben encontrarse disponibles para cuando se requiera su presencia
	Trazabilidad	3	Es necesario conocer desde donde estos usuarios realizaron sus accesos
Edificio	Confidencialidad	1	Es un edificio público
	Integridad	3	Se debe proteger la integridad física del edificio Matriz donde se encuentran los servidores
	Disponibilidad	1	Si no pueden acceder al edificio, se puede acceder remotamente a la aplicación del Sistema
	Trazabilidad	1	Mínimamente requerida
Canal de Internet	Integridad	2	Se necesita que los servicios de comunicaciones

			funcionen adecuadamente
	Disponibilidad	3	Se requiere que estén disponibles, debido
			a que son necesarias para las actualizaciones en especial las de seguridad
	Confidencialidad	2	Se debe proteger que las líneas no sean interceptadas.
	Trazabilidad	2	Es necesaria de forma referencial la trazabilidad de los sitios donde se conectan
	Integridad	2	Se necesita que los servicios de file server no sea manipulado por personal no autorizado.
	Disponibilidad	3	Se requiere que estén disponibles.
Repositorio de archivos			Es necesario para que los usuarios puedan acceder a su información histórica.
	Confidencialidad	4	Se debe proteger que solo las personas autorizadas tengan acceso al servicio.
	Trazabilidad	3	Se necesita que los servicios de file server sean auditables.
	Integridad	3	Se necesita que los servicios que se brinda
Web Institucional	Disponibilidad	3	Se requiere que estén disponibles, debido

			a que son necesarias para el consumo de los servicios por los clientes
	Confidencialidad	1	El sitio Web debe ser accesible por cualquier persona, en cualquier momento
	Trazabilidad	2	Es necesario conocer hacia donde se conecta la web institucional.
	Integridad	3	Es necesario que los correos electrónicos no
	Disponibilidad	1	La disponibilidad no es tan importante debido los respaldos que se disponen.
Correo electrónico	Confidencialidad	4	Se debe proteger para que el servicio solo esté disponible al personal autorizado
	Trazabilidad	3	Es necesario conocer el origen y destino de los correos.
	Confidencialidad	1	Este es un software estándar el cual no es
	Integridad	2	El software debe funcionar correctamente
Aplicación de Ofimática	Disponibilidad	2	El software debe estar disponible durante horas de trabajo, pero si hay un problema con un computador puede ser restaurado.
	Trazabilidad	1	No es necesaria la trazabilidad
	Confidencialidad	4	Alta confidencialidad porque maneja
Sistema de Gestión de Base de datos	Integridad	3	La aplicación debe mantener la integridad para evitar

			modificaciones en la información sensible
	Disponibilidad	3	Es importante tener siempre disponible la información de los usuarios, pero si no estuviera disponible en todo momento
	Trazabilidad	3	Relevante que se realice la trazabilidad sobre lo que se haga en este activo
	Confidencialidad	4	Los datos de los clientes, que es información personal procesada en el servidor,
	Integridad	3	Los datos de los clientes, que es información personal es procesada en el servidor, estos datos deben ser correctos
Sistema Operativos	Disponibilidad	3	La continua disponibilidad del servidor es necesaria para un exitoso desempeño de la organización
	Trazabilidad	3	Los accesos que se realicen desde y hacia estos sistemas deben ser registrados a nombre del usuario que ingreso
	Confidencialidad	4	Alta confidencialidad porque maneja
Sistema de Gestión de Respaldos	Integridad	3	La aplicación debe mantener la integridad para evitar modificaciones en la información sensible

Sistema de Monitoreo de Seguridad	Disponibilidad	3	Es importante tener siempre disponible la información de los usuarios.
	Trazabilidad	3	Muy relevante que se realice la trazabilidad sobre lo que se haga con este activo
	Confidencialidad	4	Alta confidencialidad porque maneja
	Integridad	3	La aplicación debe mantener la integridad para evitar modificaciones en la información sensible
	Disponibilidad	3	Es importante tener siempre disponible los sistemas 24/7
	Trazabilidad	3	Muy relevante que se realice la trazabilidad sobre lo que se haga en este activo
Servicio de Energía Eléctrica	Confidencialidad	1	La entrada de la red eléctrica no requiere
	Integridad	2	La entrada de la red eléctrica no debe sufrir de manipulaciones
	Disponibilidad	3	Para que las operaciones de la empresa sean desarrolladas es importante que esté en funcionamiento la mayor parte del tiempo la entrada de la red eléctrica
	Trazabilidad	1	No precisa de este criterio
	Confidencialidad	1	La entrada del ACC no

	Integridad	3	El acá no debe sufrir de manipulaciones no autorizadas
Aire acondicionado en el centro de datos	Disponibilidad	3	Para que las operaciones de la empresa sean desarrolladas es importante que esté en funcionamiento la mayor parte del tiempo.
	Trazabilidad	1	Mínimamente requerida
	Confidencialidad	1	La entrada de estos equipos no requiere
	Integridad	3	El sistema no debe sufrir de manipulaciones no autorizadas
Equipo contra incendio en el centro de datos	Disponibilidad	3	Para que las operaciones de la empresa sean desarrolladas ante una eventualidad es importante que esté Operativo
	Trazabilidad	1	Mínimamente requerida
	Confidencialidad	3	La entrada de estos equipos requiere que su configuración sea solo
	Integridad	3	El sistema no debe sufrir de manipulaciones no autorizadas
Equipo UPS centro de datos	Disponibilidad	3	Para que las operaciones de la empresa sean desarrolladas ante una eventualidad es importante que esté Operativo
	Trazabilidad	1	Mínimamente requerida
	Confidencialidad	1	No requiere mayormente
Cableado	Integridad	3	El cableado debe ser integro para no perder performance o interrupciones en el

			tráfico que transitan por ellos.
	Disponibilidad	3	Es importante tener siempre disponible las conexiones.
	Trazabilidad	1	Mínimamente requerida
	Confidencialidad	1	No requiere mayormente
	Integridad	1	No requiere mayormente de este criterio
Red de telefonía	Disponibilidad	3	Es importante, aunque no imprescindible tener la red disponible
	Trazabilidad	1	Mínimamente requerida
	Confidencialidad	4	La red debe ser solo utilizada por el personal
	Integridad	3	La red no debe ser susceptible a manipulaciones
Red LAN	Disponibilidad	3	La red debe estar disponibles en especial para equipos críticos en las operaciones de la institución, así como de los de seguridad
	Trazabilidad	3	Se debe auditar el tráfico y parametrización de la red
	Confidencialidad	4	La red debe ser solo utilizada por el personal
	Integridad	3	La red no debe ser susceptible a manipulaciones
Red WAN	Disponibilidad	3	La red debe estar disponibles en especial para equipos críticos en las operaciones de la institución, así como de los de seguridad

Trazabilidad	3	Se debe auditar el tráfico y parametrización de la red

Fuente: Creación Propia

4.2.5 Análisis De Amenazas.

El objetivo es identificar las amenazas a las que se exponen los activos descritos dentro del alcance del SGSI y las vulnerabilidades que pueden ser explotadas por las amenazas.

A continuación, detallamos las principales amenazas clasificadas por activos de información (Véase Tabla 14):

Tabla 14

Amenazas clasificadas por activos de información

Tipo	Amenazas
[S] Servicios	Fuego / Inundación/ Desastres naturales / Corte suministro eléctrico.
[SW] Software	Errores de usuarios/ Errores de configuración/ Alteración de información / Divulgación de información / Errores de actualización / Virus de computadora / Corrupción de archivos /Desastres naturales.
[D] Documentos	Fuego / Inundación/ Desastres naturales / Corte suministro eléctrico / Condiciones inadecuadas de temperatura.

[HW] Hardware	Fuego / Inundación/ Desastres naturales / Corte suministro eléctrico / Degradación del Hardware / Virus de computadora.
[M] Soportes	Fuego / Inundación/ Desastres naturales / Corte suministro eléctrico / Degradación/ Condiciones ambientales no adecuadas.
[AUX] Equipamiento Auxiliar	Mantenimiento no adecuado / Inundación/ Desastres naturales / variación del suministro eléctrico / Degradación/ Condiciones ambientales no adecuadas.
[COM] Comunicaciones Redes	Fuego / Inundación/ Desastres naturales / Corte suministro eléctrico / Degradación/ Condiciones ambientales no adecuadas.
[I] Instalaciones	Fuego / Inundación/ Desastres naturales / Corte suministro eléctrico /
[P] Personal	Ausencia de personal / Huelgas

Fuente: Creación Propia

A continuación, se detallan las vulnerabilidades que se presentan en cada uno de los activos y las amenazas que pueden explotar dichas vulnerabilidades (Véase Tabla 15):

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Computador Portátil	Fuego	Falta de protección contra fuego

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Acceso no autorizado a la Portátil	Falta de Protección por desatención de equipos
	Corte de la luz o insuficiencia en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado
	Instalación no autorizada o cambios de Software	Falta de control de acceso
	Incumplimiento con la normas legales	Falta de conocimiento de derechos de software por parte de los Empleados
	Uso no previsto	Falta de políticas
	Incumplimiento con	Falta de conocimiento de seguridad
	controles de seguridad	por parte del personal
	Degradación del hardware	Falta de mantenimiento adecuado

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Computador de escritorio	Inautorizada copia de software o información propietaria	Falta de políticas
	Ataque destructivo	Ausencia de seguridad fisica
	Robo	Ausencia de seguridad fisica adecuada
	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Condiciones locales donde los recursos son fácilmente afectados
	Acceso no autorizado a las PCs de oficina	Falta de Protección por desatención de equipos
	Corte de la luz o insuficiencia en el aire acondicionado	Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado.
	Instalación no autorizada o cambios de Software	Falta de control de acceso

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Incumplimiento con la normas legales	Falta de conocimiento de derechos de software por parte de los Empleados
	Uso no previsto	Falta de políticas
	Incumplimiento con controles de seguridad	Desconocimiento por parte del personal en temas de seguridad.
	Degradación del hardware	Falta de mantenimiento adecuado
	Copia de software sin autorizar, información propietaria	Falta de políticas
	Ataque destructivo	Ausencia de seguridad fisica
	Robo	Ausencia de seguridad fisica adecuada
Servidores	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Corrupción de archivos de Registros	Falta de Protección de los archivos de registro
	Negación de Servicio	Incapacidad de distinguir una petición real de una falsa
	Corte de suministro	Funcionamiento no confiable del
	eléctrico o Falla en el aire acondicionado	UPS o funcionamiento no adecuado del aire acondicionado
	Acceso no autorizado a través de la red	Código malicioso desconocido
	Degradación o Falla del hardware	Falta de mantenimiento adecuado
	Manipulación de la Configuración	Falta de control de acceso
	Incumplimiento con controles de seguridad	Desconocimiento por parte del personal en temas de seguridad.
	Incapacidad de restauración	Falta de planes de continuidad del negocio
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Brechas de seguridad no detectadas	Falta de monitoreo de los Servidores
	Ataque destructivo	Ausencia de seguridad fisica
Impresoras	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Degradación o Falla de hardware	Falta de Mantenimiento
	Ataque destructivo	Ausencia de seguridad fisica
	Uso no previsto	Falta de políticas
		Falta de control de acceso
Equipos de Red	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Equipos de Monitoreo	Degradación o Falla de hardware	Falta de Mantenimiento
	Ataque destructivo	Ausencia de seguridad fisica
	Uso no previsto	Falta de políticas
		Falta de control de acceso
	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Degradación o Falla de hardware	Falta de Mantenimiento
	Ataque destructivo	Ausencia de seguridad fisica
	Uso no previsto	Falta de políticas
		Falta de control de acceso
Cintas de Respaldos	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Condiciones inadecuadas de temperatura y/o humedad	Susceptible al calor y humedad
	Ataque destructivo	Ausencia de seguridad fisica
	Robo	Falta de atención del personal
Contrato de Proveedores	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad física adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Pérdida de información	Errores de los empleados
		Almacenamiento no protegido
	Divulgación de información de clientes	Almacenamiento no protegido
	Incumplimiento de leyes en	Falta de conocimiento de los empleados

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	cuanto a la información	
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema
	Contratos no completos	Falta de control para la revisión de contratos
	Ataque destructivo	Ausencia de seguridad fisica
	Incapacidad de Restauración	Falta de planes de continuidad del Negocio
	Modificación no autorizada de información	Insuficiente entrenamiento de Empleados
Procedimientos	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Pérdida de información	Errores de los empleados
		Almacenamiento no protegido

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Divulgación de información de clientes	Almacenamiento no protegido
	Incumplimiento de leyes en cuanto a la información	Falta de conocimiento de los empleados
	Incorrecta o incompleta documentación del sistema	Falta de documentación actualizada del sistema
	Contratos no completos	Falta de control para la revisión de contratos
	Ataque destructivo	Ausencia de seguridad fisica
	Incapacidad de restauración	Falta de planes de continuidad del negocio
	Modificación no autorizada de información	Insuficiente entrenamiento de Empleados
Usuarios Internos	Errores de los empleados, ejecutan acciones no apropiadas	Falta de conocimiento
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
Usuarios Externos	Errores de los empleados, ejecutan acciones no apropiadas	Falta de conocimiento
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
Operadores de Monitoreo	Errores de los empleados, ejecutan acciones no apropiadas	Falta de conocimiento
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
Operadores de Infraestructura	Errores de los empleados, ejecutan acciones no apropiadas	Falta de conocimiento

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Proveedores	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
	Errores de los empleados, ejecutan acciones no apropiadas	Falta de conocimiento
	Insuficiente personal	Falta de acuerdos definidos para reemplazo de empleados
	Divulgación de información confidencial	Falta de acuerdos de confidencialidad
Edificio	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Acceso no autorizado	Falta de políticas
		Ausencia de seguridad fisica
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Canal de Internet	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Acceso no autorizado	Falta de políticas
		Ausencia de seguridad fisica
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
Repositorios de Archivos	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Acceso no autorizado	Falta de políticas
		Ausencia de seguridad fisica
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
Web institucional	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
		Falta de políticas

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Correo Electrónico	Acceso no autorizado	Ausencia de seguridad fisica
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
		Falta de mantenimiento adecuado
	Errores de configuración	Falta de conocimiento del administrador
	Manipulación de la Configuración	Falta de control de acceso
	Uso no previsto	Falta de políticas
	Ataque destructivo	Ausencia de seguridad fisica
Aplicaciones de Ofimática	Negación de Servicio	Capacidad no adecuada de recursos
	Virus de Computación, Fuerza Bruta y	Falta de Protección(AV) actualizada

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Sistema de Gestión de Base de Datos	ataques de Diccionario	
	Spoofing, Salida no autorizada de Información	Falta de control de acceso
		Falta de copias backup continuas
	Negación de Servicio	Capacidad no adecuada de recursos
	Errores de Configuración del servicio	Administador sin la capacitación adecuada Incompleto o incorrecto documentación del sistema
	Virus de Computación, Fuerza Bruta y ataques de Diccionario	Falta de Protección actualizada
		Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas
		Instalación de software no autorizado
	Controles de Seguridad no Cumplidos	Falta de Políticas de Seguridad
		Falta de control de acceso
Sistemas Operativos	Negación de Servicio	Capacidad no adecuada de recursos
	Errores de Configuración del servicio	Administador sin la capacitación adecuada

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
		Incompleto o incorrecto documentación del sistema
	Virus de Computación, Fuerza Bruta y ataques de Diccionario	Falta de Protección actualizada
		Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas
		Instalación de software no autorizado
	Controles de Seguridad no Cumplidos	Falta de Políticas de Seguridad
		Falta de control de acceso
Sistemas de Gestión de Respaldos	Negación de Servicio	Capacidad no adecuada de recursos
	Errores de Configuración del servicio	Administador sin la capacitación adecuada
		Incompleto o incorrecto documentación del sistema
	Virus de Computación, Fuerza Bruta y ataques de Diccionario	Falta de Protección actualizada
		Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas
		Instalación de software no autorizado

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Controles de Seguridad no Cumplidos	Falta de Políticas de Seguridad
		Falta de control de acceso
Sistema de monitoreo de Seguridad	Negación de Servicio	Capacidad no adecuada de recursos
	Errores de Configuración del servicio	Administador sin la capacitación adecuada Incompleto o incorrecto documentación del sistema
	Virus de Computación, Fuerza Bruta y ataques de Diccionario	Falta de Protección actualizada
		Falta de copias de backup continuas
	Pérdida de Servicio	Actualizaciones incorrectas
		Instalación de software no autorizado
	Controles de Seguridad no Cumplidos	Falta de Políticas de Seguridad
		Falta de control de acceso
Servicio de Energía Eléctrica	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Aire acondicionado en el centro de datos	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
Equipo contra incendio el centro de datos	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
Equipo UPS en el centro de datos	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
Cableado	Fuego	Falta de protección contra fuego
	Daños por agua	Ausencia de seguridad fisica adecuada

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
	Desastres naturales	Situación local donde los recursos pueden ser afectados por desastres
	Ataque destructivo	Ausencia de seguridad fisica
Red de telefonía	Errores de los usuarios	Falta de conocimiento del uso del Servicio
	Suplantación de la identidad del usuario	Falta de control de acceso
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Uso no previsto	Falta de políticas
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes
Red LAN	Errores de los usuarios	Falta de conocimiento del uso del Servicio
	Suplantación de la identidad del usuario	Falta de control de acceso
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)

Tabla 15

Activos y Vulnerabilidades

ACTIVOS	AMENAZAS	VULNERABILIDADES
Red WAN	Uso no previsto	Falta de políticas
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes
	Errores de los usuarios	Falta de conocimiento del uso del Servicio
	Suplantación de la identidad del usuario	Falta de control de acceso
	Análisis de tráfico	Falta de establecimiento de una conexión segura (VPN)
	Uso no previsto	Falta de políticas
	Fallas de servicios de soporte (telefonía, servicios de Internet)	Falta de acuerdos bien definidos con terceras partes

Se realizó la estimación de cuan vulnerable es cada activo a la materialización de la amenaza, la frecuencia estimada con que pueden producirse y el impacto en las distintas dimensiones de la

seguridad *(Ver Tabla 16).*

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Computador Portátil	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No cuentan con protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Se han registrado incidentes por el terremoto
	A4: Acceso no autorizado a la Portátil	Media	No todos los usuarios cumplen con las políticas de seguridad, no protegen las máquinas con contraseña.
	V4: Falta de Protección por desatención de equipos	Alta	Fácil acceso a la máquina al no tener contraseña

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A5: Corte de la luz o insuficiencia en el aire acondicionado	Media	Los cortes eléctricos se presentan todos los años en el país no son frecuentes.
	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	Media	Las portátiles no se conectan a un UPS, cuenta con la batería solamente.
	A6: Instalación no autorizada o cambios de Software	Baja	No existen registros de que este problema haya ocurrido.
	V6: Falta de control de acceso	Media	Los usuarios no tienen permiso para la instalación de programas, pero pueden violar las seguridades para realizar las instalaciones.
	A7: Incumplimiento con la normas legales	Baja	No se presentan registros
	V7: Falta de conocimiento de derechos de software por parte de los Empleados	Alta	En la empresa no se tiene conocimiento de las leyes de protección de derechos de autor

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A8: Uso no previsto	Media	Se cuentan con registros de que los equipos son utilizados para otras actividades que no corresponden a la empresa
	V8: Falta de políticas	Alta	Políticas de uso no definidas.
	A9: Incumplimiento con la normas legales	Baja	No se presentan registros
	V9: Falta de conocimiento de seguridad	Alta	Los usuarios no tienen conocimiento de las políticas de seguridad que se deben de implementar.
	A10: controles de seguridad	Alta	No se encuentran definidos
	V10: por parte del personal	Alta	Los usuarios no hacen uso de las políticas de seguridad, no tienen conocimiento y no se encuentran definidas en un instructivo.
	A11: Degradación del hardware	Media	Se encuentran casos registrados en que los equipos sufren golpes o daños en pantalla y daños en baterías, nunca apagan las máquinas.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V11: Falta de mantenimiento adecuado	Media	No se da un mantenimiento preventivo adecuado a los equipos.
	A12: Inautorizada copia de software o información propietaria	Alta	Los usuarios realizan respaldos de la información en discos personales o en correos que no son de la institución.
	V12: Falta de políticas	Alta	No se encuentran establecidas las políticas de respaldo de información.
	A13: Ataque destructivo	Baja	No se han registrado
	V13: Ausencia de seguridad fisica	Baja	No existe protección física.
	A14: Robo	Media	Se ha registrado 1 robo el último año
	V14: Ausencia de seguridad fisica adecuada	Media	Se ha registrado 1 robo de portátil el último año.
Computador de escritorio	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Condiciones locales donde los recursos son fácilmente afectados	Media	Se han registrado incidentes por el terremoto
	A4: Acceso no autorizado a las PCs de oficina	Media	No todos los usuarios cumplen con las políticas de seguridad dejan la máquina sin clave
	V4: Falta de Protección por desatención de equipos	Alta	Fácil acceso a la máquina al no tener contraseña
	A5: Corte de la luz o insuficiencia en el aire acondicionado	Media	Los cortes eléctricos se presentan todos los años en el país no son frecuentes.
	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del	Media	Las portátiles no se conectan a un UPS, cuenta con la batería solamente.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	aire acondicionado.		
	A6: Instalación no autorizada o cambios de Software	Baja	Este problema no ha ocurrido.
	V6: Falta de control de acceso	Media	Los usuarios no tienen permiso para la instalación de programas, pero pueden violar las seguridades para realizar las instalaciones.
	A7: Incumplimiento con la normas legales	Baja	No se presentan registros
	V7: Falta de conocimiento de derechos de software por parte de los Empleados	Alta	En la empresa no se tiene conocimiento de las leyes de protección de derechos de autor
	A8: Uso no previsto	Media	Es considerable el porcentaje de personas que utilizan los recursos para otras actividades que no corresponden a la empresa
	V8: Falta de políticas	Alta	No se encuentran definidas las políticas

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A9: Incumplimiento con controles de seguridad	Baja	No se presentan registros
	V9: Desconocimiento por parte del personal en temas de seguridad.	Baja	Los usuarios no tienen conocimiento de las políticas de seguridad que se deben de implementar.
	A10: Degradación del hardware	Alta	No se encuentran definidos
	V10: Falta de mantenimiento adecuado	Alta	Los usuarios no hacen uso de las políticas de seguridad, no tienen conocimiento y no se encuentran definidas en un instructivo.
	A11: Inautorizada copia de software información propietaria	Alta	Los usuarios realizan respaldos de la información en discos personales o en correos que no son de la institución.
	V11: Falta de políticas	Alta	No se encuentran establecidas las políticas de respaldo de información.
	A12: Ataque destructivo	Baja	No se han registrado

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V12: Ausencia de seguridad fisica	Baja	No existe protección física.
	A13: Robo	Media	Se ha registrado 1 robo el último año
	V13: Ausencia de seguridad fisica adecuada	Media	Se ha registrado 1 robo de portátil el último año.
Servidores	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Se han registrado incidentes por el terremoto
	A4: Corrupción de archivos de Registros	Media	No se cumplen las políticas de seguridad definidas.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V4: Falta de Protección de los archivos de registro	Alta	Se pueden extraer registros desde el servidor principal, no cuenta con los permisos establecidos a nivel de archivos.
	A5: Negación de Servicio	Alta	La seguridad implementada es propensa a ataques DDOS.
	V5: Incapacidad de distinguir una petición real de una falsa	Alta	No mitiga los ataques Ddos por medio de la absorción de tráfico Ddos
	A6: Corte de suministro	Baja	Son pocas las ocasiones en que se han presentado cortes de suministro de energía
	V6: Funcionamiento no confiable del suministro	Media	Se desconoce el mantenimiento que se esté brindando al suministro.
	A7: Falla en el aire acondicionado o sistema eléctrico	Baja	No se han presentado fallas en el sistema eléctrico o de aire acondicionado.
	V7: UPS o funcionamiento no adecuado del aire acondicionado	Baja	Se realizan mantenimientos periódicos para evitar el malfuncionamiento de aires acondicionados o sistemas eléctricos y UPS

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A8: Acceso no autorizado a través de la red	Media	Es considerable el porcentaje de personas que utilizan los recursos para otras actividades que no corresponden a la empresa
	V8: Código malicioso desconocido	Alta	No se encuentran definidas las políticas
	A9: Degradación o Falla del hardware	Baja	No se presentan registros
	V9: Falta de mantenimiento adecuado	Baja	Los usuarios no tienen conocimiento de las políticas de seguridad que se deben de implementar.
	A10: Manipulación de la Configuración	Alta	No se encuentran definidos
	V10: Falta de control de acceso	Alta	Los usuarios no hacen uso de las políticas de seguridad, no tienen conocimiento y no se encuentran definidas en un instructivo.
	A11: Incumplimiento con controles de seguridad	Alta	Los usuarios realizan respaldos de la información en discos personales o en correos que no son de la institución.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V11: Desconocimiento por parte del personal en temas de seguridad.	Alta	No se encuentran establecidas las políticas de respaldo de información.
	A12: Incapacidad de restauración	Baja	No se ha realizado un plan de restauración.
	V12: Falta de planes de continuidad del negocio	Baja	No ha sucedido un
	A13: Análisis de tráfico	Media	Se ha registrado 1 robo el último año
	V13: Falta de establecimiento de una conexión segura (VPN)	Media	Se ha registrado 1 robo de portátil el último año.
	A14: Brechas de seguridad no detectadas	Alta	No se ha realizado un análisis de las brechas de seguridad
	V14: Falta de monitoreo de los Servidores	Alta	No se realiza el monitoreo de los servidores de manera periódica.
	A15: Ataque destructivo	Baja	No se han registrado
	V15: Ausencia de seguridad fisica	Baja	No existe protección física.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Impresoras	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Se han registrado incidentes por el terremoto
	A4: Degradación o Falla de hardware	Media	Existen otras impresoras que pueden trabajar como respaldo de la impresora dañada
	V4: Falta de Mantenimiento	Baja	Se cuenta con una empresa externa que brinda mantenimiento preventivo a las impresoras.
	A5: Ataque destructivo	Baja	No existen registros de esta incidencia

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V5: Ausencia de seguridad fisica	Baja	No se han registrado daños en impresoras.
	A6: Uso no previsto	Alta	Los usuarios utilizan las impresoras para documentos que no se encuentran vinculados con la compañía.
	V6: Falta de políticas	Alta	No existen políticas para las impresiones.
	V7: Falta de control de acceso	Media	Todo usuario registrado en el dominio tiene acceso a las impresoras.
Equipos de Red	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden	Media	Se han registrado incidentes por el terremoto

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	ser afectados por desastres		
	A4: Degradación o Falla de hardware	Alta	Los usuarios no realizan respaldos a sus equipos, por lo que el riesgo de perder la información es alto.
	V4: Falta de Mantenimiento	Baja	No se dan mantenimientos preventivos a las máquinas, si existe algún fallo, proceden al formateo del disco.
	A5: Ataque destructivo	Baja	No se han dado casos de ataques destructivos a la red
	V5: Ausencia de seguridad fisica	Baja	No se han visto en la necesidad de tener protección física a los equipos.
	A6: Uso no previsto	Alta	Existen uso de los equipos para actividades que no conciernen a la empresa
	V6: Falta de políticas	Alta	No existen políticas para el uso de equipos en la red.
	V7: Falta de control de acceso	Alta	No existe el control respectivo de acceso a la red.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Equipos de Monitoreo	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Localmente no hubo daños en los equipos
	A4: Degradación o Falla de hardware	Baja	
	V4: Falta de Mantenimiento	Baja	No se ha dado el caso de requerir a un mantenimiento a los equipos de monitoreo
	A5: Ataque destructivo	Baja	Hasta la fecha no existen ataques destructivos a la red.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V5: Ausencia de seguridad fisica	Baja	No hay protección física a los equipos de monitoreo.
	A6: Uso no previsto	Baja	El uso de los equipos de monitoreo es solo para el personal autorizado
	V6: Falta de políticas	Baja	No existe manual de políticas de uso para los equipos de monitoreo
	V7: Falta de control de acceso	Baja	No existe un control de acceso al área de los equipos de monitoreo.
Cintas de Respaldos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Se han registrado incidentes por el terremoto
	A4: Condiciones inadecuadas de temperatura y/o humedad	Alta	La temperatura en invierno puede llegar a 41 C
	V4: Susceptibilidad al calor y humedad	Alta	Las cintas pueden quedar obsoletas por la humedad y calor
	A5: Ataque destructivo	Media	No se han registrado incidentes de ataques
	V5: Ausencia de seguridad fisica	Alta	Se requiere la protección física para las cintas de respaldo.
	A6: Robo	Alta	Se han registrado incidentes de pérdidas de cintas.
	V6: Falta de atención del personal	Baja	Las cintas de respaldo no son revisadas posteriores a la ejecución del backup en cinta
Contrato de Proveedores	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Se han registrado incidentes por el terremoto
	A4: Pérdida de información	Media	No existe un proceso para salvaguardar la información de los proveedores, por lo que estos documentos quedan vulnerables.
	V4: Errores de los empleados	Baja	Lo empleados no cuentan con un proceso para el almacenamiento de esta información, utilizan un Excel el cual no se encuentra actualizado y respaldado.
	V5: Almacenamiento no protegido	Baja	El almacenamiento de esta información se encuentra bajo ningún resguardo, a la vista de todo el personal.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A6: Divulgación de información de clientes	Alta	La información no se encuentra bajo ninguna contraseña establecida
	V6: Almacenamiento no protegido	Baja	No se protege la información de proveedores y no se respalda
	A7: Incumplimiento de leyes en cuanto a la información	Alta	No se cuenta con un manual de especificaciones funcionales donde detalle los documentos requeridos a los proveedores.
	V7: Falta de conocimiento de los empleados	Alta	La falta de conocimiento de los empleados obstaculiza el procedimiento correcto para el contrato del proveedor
	A8: Incorrecta o incompleta documentación del sistema	Media	Los empleados almacenan información de los proveedores en sus Pocas no que almacenada en el sistema.
	V8: Falta de documentación actualizada del sistema	Alta	Documentación desactualizada
	A9: Contratos no completos	Alta	Los contratos no se encuentran completos ya que las tareas no se encuentran establecidas y no existe

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
			un manual de funciones adecuado para que el personal conozca la función a seguir.
	V9: Falta de control para la revisión de contratos	Baja	Los contratos no son supervisados o revisados bajo responsabilidad de un funcionario previo a la firma de la gerencia general.
	A10: Ataque destructivo	Baja	No se han registrado este tipo de ataques
	V10: Ausencia de seguridad fisica	Baja	No se requiere protección física para la información de proveedores
	A11: Incapacidad de Restauración	Baja	La información se encuentra de manera física.
	V11: Falta de planes de continuidad del Negocio	Baja	La pérdida de esta información no impide la continuidad del negocio.
	A12: Modificación no autorizada de información	Baja	La información de se encuentra bajo ningún esquema de autorización.
	V12: Insuficiente entrenamiento de Empleados	Baja	Los empleados actualizan la información sin ninguna autorización.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Procedimientos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Se han registrado incidentes por el terremoto
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	Se han registrado incidentes por el terremoto
	A4: Pérdida de información	Alta	No se tiene información almacenada de procedimientos.
	V4: Errores de los empleados	Alta	Los empleados no conocen los procedimientos de las funciones a realizar.
	V5: Almacenamiento no protegido	Media	La documentación de los procedimientos no es almacenada o respaldada.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A6: Divulgación de información de clientes	Alta	Se divulga información o documentos de procedimientos, no se cuenta con la seguridad respectiva.
	V6: Almacenamiento no protegido	Baja	No cuentan con protección de la información almacenada
	A7: Incumplimiento de leyes en cuanto a la información	Alta	No se tiene conocimiento del código penal para delitos informáticos
	V7: Falta de conocimiento de los empleados	Alta	El usuario no conoce los procedimientos.
	A8: Incorrecta o incompleta documentación del sistema	Alta	La documentación se encuentra incompleta, las actualizaciones se las realiza en un documento compartido en Excel.
	V8: Falta de documentación actualizada del sistema	Alta	No existe documentación actualizada con los últimos cambios desarrollados en el sistema.
	A9: Contratos no completos	Baja	Lo contratos no se encuentran completos con toda la documentación obligatoria.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V9: Falta de control para la revisión de contratos	Baja	No se cuenta con la respectiva autorización y validación para el establecimiento de contratos.
	A10: Ataque destructivo	Baja	No se han encontrado registros de ataques informáticos.
	V10: Ausencia de seguridad fisica	Baja	No se cuenta con protección física para documentos de procedimiento de la empresa
	A11: Modificación no autorizada de información	Baja	La información está accesible para todo el usuario no se encuentran establecidos permisos o roles necesarios para impedir el acceso.
	V11: Insuficiente entrenamiento de Empleados	Alta	Los empleados no tienen conocimiento de los procedimientos de la empresa, tampoco conocen donde se encuentran los documentos o su última actualización.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Usuarios Internos	A1: Errores de los empleados, ejecutan acciones no apropiadas	Media	Existe un margen de error del 30% en otorgamiento de solicitudes de crédito donde se ha evidenciado documentación obligatoria incompleta y otorgamiento de crédito autorizados cuando deberían de ser rechazados.
	V1: Falta de conocimiento	Media	El entrenamiento se lo realiza en persona, no existe documentación donde se especifiquen los procedimientos o funciones.
	A2: Insuficiente personal	Media	La empresa cuenta con un número de 1-50 empleados
	V2: Falta de acuerdos definidos para reemplazo de empleados	Media	No se tienen documentos funcionales para que otro empleado pueda ejercer las funciones de manera eficaz
	A3: Divulgación de información confidencial	Alta	La información no se encuentra restringida
	V3: Falta de acuerdos de confidencialidad	Alta	No hay documentación de acuerdos de confidencialidad

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Usuarios Externos	A1: Errores de los empleados, ejecutan acciones no apropiadas	Alta	Los empleados suelen cometer errores al realizar sus funciones.
	V1: Falta de conocimiento	Alta	Los empleados no cuentan con un entrenamiento previo
	A2: Insuficiente personal	Media	La empresa cuenta con poco personal
	V2: Falta de acuerdos definidos para reemplazo de empleados	Media	No se cuenta con documentación de las funcionalidades para reemplazar a un empleado.
	A3: Divulgación de información confidencial	Alta	La información confidencial puede divulgarse
	V3: Falta de acuerdos de confidencialidad	Alta	No existen acuerdos de confidencialidad firmados por los empleados.
Operadores de Monitoreo	A1: Errores de los empleados, ejecutan acciones no apropiadas	Baja	Los empleados no conocen las funciones.
	V1: Falta de conocimiento	Baja	No se cuenta con manual de especificaciones funcionales

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A2: Insuficiente personal	Baja	No se cuenta con suficiente personal, no se tiene personal de respaldo.
	V2: Falta de acuerdos definidos para reemplazo de empleados	Baja	No se cuenta con documentación de funciones de los empleados para el reemplazo
	A3: Divulgación de información confidencial	Baja	La información confidencial puede divulgarse
	V3: Falta de acuerdos de confidencialidad	Baja	No existen acuerdos de confidencialidad firmados por los empleados.
Operadores de Infraestructura	A1: Errores de los empleados, ejecutan acciones no apropiadas	Baja	Los empleados no conocen las funciones.
	V1: Falta de conocimiento	Baja	No se cuenta con manual de especificaciones funcionales
	A2: Insuficiente personal	Baja	No se cuenta con suficiente personal, no se tiene personal de respaldo.
	V2: Falta de acuerdos definidos para	Baja	No existen acuerdos para la subrogación de empleados.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	reemplazo de empleados		
	A3: Divulgación de información confidencial	Baja	La información puede ser divulgada, no se cuenta con claves de acceso.
	V3: Falta de acuerdos de confidencialidad	Baja	No se cuenta con documentación de funciones de los empleados para el reemplazo
Proveedores	A1: Errores de los empleados, ejecutan acciones no apropiadas	Baja	Los empleados no conocen el documento de funciones.
	V1: Falta de conocimiento	Baja	No se cuenta con manual de especificaciones funcionales
	A2: Insuficiente personal	Baja	La cantidad de personal de la institución es de 1-50 empleados
	V2: Falta de acuerdos definidos para reemplazo de empleados	Alta	Los empleados no firman un acuerdo al asignarle un cargo
	A3: Divulgación de información confidencial	Alta	La información no se encuentra segura bajo clave

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V3: Falta de acuerdos de confidencialidad	Alta	Los empleados pueden distribuir información confidencial sin existir alguna penalidad por esta acción.
Edificio	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Acceso no autorizado	Alta	No se realiza un control de acceso al edificio
	V3: Falta de políticas	Media	Se puede ingresar al edificio sin autorización.
	V4: Ausencia de seguridad fisica	Alta	No hay seguridad en el edificio.
	A5: Desastres naturales	Media	Los desastres naturales como terremoto afectan la estructura del edificio.
	V5: Situación local donde los recursos pueden	Media	Las oficinas pueden estar seriamente afectadas ante un desastre natural

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	ser afectados por desastres		impidiendo la continuidad del negocio.
	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
Canal de Internet	A3: Acceso no autorizado	Alta	
	V3: Falta de políticas	Media	
	V4: Ausencia de seguridad fisica	Media	
	A5: Desastres naturales	Media	
	V5: Situación local donde los recursos pueden ser afectados por desastres	Media	

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Repositorios de Archivos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Acceso no autorizado	Alta	
	V3: Falta de políticas	Alta	
	V4: Ausencia de seguridad fisica	Media	
	A5: Desastres naturales	Media	
	V5: Situación local donde los recursos pueden ser afectados por desastres	Media	
Web institucional	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Acceso no autorizado	Alta	
	V3: Falta de políticas	Media	
	V4: Ausencia de seguridad fisica	Media	
	A5: Desastres naturales	Media	
	V5: Situación local donde los recursos pueden ser afectados por desastres	Media	
Correo Electrónico	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V2: Ausencia de seguridad fisica adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Impide la comunicación y continuidad del negocio.
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	El servidor de correo electrónico quedar severamente afectado.
	A4: Degradación del servicio y Equipos	Alta	Los servidores pueden quedar fuera de línea afectando los servicios.
	V4: Falta de mantenimiento adecuado	Baja	La falta de mantenimiento del servidor de correos puede ocasionar daños al equipo
	A5: Errores de configuración	Alta	Servidor de correo no es encuentre configurado correctamente
	V5: Falta de conocimiento del administrador	Alta	El administrador de correos no pueda configurar el correo por falta de conocimiento.
	A6: Manipulación de la Configuración	Alta	La configuración del correo sea de fácil manipulación bajo ninguna autorización

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V6: Falta de control de acceso	Alta	Los equipos y servidores quedan expuestos sin seguridades de ingreso
	A7: Uso no previsto	Baja	El uso no previsto de equipos puede ocasionar daños.
	V7: Falta de políticas	Media	Las faltas de políticas debidamente documentadas pueden ocasionar brechas de seguridad de la información.
	A8: Ataque destructivo	Baja	No se han dado casos de ataques destructivos a la red
	V8: Ausencia de seguridad fisica	Baja	No se cuenta con un área de servidores asegurada que resguarde los equipos y servidores.
Aplicaciones de Ofimática	A1: Negación de Servicio	Baja	No se han registrado casos de negación de servicio
	V1: Capacidad no adecuada de recursos	Media	La actualización del hardware en los pc personales obstaculiza el uso del equipo e impide la continuidad del negocio con normalidad, afectando los tiempos.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A2: Virus de Computación, Fuerza Bruta y ataques de Diccionario	Baja	No se han registrado este tipo de ataques.
	V2: Falta de Protección(AV) actualizada	Alta	La información queda expuesta ante ataques
	A3: Spoofing, Salida no autorizada de información	Baja	No se han registrado este tipo de ataques
	V3: Falta de control de acceso	Alta	La información queda expuesta cualquier usuario puede tener acceso
	A4: Falta de capacidad de Restauración	Alta	Pérdida de datos afectando el tiempo de recuperación de la continuidad del negocio.
	V4: Falta de copias backup continuas	Alta	Pérdida de información.
Sistema de Gestión de Base de Datos	A1: Negación de Servicio	Baja	No se han registrado casos de negación de servicio
	V1: Capacidad no adecuada de recursos	Alta	Afecta los sistemas y la continuidad normal del negocio, ocasiona lentitud en el servidor.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A2: Errores de Configuración del servicio	Baja	Se presentarían brechas de seguridad y servicios activos innecesarios.
	V2: Administador sin la capacitación adecuada Incompleto o incorrecto documentación del sistema	Alta	De ocasionar un problema de restauración de base de datos u otro evento el dba debe de tener una competa capacitación para solventar estas eventualidades.
	A3: Virus de Computación, Fuerza Bruta y ataques de Diccionario	Alta	Afecta la base de datos y la funcionalidad del servidor.
	V3: Falta de Protección actualizada	Alta	El servidor queda vulnerable ante ataques, malware y virus
	A4: Falta de capacidad de Restauración	Alta	Al no tener capacidad de restauración, la base de datos no puede ser restaurada. Se debe de contar siempre con la capacidad suficiente de hardware y el desarrollo del capacity plan del sistema a 5 años.
	V4: Falta de copias de backup continuas	Alta	Pérdida de información. Se ha registrado que no se han realizado copias

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
			de base de manera continua.
	A5: Pérdida de Servicio	Media	La pérdida de servicio ocasiona a que el usuario no tenga acceso a la información, esto impide el flujo normal del negocio.
	V5: Actualizaciones incorrectas	Alta	Afecta al servidor de base de datos
	V6: Instalación de software no autorizado	Media	Al servidor de base de datos puede estar vulnerable por un virus
	A7: Controles de Seguridad no Cumplidos	Baja	No se cuenta con la documentación respectiva para los controles de seguridad
	V7: Falta de Políticas de Seguridad	Alta	No es posible determinar la persona que ingresa al servidor y realiza actualizaciones.
	A8: Alteración no autorizado de la configuración	Alta	Al modificar la configuración puede afectar directamente al acceso a los datos
	V8: Falta de control de acceso	Alta	No se tiene un registro de las modificaciones o trabajos realizados en el servidor.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
Sistemas Operativos	A1: Negación de Servicio	Baja	No se han registrado casos de negación de servicio
	V1: Capacidad no adecuada de recursos	Media	Normalmente problema de memoria afecta directamente a las actividades del empleado, se tiene reporte de estos casos por falta de actualización de hardware.
	A2: Errores de Configuración del servicio	Baja	Se presentarían brechas de seguridad y sistemas sin licencias instalados.
	V2: Administrador sin la capacitación adecuada Incompleto o incorrecto documentación del sistema	Baja	El administrador de redes debe de tener la documentación completa y actualizada.
	A3: Virus de Computación, Fuerza Bruta y ataques de Diccionario	Baja	No se han registrado este tipo de ataques
	V3: Falta de Protección actualizada	Alta	Se ha determinado antivirus no actualizado, o máquinas con el antivirus inactivo.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A4: Falta de capacidad de Restauración	Alta	No se cuenta con respaldos de información por usuario.
	V4: Falta de copias de backup continuas	Alta	No se tienen backup de las máquinas de los empleados por falta de recursos y conocimiento.
	A5: Pérdida de Servicio	Alta	Se han registrado errores en el sistema operativo se realiza una reparación desde formateo del equipo perdiendo la información.
	V5: Actualizaciones incorrectas	Baja	Los usuarios no realizan las actualizaciones de los sistemas operativos, esta actividad es ejecutada por el administrador de redes.
	V6: Instalación de software no autorizado	Alta	Se tienen registros de instalación de software sin autorización y sin licencia.
	A7: Controles de Seguridad no Cumplidos	Alta	No se cuenta con los conocimientos de los controles de seguridad previstos por el área de informática.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V7: Falta de Políticas de Seguridad	Alta	La información queda vulnerable.
	A8: Alteración no autorizado de la configuración	Alta	Esto ocasiona que existan brechas de seguridad en la red y en la información que contiene el equipo.
	V8: Falta de control de acceso	Alta	Los usuarios pueden acceder a los equipos que no están configurados con contraseña, se puede extraer información no autorizada.
Sistemas de Gestión de Respaldos	A1: Negación de Servicio	Baja	No se han registrado casos de negación de servicio
	V1: Capacidad no adecuada de recursos	Alta	Al no tener los recursos suficientes la actividad de gestión de respaldos no puede efectuarse.
	A2: Errores de Configuración del servicio	Baja	Se presentarían brechas de seguridad en los sistemas de gestión de respaldos.
	V2: Administrador sin la capacitación adecuada Incompleto o incorrecto	Baja	El administrador debe de tener el conocimiento adecuado para efectuar la gestión de respaldos.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	documentación del sistema		
	A3: Virus de Computación, Fuerza Bruta y ataques de Diccionario	Baja	No se han registrado este tipo de ataques
	V3: Falta de Protección actualizada	Alta	Se ha determinado antivirus no actualizado, o máquinas con el antivirus inactivo.
	A4: Falta de capacidad de Restauración	Alta	No se cuenta con pruebas de backup, o revisión de los respaldos obtenidos.
	V4: Falta de copias de backup continuas	Alta	No se tienen respaldos continuos.
	A5: Pérdida de Servicio	Alta	se han registrado ocasiones en que el sistema de respaldo falla o no se puede ingresar y se debe de reiniciar el sistema
	V5: Actualizaciones incorrectas	Baja	Solo tiene acceso el administrador
	V6: Instalación de software no autorizado	Baja	Solo tiene acceso el administrador

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A7: Controles de Seguridad no Cumplidos	Alta	No cuenta con los controles de seguridad adecuados.
	V7: Falta de Políticas de Seguridad	Alta	No se cuenta con las políticas de seguridad-
	A8: Alteración no autorizado de la configuración	Alta	La configuración puede ser alterada por cualquiera que tenga acceso al equipo.
	V8: Falta de control de acceso	Alta	Ambos usuarios administradores (redes y base de datos) cuentan con el mismo usuario para acceder al equipo.
Sistema de monitoreo de Seguridad	A1: Negación de Servicio	Baja	No se han registrado casos de negación de servicio
	V1: Capacidad no adecuada de recursos	Media	Al no tener los recursos suficientes la actividad de gestión de respaldos no puede efectuarse.
	A2: Errores de Configuración del servicio	Baja	Se presentarían brechas de seguridad en los sistemas de gestión de respaldos.
	V2: Administrador sin la capacitación adecuada Incompleto o incorrecto	Baja	El administrador debe de tener el conocimiento adecuado para efectuar la gestión de respaldos.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	documentación del sistema		
	A3: Virus de Computación, Fuerza Bruta y ataques de Diccionario	Baja	No se han registrado este tipo de ataques
	V3: Falta de Protección actualizada	Alta	Se ha determinado antivirus no actualizado, o máquinas con el antivirus inactivo.
	A4: Falta de capacidad de Restauración	Alta	No se cuenta con pruebas de backup, o revisión de los respaldos obtenidos.
	V4: Falta de copias de backup continuas	Alta	No se tienen respaldos continuos.
	A5: Pérdida de Servicio	Alta	se han registrado ocasiones en que el sistema de respaldo falla o no se puede ingresar y se debe de reiniciar el sistema
	V5: Actualizaciones incorrectas	Baja	Solo tiene acceso el administrador
	V6: Instalación de software no autorizado	Alta	Solo tiene acceso el administrador

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A7: Controles de Seguridad no Cumplidos	Alta	No cuenta con los controles de seguridad adecuados.
	V7: Falta de Políticas de Seguridad	Alta	No se cuenta con las políticas de seguridad-
	A8: Alteración no autorizado de la configuración	Alta	La configuración puede ser alterada por cualquiera que tenga acceso al equipo.
	V8: Falta de control de acceso	Alta	Ambos usuarios administradores (redes y base de datos) cuentan con el mismo usuario para acceder al equipo.
Servicio de Energía Eléctrica	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad física adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Ecuador presenta temblores frecuentes desde el terremoto.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	El país presenta riesgo de vulnerabilidad sísmica
Aire acondicionado en el centro de datos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad física adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Ecuador presenta temblores frecuentes desde el terremoto.
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	El país presenta riesgo de vulnerabilidad sísmica
Equipo contra incendio el centro de datos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad física adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Ecuador presenta temblores frecuentes desde el terremoto.
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	El país presenta riesgo de vulnerabilidad sísmica
Equipo UPS en el centro de datos	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad física adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Ecuador presenta temblores frecuentes desde el terremoto.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	El país presenta riesgo de vulnerabilidad sísmica
Cableado	A1: Fuego	Baja	Es baja la probabilidad de incendios en el sector
	V1: Falta de protección contra fuego	Media	No se tienen protección contra el fuego
	A2: Daños por agua	Baja	No se ha registrado este tipo de amenaza
	V2: Ausencia de seguridad física adecuada	Baja	Los lugares donde se encuentran los equipos portátiles no presentan daños por inundación
	A3: Desastres naturales	Media	Ecuador presenta temblores frecuentes desde el terremoto.
	V3: Situación local donde los recursos pueden ser afectados por desastres	Media	El país presenta riesgo de vulnerabilidad sísmica
	A4: Ataque destructivo	Baja	No se han registrado incidentes de ataques
	V4: Ausencia de seguridad fisica	Alta	El sistema de cableado se encuentra organizado en el armario rack, pero

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
			existen cables que están expuestos.
Red de telefonía	A1: Errores de los usuarios	Baja	El usuario no presenta errores con la red de telefonía
	V1: Falta de conocimiento del uso del Servicio	Baja	El usuario conoce el servicio
	A2: Suplantación de la identidad del usuario	Baja	No se suplanta identidad, se tiene extensiones en los puestos.
	V2: Falta de control de acceso	Media	Es de libre acceso no se tiene restringido llamadas externas
	A3: Análisis de tráfico	Baja	No se cuenta con análisis de tráfico
	V3: Falta de establecimiento de una conexión segura (VPN)	Baja	La red no cuenta con VPN
	A4: Uso no previsto	Media	La red telefónica no tiene limitaciones de llamadas, el usuario la utiliza para llamadas personales.
	V4: Falta de políticas	Baja	No se cuenta con políticas publicadas sobre el uso de la red telefónica.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	Alta	Se han registrado fallas de la red telefónica, en el invierno con mayor frecuencia.
	V5: Falta de acuerdos bien definidos con terceras partes	Baja	No se tienen acuerdos definidos con terceras partes
Red LAN	A1: Errores de los usuarios	Baja	El usuario tiene errores al ingresar a la red por pérdida de clave.
	V1: Falta de conocimiento del uso del Servicio	Baja	No todos los usuarios tienen altos conocimientos de informática.
	A2: Suplantación de la identidad del usuario	Baja	No se han registrado incidentes de suplantación de identidad.
	V2: Falta de control de acceso	Baja	Cada usuario cuenta con un usuario de red.
	A3: Análisis de tráfico	Media	El análisis de tráfico lo realiza el administrador de red, pero esta actividad no es realizada con frecuenta.
	V3: Falta de establecimiento	Baja	No se cuenta con conexión segura VPN

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	de una conexión segura (VPN)		
	A4: Uso no previsto	Media	El usuario utiliza la red para descargar archivos personales o de gran tamaño.
	V4: Falta de políticas	Baja	No se cuenta con políticas de uso
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	Baja	Se han registrado fallas de este servicio.
	V5: Falta de acuerdos bien definidos con terceras partes	Baja	No se cuenta con acuerdos definidos con terceras partes.
Red WAN	A1: Errores de los usuarios	Baja	El usuario tiene errores al ingresar a la red por pérdida de clave.
	V1: Falta de conocimiento del uso del Servicio	Baja	El usuario tiene errores al ingresar a la red por pérdida de clave.
	A2: Suplantación de la identidad del usuario	Baja	No se han registrado incidentes de suplantación de identidad.
	V2: Falta de control de acceso	Baja	Cada usuario cuenta con un usuario de red.

Tabla 16

Estimación de la vulnerabilidad del activo a la materialización de la amenaza

ACTIVOS	AMENAZA	VALOR	DESCRIPCIÓN
	A3: Análisis de tráfico	Media	El análisis de tráfico lo realiza el administrador de red, pero esta actividad no es realizada con frecuenta.
	V3: Falta de establecimiento de una conexión segura (VPN)	Baja	No se cuenta con conexión segura VPN
	A4: Uso no previsto	Media	El usuario utiliza la red para descargar archivos personales o de gran tamaño.
	V4: Falta de políticas	Baja	No se cuenta con políticas de uso
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	Baja	Se han registrado fallas de este servicio.
	V5: Falta de acuerdos bien definidos con terceras partes	Baja	No se cuenta con acuerdos definidos con terceras partes.

Tabla 17

Anexo B

#	CODIGO	ACTIVO	VALORACION
1	HW1	Computador Portátil	Medio
2	HW2	Computador de Escritorio	Medio
4	HW3	Impresoras	Alto
5	HW4	Equipos de Red	Alto
6	HW5	Equipos de Monitoreo	Alto
7	M1	Cintas de Respaldo	Medio
8	D1	Contrato de Proveedores	Medio
10	P1	Usuarios Internos	Medio
11	P2	Usuarios Externos	Medio
12	P3	Operadores de Monitoreo	Alto
13	P4	Operadores de Infraestructura	Alto
14	P5	Proveedores	Alto
15	L1	Edificio	Medio
16	S1	Canal de Internet	Medio
17	S2	Repositorio de archivos	Alto
18	S3	Web Institucional	Medio
19	S4	Correo Electrónico	Alto
21	SW1	Sistema de Gestión de Base de datos	Alto
23	SW2	Sistema de Gestión de Respaldos	Alto
25	AUX1	Servicio de Energía Eléctrica	Medio

Tabla 17

Anexo B

#	CODIGO	ACTIVO	VALORACION
29	AUX2	Cableado	Medio
31	COM2	Red LAN	Alto
32	COM3	Red WAN	Alto

Creación: Creación Propia

CAPÍTULO 5
IMPLEMENTACIÓN Y PRUEBAS

5.1 PLAN DE TRATAMIENTO DE RIESGOS

Se procedió a realizar la valoración de los riesgos en función del inventario de activos de información obtenido, determinando las categorías de los mismos y el criterio para la evaluación de amenazas y vulnerabilidades.

El valor de un riesgo fue calculado usando la fórmula descrita, basado en el componente para el “valor de los activos de información”, “escala de las amenazas” y “nivel de vulnerabilidad”.

C: Valor del riesgo por la confidencialidad

I: Valor del riesgo por la integridad

D: Valor del riesgo por la disponibilidad

T: Valor del riesgo por la trazabilidad

Valor del riesgo = “Valor del activo” x “Amenazas” x “Vulnerabilidades”

Luego de obtener la valoración de los riesgos, se decidirá en aceptar el riesgo o reducirlo, para lo cual se determinará un valor mínimo como límite de aceptación del riesgo, sobre ese valor deben tomarse medidas. La organización seleccionó que el nivel límite de riesgo es de 4, es decir para valores menores o iguales a 4 se aceptara el riesgo.

Tabla 18

Cálculo del total del riesgo

ACTIVO	VALOR	AMENAZA	VALOR DE LA AMENAZA	VULNERA	VALOR DE LA VULNERALIDAD	TOTAL DEL RIESGO
Computador Portátil	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	2	V3	2	12
		A4	2	V4	3	18
		A5	2	V5	2	12
		A6	1	V6	2	6
		A7	1	V7	3	9
		A8	2	V8	3	18
		A9	1	V9	3	9
		A10	3	V10	3	27
		A11	2	V11	2	12
		A12	3	V12	3	27
		A13	1	V13	1	3
		A14	2	V14	2	12
Computador de Escritorio	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	2	V3	2	12

Tabla 18

Cálculo del total del riesgo

ACTIVO	VALOR	AMENAZA	VALOR DE LA AMENAZA	VULNERA	VALOR DE LA VULNERALIDAD	TOTAL DEL RIESGO
		A4	2	V4	3	18
		A5	2	V5	2	12
		A6	1	V6	2	6
		A7	1	V7	3	9
		A8	2	V8	3	18
		A9	1	V9	1	3
		A10	3	V10	3	27
		A11	3	V11	3	27
		A12	1	V12	1	3
		A13	2	V13	2	12
Servidores	4	A1	1	V1	2	8
		A2	2	V2	1	8
		A3	2	V3	2	16
		A4	2	V4	3	24
		A5	3	V5	3	36
		A6	1	V6	2	8
		A7	2	V7	1	8
		A8	2	V8	3	24
		A9	2	V9	1	8
		A10	3	V10	3	36
		A11	3	V11	3	36
		A12	2	V12	1	8
		A13	2	V13	2	16
		A14	3	V14	3	36
		A15	2	V15	1	8
Impresoras	4	A1	1	V1	2	8
		A2	1	V2	1	4
		A3	2	V3	2	16
		A4	2	V4	1	8
		A5	1	V5	1	4
		A6	3	V6	3	36
Equipos de Red	4	A1	1	V1	2	8
		A2	2	V2	1	8
		A3	2	V3	2	16

Tabla 18

Cálculo del total del riesgo

ACTIVO	VALOR	AMENAZA	VALOR DE LA AMENAZA	VULNERA	VALOR DE LA VULNERALIDAD	TOTAL DEL RIESGO
		A4	3	V4	1	12
		A5	1	V5	1	4
		A6	3	V6	3	36
Equipos de Monitoreo	4	A1	1	V1	2	8
		A2	2	V2	1	8
		A3	2	V3	2	16
		A4	2	V4	1	8
		A5	2	V5	1	8
		A6	1	V6	1	4
Contrato de Proveedores	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	2	V3	2	12
		A4	2	V4	1	6
		A6	3	V6	1	9
		A7	3	V7	3	27
		A8	2	V8	3	18
		A9	3	V9	1	9
		A10	1	V10	1	3
		A11	1	V11	1	3
		A12	1	V12	1	3
Procedimientos	4	A1	1	V1	2	8
		A2	1	V2	1	4
		A3	2	V3	2	16
		A4	3	V4	3	36
		A6	3	V6	1	12
		A7	3	V7	3	36
		A8	3	V8	3	36
		A9	2	V9	1	8
		A10	1	V10	1	4
		A11	1	V11	3	12
		A12	1	V12	3	12
Usuarios Internos	3	A1	2	V1	2	12
		A2	2	V2	2	12
		A3	3	V3	3	27

Tabla 18

Cálculo del total del riesgo

ACTIVO	VALOR	AMENAZA	VALOR DE LA AMENAZA	VULNERA	VALOR DE LA VULNERALIDAD	TOTAL DEL RIESGO
Operadores de Monitoreo	4	A1	3	V1	1	12
		A2	3	V2	1	12
		A3	3	V3	1	12
Operadores de Infraestructura	4	A1	3	V1	1	12
		A2	3	V2	1	12
		A3	3	V3	1	12
Proveedores	4	A1	2	V1	1	8
		A2	1	V2	3	12
		A3	3	V3	3	36
Edificio	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	3	V3	2	18
		A5	2	V5	2	12
Canal de Internet	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	3	V3	2	18
		A5	2	V5	2	12
Correo Electrónico	4	A1	1	V1	2	8
		A2	2	V2	1	8
		A3	2	V3	2	16
		A4	3	V4	1	12
		A5	3	V5	3	36
		A6	3	V6	3	36
		A7	1	V7	2	8
		A8	1	V8	1	4
Sistema de Gestión de Base de datos	4	A1	1	V1	3	12
		A2	1	V2	3	12
		A3	3	V3	3	36
		A4	3	V4	3	36
		A5	2	V5	3	24
		A7	1	V7	3	12
		A8	3	V8	3	36
	4	A1	1	V1	2	8
		A2	2	V2	1	8

Tabla 18

Cálculo del total del riesgo

ACTIVO	VALOR	AMENAZA	VALOR DE LA AMENAZA	VULNERA	VALOR DE LA VULNERALIDAD	TOTAL DEL RIESGO
Sistema de Monitoreo de Seguridad		A3	1	V3	3	12
		A4	3	V4	3	36
		A5	3	V5	1	12
		A7	3	V7	3	36
		A8	3	V8	3	36
Servicio de Energía Eléctrica	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	2	V3	2	12
Aire acondicionado en el centro de datos	3	A1	1	V1	2	6
		A2	1	V2	1	3
		A3	2	V3	2	12
Cableado	3	A1	1	V1	2	6
		A2	2	V2	1	8
		A3	2	V3	2	12
		A4	1	V4	3	9
Red LAN	4	A1	3	V1	1	12
		A2	2	V2	1	12
		A3	2	V3	1	8
		A4	2	V4	1	8
		A5	2	V5	1	8
Red WAN	4	A1	3	V1	1	12
		A2	3	V2	1	12
		A3	2	V3	1	8
		A4	2	V4	1	8
		A5	2	V5	1	8

Continuando con el procedimiento de medición de riesgo, el siguiente paso es la aceptación de los riesgos menores o iguales a 4 como se muestra en la tabla 18, los cuales impactan en forma no representativa a la organización.

A continuación, se describen las opciones para el tratamiento de los riesgos:

Tabla 19

Plan de tratamiento del riesgo

ACTIVO	AMENAZA	VULNERALIDAD	TOTRIESGO
Computador Portátil	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad fisica adecuada	ACEPTACIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Acceso no autorizado a la Portátil	V4: Falta de Protección por desatención de equipos	REDUCCIÓN
	A5: Corte de la luz o insuficiencia en el aire acondicionado	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado	REDUCCIÓN
	A6: Instalación no autorizada o cambios de Software	V6: Falta de control de acceso	REDUCCIÓN
	A7: Incumplimiento con la normas legales	V7: Falta de conocimiento de derechos de software por parte de los Empleados	REDUCCIÓN

	A8: Uso no previsto	V8: Falta de políticas	REDUCCIÓN
	A9: Incumplimiento con la normas legales	V9: Falta de conocimiento de seguridad	REDUCCIÓN
	A10: controles de seguridad	V10: por parte del personal	REDUCCIÓN
	A11: Degradación del hardware	V11: Falta de mantenimiento adecuado	REDUCCIÓN
	A12: No autorizada copia de software o información propietaria	V12: Falta de políticas	REDUCCIÓN
	A13: Ataque destructivo	V13: Ausencia de seguridad fisica	ACEPTACIÓN
	A14: Robo	V14: Ausencia de seguridad fisica adecuada	REDUCCIÓN
Computador de Escritorio	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad fisica adecuada	ACEPTACIÓN
	A3: Desastres naturales	V3: Condiciones locales donde los recursos son fácilmente afectados	REDUCCIÓN

A4: Acceso no autorizado a las PCs de oficina	V4: Falta de Protección por desatención de equipos	REDUCCIÓN
A5: Corte de la luz o insuficiencia en el aire acondicionado	V5: Funcionamiento no confiable del UPS o funcionamiento no adecuado del aire acondicionado.	REDUCCIÓN
A6: Instalación no autorizada o cambios de Software	V6: Falta de control de acceso	REDUCCIÓN
A7: Incumplimiento con la normas legales	V7: Falta de conocimiento de derechos de software por parte de los Empleados	REDUCCIÓN
A8: Uso no previsto	V8: Falta de políticas	REDUCCIÓN
A9: Incumplimiento con controles de seguridad	V9: Desconocimiento por parte del personal en temas de seguridad.	ACEPTACIÓN
A10: Degradación del hardware	V10: Falta de mantenimiento adecuado	REDUCCIÓN
A11: No autorizada copia de software información propietaria	V11: Falta de políticas	REDUCCIÓN

	A12: Ataque destructivo	V12: Ausencia de seguridad física	ACEPTACIÓN
	A13: Robo	V13: Ausencia de seguridad física adecuada	REDUCCIÓN
Servidores	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	REDUCCIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Corrupción de archivos de Registros	V4: Falta de Protección de los archivos de registro	REDUCCIÓN
	A5: Negación de Servicio	V5: Incapacidad de distinguir una petición real de una falsa	REDUCCIÓN
	A6: Corte de suministro	V6: Funcionamiento no confiable del suministro	REDUCCIÓN
	A7: Falla en el aire acondicionado o sistema eléctrico	V7: UPS o funcionamiento no adecuado del aire acondicionado	REDUCCIÓN
	A8: Acceso no autorizado a través de la red	V8: Código malicioso desconocido	REDUCCIÓN

	A9: Degradación o Falla del hardware	V9: Falta de mantenimiento adecuado	REDUCCIÓN
	A10: Manipulación de la Configuración	V10: Falta de control de acceso	REDUCCIÓN
	A11: Incumplimiento con controles de seguridad	V11: Desconocimiento por parte del personal en temas de seguridad.	REDUCCIÓN
	A12: Incapacidad de restauración	V12: Falta de planes de continuidad del negocio	REDUCCIÓN
	A13: Análisis de tráfico	V13: Falta de establecimiento de una conexión segura (VPN)	REDUCCIÓN
	A14: Brechas de seguridad no detectadas	V14: Falta de monitoreo de los Servidores	REDUCCIÓN
	A15: Ataque destructivo	V15: Ausencia de seguridad física	REDUCCIÓN
Impresoras	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	ACEPTACIÓN

	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Degradación o Falla de hardware	V4: Falta de Mantenimiento	REDUCCIÓN
	A5: Ataque destructivo	V5: Ausencia de seguridad física	ACEPTACIÓN
	A6: Uso no previsto	V6: Falta de políticas	REDUCCIÓN
Equipos de Red	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	REDUCCIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Degradación o Falla de hardware	V4: Falta de Mantenimiento	REDUCCIÓN
	A5: Ataque destructivo	V5: Ausencia de seguridad física	ACEPTACIÓN
	A6: Uso no previsto	V6: Falta de políticas	REDUCCIÓN
Equipos de Monitoreo	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN

	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	REDUCCIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Degradación o Falla de hardware	V4: Falta de Mantenimiento	REDUCCIÓN
	A5: Ataque destructivo	V5: Ausencia de seguridad física	REDUCCIÓN
	A6: Uso no previsto	V6: Falta de políticas	ACEPTACIÓN
Contrato de Proveedores	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	ACEPTACIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Pérdida de información	V4: Errores de los empleados	REDUCCIÓN
	A6: Divulgación de información de clientes	V6: Almacenamiento no protegido	REDUCCIÓN

	A7: Incumplimiento de leyes en cuanto a la información	V7: Falta de conocimiento de los empleados	REDUCCIÓN
	A8: Incorrecta o incompleta documentación del sistema	V8: Falta de documentación actualizada del sistema	REDUCCIÓN
	A9: Contratos no completos	V9: Falta de control para la revisión de contratos	REDUCCIÓN
	A10: Ataque destructivo	V10: Ausencia de seguridad física	ACEPTACIÓN
	A11: Incapacidad de Restauración	V11: Falta de planes de continuidad del Negocio	ACEPTACIÓN
	A12: Modificación no autorizada de información	V12: Insuficiente entrenamiento de Empleados	ACEPTACIÓN
Procedimientos	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	REDUCCIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN

	A4: Pérdida de información	V4: Errores de los empleados	REDUCCIÓN
	A6: Divulgación de información de clientes	V6: Almacenamiento no protegido	REDUCCIÓN
	A7: Incumplimiento de leyes en cuanto a la información	V7: Falta de conocimiento de los empleados	REDUCCIÓN
	A8: Incorrecta o incompleta documentación del sistema	V8: Falta de documentación actualizada del sistema	REDUCCIÓN
	A9: Contratos no completos	V9: Falta de control para la revisión de contratos	REDUCCIÓN
	A10: Ataque destructivo	V10: Ausencia de seguridad física	REDUCCIÓN
	A11: Modificación no autorizada de información	V11: Insuficiente entrenamiento de Empleados	REDUCCIÓN
Usuarios Internos	A1: Errores de los empleados, ejecutan acciones no apropiadas	V1: Falta de conocimiento	REDUCCIÓN

	A2: Insuficiente personal	V2: Falta de acuerdos definidos para reemplazo de empleados	REDUCCIÓN
	A3: Divulgación de información confidencial	V3: Falta de acuerdos de confidencialidad	REDUCCIÓN
Operadores de Monitoreo	A1: Errores de los empleados, ejecutan acciones no apropiadas	V1: Falta de conocimiento	REDUCCIÓN
	A2: Insuficiente personal	V2: Falta de acuerdos definidos para reemplazo de empleados	REDUCCIÓN
	A3: Divulgación de información confidencial	V3: Falta de acuerdos de confidencialidad	REDUCCIÓN
Operadores de Infraestructura	A1: Errores de los empleados, ejecutan acciones no apropiadas	V1: Falta de conocimiento	REDUCCIÓN
	A2: Insuficiente personal	V2: Falta de acuerdos definidos para reemplazo de empleados	REDUCCIÓN

	A3: Divulgación de información confidencial	V3: Falta de acuerdos de confidencialidad	REDUCCIÓN
Proveedores	A1: Errores de los empleados, ejecutan acciones no apropiadas	V1: Falta de conocimiento	REDUCCIÓN
	A2: Insuficiente personal	V2: Falta de acuerdos definidos para reemplazo de empleados	REDUCCIÓN
	A3: Divulgación de información confidencial	V3: Falta de acuerdos de confidencialidad	REDUCCIÓN
Edificio	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	ACEPTACIÓN
	A3: Acceso no autorizado	V3: Falta de políticas	REDUCCIÓN
	A5: Desastres naturales	V5: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
Canal de Internet	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN

	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	ACEPTACIÓN
	A3: Acceso no autorizado	V3: Falta de políticas	REDUCCIÓN
	A5: Desastres naturales	V5: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
Correo Electrónico	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	REDUCCIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Degradación del servicio y Equipos	V4: Falta de mantenimiento adecuado	REDUCCIÓN
	A5: Errores de configuración	V5: Falta de conocimiento del administrador	REDUCCIÓN
	A6: Manipulación de la Configuración	V6: Falta de control de acceso	REDUCCIÓN
	A7: Uso no previsto	V7: Falta de políticas	REDUCCIÓN
	A8: Ataque destructivo	V8: Ausencia de seguridad física	ACEPTACIÓN

Sistema de Gestión de Base de datos	A1: Negación de Servicio	V1: Capacidad no adecuada de recursos	REDUCCIÓN
	A2: Errores de Configuración del servicio	V2: Administrador sin la capacitación adecuada Incompleto o incorrecto documentación del sistema	REDUCCIÓN
	A3: Virus de Computación, Fuerza Bruta y ataques de Diccionario	V3: Falta de Protección actualizada	REDUCCIÓN
	A4: Falta de capacidad de Restauración	V4: Falta de copias de backup continuas	REDUCCIÓN
	A5: Pérdida de Servicio	V5: Actualizaciones incorrectas	REDUCCIÓN
	A7: Controles de Seguridad no Cumplidos	V7: Falta de Políticas de Seguridad	REDUCCIÓN
	A8: Alteración no autorizado de la configuración	V8: Falta de control de acceso	REDUCCIÓN
Sistema de Monitoreo de Seguridad	A1: Negación de Servicio	V1: Capacidad no adecuada de recursos	REDUCCIÓN

	A2: Errores de Configuración del servicio	V2: Administrador sin la capacitación adecuada Incompleto o incorrecto documentación del sistema	REDUCCIÓN
	A3: Virus de Computación, Fuerza Bruta y ataques de Diccionario	V3: Falta de Protección actualizada	REDUCCIÓN
	A4: Falta de capacidad de Restauración	V4: Falta de copias de backup continuas	REDUCCIÓN
	A5: Pérdida de Servicio	V5: Actualizaciones incorrectas	REDUCCIÓN
	A7: Controles de Seguridad no Cumplidos	V7: Falta de Políticas de Seguridad	REDUCCIÓN
	A8: Alteración no autorizado de la configuración	V8: Falta de control de acceso	REDUCCIÓN
Servicio de Energía Eléctrica	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	ACEPTACIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN

Aire acondicionado en el centro de datos	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	ACEPTACIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
Cableado	A1: Fuego	V1: Falta de protección contra fuego	REDUCCIÓN
	A2: Daños por agua	V2: Ausencia de seguridad física adecuada	REDUCCIÓN
	A3: Desastres naturales	V3: Situación local donde los recursos pueden ser afectados por desastres	REDUCCIÓN
	A4: Ataque destructivo	V4: Ausencia de seguridad física	REDUCCIÓN
Red LAN	A1: Errores de los usuarios	V1: Falta de conocimiento del uso del Servicio	REDUCCIÓN
	A2: Suplantación de la identidad del usuario	V2: Falta de control de acceso	REDUCCIÓN
	A3: Análisis de tráfico	V3: Falta de establecimiento de una conexión segura (VPN)	REDUCCIÓN

	A4: Uso no previsto	V4: Falta de políticas	REDUCCIÓN
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	V5: Falta de acuerdos bien definidos con terceras partes	REDUCCIÓN
Red WAN	A1: Errores de los usuarios	V1: Falta de conocimiento del uso del Servicio	REDUCCIÓN
	A2: Suplantación de la identidad del usuario	V2: Falta de control de acceso	REDUCCIÓN
	A3: Análisis de tráfico	V3: Falta de establecimiento de una conexión segura (VPN)	REDUCCIÓN
	A4: Uso no previsto	V4: Falta de políticas	REDUCCIÓN
	A5: Fallas de servicios de soporte (telefonía, servicios de Internet)	V5: Falta de acuerdos bien definidos con terceras partes	REDUCCIÓN

En base a las vulnerabilidades identificadas en la tabla 19 se describen los controles que minimizan los riesgos asociados. *(Ver Anexo 1).*

5.2 PROPUESTA DE PROYECTOS

Las fases de los proyectos a realizar, serán definidas y puestas en

producción por personal propio de la institución, sin embargo, se darán lineamentos generales para cada una de las etapas.

Los proyectos están basados en los eventos de riesgos que fueron aceptados para ser mitigados.

5.2.1 Gestión De Los Usuarios En Los Sistemas

Los controles definidos a implementar en el proceso especificado, corresponde a los siguientes dominios:

Control de acceso

9.2.2 Gestión de los derechos de acceso asignados a usuarios

9.2.3 Gestión de derechos de accesos con privilegios especiales.

9.2.5 Revisión de los derechos de acceso a los usuarios.

9.2.6 Retirada de los derechos de acceso.

9.4.1 Restricción del acceso a la información.

Cifrado 10

10.1.2 Gestión de claves.

Seguridad en la Operatividad

12.4.1 Registro y gestión de evento de actividad

5.2.2 Planificación

La definición de las tareas, estimación, duración, costos, calendarización y presupuesto estará a cargo del personal de la institución de acuerdo a su planificación interna *(Ver Figura 5.1).*

Nombre de tarea	Duración	Comienzo	Fin
PLAN DE ACCIÓN DEPARTAMENTO DE SEGURIDAD DE INFORMACIÓN	**318 días**	**mié 25/10/17**	**vie 11/01/19**
Elaboración de Manuales, Políticas y Procedimientos de SI	**318 días**	**mié 25/10/17**	**vie 11/01/19**
Manual de Procedimiento de Revisión/Actualización de perfiles de navegación por internet	**12 días**	**mié 25/10/17**	**jue 9/11/17**
Levantamiento de Información	2 días	mié 25/10/17	jue 26/10/17
Análisis del Procedimiento	1 día	vie 27/10/17	vie 27/10/17
Elaboración de Formularios	2 días	lun 30/10/17	mar 31/10/17
Elaboración de Flujogramas	1 día	mié 1/11/17	mié 1/11/17
Rediseño del Manual de Procedimiento	3 días	jue 2/11/17	lun 6/11/17
Revisión de Documentación RO	1 día	mar 7/11/17	mar 7/11/17
Elaboración de cambios en la documentación	2 días	mié 8/11/17	jue 9/11/17
Manual de Procedimiento de Gestión de Usuarios	**12 días**	**vie 10/11/17**	**lun 27/11/17**
Levantamiento de Información	2 días	vie 10/11/17	lun 13/11/17
Análisis del Procedimiento	1 día	mar 14/11/17	mar 14/11/17
Elaboración de Formularios - Resideño de Matriz de solicitud de acceso	2 días	mié 15/11/17	jue 16/11/17
Elaboración de Flujogramas	1 día	vie 17/11/17	vie 17/11/17
Rediseño del Manual de Procedimiento	3 días	lun 20/11/17	mié 22/11/17
Revisión de Documentación RO	1 día	jue 23/11/17	jue 23/11/17
Elaboración de cambios en la documentación	2 días	vie 24/11/17	lun 27/11/17
Manual de Procedimiento de Desvinculación de usuarios, eliminación de usuarios, roles y correos electrónicos	**12 días**	**mar 28/11/17**	**mié 13/12/17**
Levantamiento de Información	2 días	mar 28/11/17	mié 29/11/17
Análisis del Procedimiento	1 día	jue 30/11/17	jue 30/11/17
Elaboración de Formularios	2 días	vie 1/12/17	lun 4/12/17
Elaboración de Flujogramas	1 día	mar 5/12/17	mar 5/12/17

Nombre de tarea	Duración	Comienzo	Fin
Rediseño del Manual de Procedimiento	3 días	mié 6/12/17	vie 8/12/17
Revisión de Documentación RO	1 día	lun 11/12/17	lun 11/12/17
Elaboración de cambios en la documentación	2 días	mar 12/12/17	mié 13/12/17
Aprobación de Comité de Manuales, políticas y procedimientos documentados	**2 días**	**jue 14/12/17**	**vie 15/12/17**
Presentar Manual/Formularios/Matriz a Comité SI	1 día	jue 14/12/17	jue 14/12/17
Elaboación de cambios en la documentación	1 día	vie 15/12/17	vie 15/12/17
Manual de Procedimiento de Control de Acceso de usuarios privilegiados (BDD,SO, cuentas genéricas)	**19 días**	**jue 14/12/17**	**mar 9/01/18**
Levantamiento de Información	2 días	jue 14/12/17	vie 15/12/17
Análisis del Procedimiento	2 días	vie 22/12/17	lun 25/12/17
Elaboración de Formularios	2 días	mar 26/12/17	mié 27/12/17
Elaboración de FlujoGramas	2 días	jue 28/12/17	vie 29/12/17
Documentación del Manual	4 días	lun 1/01/18	jue 4/01/18
Revisión de Documentación RO	1 día	vie 5/01/18	vie 5/01/18
Elaboración de cambios en la documentación	2 días	lun 8/01/18	mar 9/01/18
Manual de Procedimiento de Monitoreo de Pistas de auditoría (todos los sistemas)	**18 días**	**mié 10/01/18**	**vie 2/02/18**
Levantamiento de Información	2 días	mié 10/01/18	jue 11/01/18
Análisis del Procedimiento	3 días	vie 12/01/18	mar 16/01/18
Elaboración de Formularios	3 días	mié 17/01/18	vie 19/01/18
Elaboración de FlujoGramas	3 días	lun 22/01/18	mié 24/01/18
Rediseño del Manual de Procedimiento	4 días	jue 25/01/18	mar 30/01/18
Revisión de Documentación RO	1 día	mié 31/01/18	mié 31/01/18
Elaboración de cambios en la documentación	2 días	jue 1/02/18	vie 2/02/18
Manual de Procedimiento de Revisión de configuración de seguridad en equipos de los funcionarios	**22 días**	**lun 5/02/18**	**mar 6/03/18**
Levantamiento de Información	1 día	lun 5/02/18	lun 5/02/18
Análisis del Procedimiento	2 días	mar 6/02/18	mié 7/02/18
Elaboración de Formularios	2 días	jue 8/02/18	vie 9/02/18
Elaboración de FlujoGramas	2 días	lun 12/02/18	mar 13/02/18
Rediseño del Manual de Procedimiento	3 días	mar 27/02/18	jue 1/03/18
Revisión de Documentación RO	1 día	vie 2/03/18	vie 2/03/18
Elaboración de cambios en la documentación	2 días	lun 5/03/18	mar 6/03/18
Aprobación de Comité de Manuales, políticas y procedimientos documentados	**2 días**	**mié 7/03/18**	**jue 8/03/18**
Presentar Manual/Formularios/Matriz a Comité SI	1 día	mié 7/03/18	mié 7/03/18
Elaboración de cambios en la documentación	1 día	jue 8/03/18	jue 8/03/18

Nombre de tarea	Duración	Comienzo	Fin
Manual de Políticas de Seguridad de la Información	**19 días**	**mié 7/03/18**	**lun 2/04/18**
Levantamiento de Información	2 días	mié 7/03/18	jue 8/03/18
Definición de Políticas de Seguridad de la Información	5 días	vie 9/03/18	jue 15/03/18
Elaboración de Formularios	2 días	vie 16/03/18	lun 19/03/18
Documentar Manual de Políticas de Seguridad de la Información	5 días	mar 20/03/18	lun 26/03/18
Revisión de Documentación RO	2 días	mar 27/03/18	mié 28/03/18
Elaboración de cambios en la documentación	3 días	jue 29/03/18	lun 2/04/18
Manual de Políticas de Sanciones de Seguridad de la Información	**18 días**	**mar 3/04/18**	**jue 26/04/18**
Levantamiento de información	2 días	mar 3/04/18	mié 4/04/18
Definición de políticas de sanción	5 días	jue 5/04/18	mié 11/04/18
Elaboración de Formularios	2 días	jue 12/04/18	vie 13/04/18
Documentar Manual de Políticas	5 días	lun 16/04/18	vie 20/04/18
Revisión de Documentación RO	2 días	lun 23/04/18	mar 24/04/18
Elaboración de cambios en la documentación	2 días	mié 25/04/18	jue 26/04/18
Manual de Monitoreo de Cumplimiento de Políticas de Seguridad y aplicar sanciones	**18 días**	**vie 27/04/18**	**mar 22/05/18**
Levantamiento de información	2 días	vie 27/04/18	lun 30/04/18
Definición de políticas de sanción	5 días	mar 1/05/18	lun 7/05/18
Elaboración de Formularios	2 días	mar 8/05/18	mié 9/05/18
Documentar Manual de Políticas	5 días	jue 10/05/18	mié 16/05/18
Revisión de Documentación RO	2 días	jue 17/05/18	vie 18/05/18
Elaboración de cambios en la documentación	2 días	lun 21/05/18	mar 22/05/18
Aprobación de Comité de Manuales, políticas y procedimientos documentados	**2 días**	**mié 23/05/18**	**jue 24/05/18**
Presentar Manual/Formularios/Matriz a Comité SI	1 día	mié 23/05/18	mié 23/05/18
Elaboración de cambios en la documentación	1 día	jue 24/05/18	jue 24/05/18
Manual de Procedimiento de Actualización de propietarios de Activos de Información	**30 días**	**mié 23/05/18**	**mar 3/07/18**
Levantamiento de Información	2 días	mié 23/05/18	jue 24/05/18
Análisis del Procedimiento	1 día	vie 25/05/18	vie 25/05/18
Elaboración de Formularios	2 días	lun 28/05/18	mar 29/05/18
Elaboración de FlujoGramas	2 días	mié 30/05/18	jue 31/05/18
Rediseño del Manual de Procedimiento	3 días	mar 26/06/18	jue 28/06/18
Revisión de Documentación RO	1 día	vie 29/06/18	vie 29/06/18
Elaboración de cambios en la documentación	2 días	lun 2/07/18	mar 3/07/18
Manual de Procedimiento de Afectaciones a Base de Datos	**29 días**	**mié 4/07/18**	**lun 13/08/18**

Nombre de tarea	Duración	Comienzo	Fin
Levantamiento de Información	2 días	mié 4/07/18	jue 5/07/18
Análisis del Procedimiento	1 día	vie 6/07/18	vie 6/07/18
Elaboración de Formularios	2 días	lun 9/07/18	mar 10/07/18
Elaboración de FlujoGramas	2 días	mié 11/07/18	jue 12/07/18
Rediseño del Manual de Procedimiento	3 días	lun 6/08/18	mié 8/08/18
Revisión de Documentación RO	1 día	jue 9/08/18	jue 9/08/18
Elaboración de cambios en la documentación	2 días	vie 10/08/18	lun 13/08/18
Manual de Procedimiento de Monitoreo de sincronización de componentes tecnológicos	**13 días**	**mar 14/08/18**	**jue 30/08/18**
Levantamiento de Información	2 días	mar 14/08/18	mié 15/08/18
Análisis del Procedimiento	1 día	jue 16/08/18	jue 16/08/18
Elaboración de Formularios	2 días	vie 17/08/18	lun 20/08/18
Elaboración de FlujoGramas	2 días	mar 21/08/18	mié 22/08/18
Rediseño del Manual de Procedimiento	3 días	jue 23/08/18	lun 27/08/18
Revisión de Documentación RO	1 día	mar 28/08/18	mar 28/08/18
Elaboración de cambios en la documentación	2 días	mié 29/08/18	jue 30/08/18
Aprobación de Comité de Manuales, políticas y procedimientos documentados	**2 días**	**vie 31/08/18**	**lun 3/09/18**
Presentar Manual/Formularios/Matriz a Comité SI	1 día	vie 31/08/18	vie 31/08/18
Elaboración de cambios en la documentación	1 día	lun 3/09/18	lun 3/09/18
Manual de gestión de seguridad informática	**13 días**	**lun 10/09/18**	**mié 26/09/18**
Levantamiento de Información	2 días	lun 10/09/18	mar 11/09/18
Análisis del Procedimiento	1 día	mié 12/09/18	mié 12/09/18
Elaboración de Formularios	2 días	jue 13/09/18	vie 14/09/18
Elaboración de Flujogramas	2 días	lun 17/09/18	mar 18/09/18
Rediseño del Manual de Procedimiento	3 días	mié 19/09/18	vie 21/09/18
Revisión de Documentación RO	1 día	lun 24/09/18	lun 24/09/18
Elaboración de cambios en la documentación	2 días	mar 25/09/18	mié 26/09/18
Manual de Procedimiento de Revisión y Monitoreo de Logs/accesos/ pistas de auditoría de usuarios y usuarios privilegiados a nivel de (BDD, SO, Servidores, cuentas genéricas)	**13 días**	**jue 27/09/18**	**lun 15/10/18**
Levantamiento de Información	2 días	jue 27/09/18	vie 28/09/18
Análisis del Procedimiento	1 día	lun 1/10/18	lun 1/10/18
Elaboración de Formularios	2 días	mar 2/10/18	mié 3/10/18
Elaboración de FlujoGramas	2 días	jue 4/10/18	vie 5/10/18
Rediseño del Manual de Procedimiento	3 días	lun 8/10/18	mié 10/10/18
Revisión de Documentación RO	1 día	jue 11/10/18	jue 11/10/18

Nombre de tarea	Duración	Comienzo	Fin
Elaboración de cambios en la documentación	2 días	vie 12/10/18	lun 15/10/18
Manual de Procedimiento de Depuración de accesos de cargos de los funcionarios	**13 días**	**mar 16/10/18**	**jue 1/11/18**
Levantamiento de Información	2 días	mar 16/10/18	mié 17/10/18
Análisis del Procedimiento	1 día	jue 18/10/18	jue 18/10/18
Elaboración de Formularios	2 días	vie 19/10/18	lun 22/10/18
Elaboración de FlujoGramas	2 días	mar 23/10/18	mié 24/10/18
Rediseño del Manual de Procedimiento	3 días	jue 25/10/18	lun 29/10/18
Revisión de Documentación RO	1 día	mar 30/10/18	mar 30/10/18
Elaboración de cambios en la documentación	2 días	mié 31/10/18	jue 1/11/18
Manual de Procedimiento de Elaboración de Matriz de Riesgos SI	**13 días**	**vie 2/11/18**	**mar 20/11/18**
Levantamiento de Información	2 días	vie 2/11/18	lun 5/11/18
Análisis del Procedimiento	1 día	mar 6/11/18	mar 6/11/18
Elaboración de Formularios	2 días	mié 7/11/18	jue 8/11/18
Elaboración de FlujoGramas	2 días	vie 9/11/18	lun 12/11/18
Rediseño del Manual de Procedimiento	3 días	mar 13/11/18	jue 15/11/18
Revisión de Documentación RO	1 día	vie 16/11/18	vie 16/11/18
Elaboración de cambios en la documentación	2 días	lun 19/11/18	mar 20/11/18
Aprobación de Comité de Manuales, políticas y procedimientos documentados	**10 días**	**mié 21/11/18**	**mar 4/12/18**
Presentar Manual/Formularios/Matriz a Comité SI	1 día	mié 21/11/18	mié 21/11/18
Elaboración de cambios en la documentación	1 día	mar 4/12/18	mar 4/12/18
Manual y procedimiento de recepción, análisis, escalamiento y resolución de incidentes de SI	**12 días**	**mié 21/11/18**	**jue 6/12/18**
Levantamiento de Información	2 días	mié 21/11/18	jue 22/11/18
Análisis del Procedimiento	1 día	vie 23/11/18	vie 23/11/18
Elaboración de Formularios	2 días	lun 26/11/18	mar 27/11/18
Elaboración de Flujogramas	1 día	mié 28/11/18	mié 28/11/18
Rediseño del Manual de Procedimiento	3 días	jue 29/11/18	lun 3/12/18
Revisión de Documentación RO	1 día	mar 4/12/18	mar 4/12/18
Elaboración de cambios en la documentación	2 días	mié 5/12/18	jue 6/12/18
Manual y procedimiento de eliminación segura de datos	**12 días**	**vie 7/12/18**	**lun 24/12/18**
Levantamiento de Información	2 días	vie 7/12/18	lun 10/12/18
Análisis del Procedimiento	1 día	mar 11/12/18	mar 11/12/18
Elaboración de Formularios	2 días	mié 12/12/18	jue 13/12/18
Elaboración de Flujogramas	1 día	vie 14/12/18	vie 14/12/18

Nombre de tarea	Duración	Comienzo	Fin
Rediseño del Manual de Procedimiento	3 días	lun 17/12/18	mié 19/12/18
Revisión de Documentación RO	1 día	jue 20/12/18	jue 20/12/18
Elaboración de cambios en la documentación	2 días	vie 21/12/18	lun 24/12/18
Manual y procedimiento de revisión de privilegios y derechos de accesos a usuarios	**12 días**	**mar 25/12/18**	**mié 9/01/19**
Levantamiento de Información	2 días	mar 25/12/18	mié 26/12/18
Análisis del Procedimiento	1 día	jue 27/12/18	jue 27/12/18
Elaboración de Formularios	2 días	vie 28/12/18	lun 31/12/18
Elaboración de Flujogramas	1 día	mar 1/01/19	mar 1/01/19
Rediseño del Manual de Procedimiento	3 días	mié 2/01/19	vie 4/01/19
Revisión de Documentación RO	1 día	lun 7/01/19	lun 7/01/19
Elaboración de cambios en la documentación	2 días	mar 8/01/19	mié 9/01/19
Establecer el plan de manejo de soporte extraíbles	**12 días**	**mar 25/12/18**	**mié 9/01/19**
Levantamiento de Información	2 días	mar 25/12/18	mié 26/12/18
Análisis del Procedimiento	1 día	jue 27/12/18	jue 27/12/18
Elaboración de Formularios	2 días	vie 28/12/18	lun 31/12/18
Elaboración de Flujogramas	1 día	mar 1/01/19	mar 1/01/19
Rediseño del Manual de Procedimiento	3 días	mié 2/01/19	vie 4/01/19
Revisión de Documentación RO	1 día	lun 7/01/19	lun 7/01/19
Elaboración de cambios en la documentación	2 días	mar 8/01/19	mié 9/01/19
Aprobación de Comité de Manuales, políticas y procedimientos documentados	**2 días**	**jue 10/01/19**	**vie 11/01/19**
Identificar y actualizar el inventario de activos de la información	**18 días**	**mié 25/10/17**	**vie 17/11/17**
Elaboración de matriz de control de activos de información con campos de la normativa	1 día	mié 25/10/17	mié 25/10/17
Levantamiento de información	5 días	jue 26/10/17	mié 1/11/17
Recopilación de datos	3 días	jue 2/11/17	lun 6/11/17
Actualizar Inventario	3 días	mar 7/11/17	jue 9/11/17
Definir Metodología	2 días	vie 10/11/17	lun 13/11/17
Documentación y notificación	3 días	mar 14/11/17	jue 16/11/17
Aprobación de la Matriz por el Comité de SI	1 día	vie 17/11/17	vie 17/11/17
Análisis de Disminución de afectaciones a la BD	**14 días**	**mié 29/11/17**	**lun 18/12/17**
Identificar Afectaciones Recurrentes	3 días	mié 29/11/17	vie 1/12/17
Levantamiento de Información	2 días	lun 4/12/17	mar 5/12/17
Revisión de afectaciones recurrentes con Tecnología	2 días	mié 6/12/17	jue 7/12/17
Definición de cambios.	3 días	vie 8/12/17	mar 12/12/17

Nombre de tarea	Duración	Comienzo	Fin
Elaboración de informe	2 días	mié 13/12/17	jue 14/12/17
Seguimiento	1 día	lun 18/12/17	lun 18/12/17
Desarrollo de cronograma y temas para charlas de Seguridad Información	**8 días**	**mar 19/12/17**	**jue 28/12/17**
Definir Temas para charlas sde seguridad del año 2018	2 días	mar 19/12/17	mié 20/12/17
Elaboración de diapositivas	3 días	jue 21/12/17	lun 25/12/17
Elaboración de cronograma	2 días	mar 26/12/17	mié 27/12/17

Figura 5.1 .- Planificación Tentativa – Cronograma 2017 -2018

5.2.3 Planificación

5.2.3.1 Ejecución

La ejecución será realizada por la institución buscando la permanente compatibilidad entre las diferentes fases del proyecto cumpliendo con los requerimientos ajustado a la realidad de la institución.

Para verificar su calidad se realizarán auditorías internas de los procesos cuyo resultado dará oportunidades de mejoras.

La conformación del equipo de desarrollo estará a cargo de la institución con el personal más idóneo para estas tareas.

Adicionalmente se deberá de ser el caso elaborar contratos con los proveedores seleccionados, así como un calendario de recursos con el fin de gestionar los mismos.

5.2.3.2 SEGUIMIENTO Y CONTROL

Se deberá considerar que pueden ocurrir cambios que modifiquen la ejecución del proyecto, sean por factores de personas, tecnológicos o normativos, por lo cual se deberá manejar un control de cambios formal que incluya un proceso de revisión y verificación de entregables.

Se sugiere medir el rendimiento del trabajo y obtener un indicador horas-hombres que permitan un adecuado control de presupuesto.

5.2.3.3 Cierre

La información aprendida del proyecto, deberá ser documentada y formará parte de la información histórica de la institución con el objeto que sea referencia para futuros proyectos.

La aceptación formal por contratos, formularios, entre otros será parte de la información histórica.

5.2.4 Gestión De Monitoreo De La Seguridad Informática

Los controles definidos a implementar en el proceso especificado, corresponden a los siguientes dominios:

Políticas de Seguridad: Brinda apoyo y Orientación a la dirección

con respecto a la seguridad de la información, de acuerdo con los requisitos del negocio y los reglamentos y las leyes pertinentes. (Camelo, 2010) [2]

5.1.1 Conjunto de Políticas para la seguridad de la información.

5.1.2 Revisión de las Políticas para la seguridad de la información.

Seguridad vinculada a los recursos humanos: Todo el recurso humano que hace parte de la Organización debe estar consciente de las amenazas y vulnerabilidades relacionadas con la seguridad de la información y sus responsabilidades y deberes en el apoyo que deben brindar a la política de seguridad de la organización establecida para la reducción del riesgo de error humano. (Camelo, 2010) [2]

7.2.2 Concienciación, educación y capacitación en seguridad de la información.

7.2.3 Proceso disciplinario.

7.3.1 Cambio de puestos de trabajo.

Gestión de activos: Proveer las medidas de seguridad necesarias para proporcionar una protección adecuada a los activos de la Organización, así como controlar, generar responsabilidades,

normas de uso y clasificación sobre los activos de información. (Camelo, 2010) [2]

8.1.3 Uso aceptable de los activos.

8.2.1 Directrices de clasificación

8.2.2 Etiquetado y manipulado de la información

8.2.3 Manipulación de activos

8.3.1 Gestión de soporte extraíbles.

Control de acceso: Este Dominio tiene como propósito proteger todas las formas de acceso a la información sensible de la Organización, no solo protegiendo su hardware y software, sino también los recursos humanos involucrados con su manejo. (Camelo, 2010) [2]

9.2.2 Gestión de los derechos de acceso asignados a usuarios.

Seguridad física y ambiental: Todos los centros de almacenamiento de información de la Organización o instalaciones que estén involucradas con los activos de información deben cumplir con las normas de seguridad física y ambiental, para garantizar que la información manejada en éstas permanezca siempre protegida de accesos físicos por parte de personal no autorizado o por factores

ambientales que no se puedan controlar. (Camelo, 2010) [2]

11.1.3 Seguridad de oficinas, despachos y recursos.

11.1.4 Protección contra amenazas externas y ambientales.

11.1.5 El trabajo en áreas seguras.

11.1.6 Áreas de acceso público, carga y descarga

11.2.3 Seguridad del cableado.

11.2.4 Mantenimiento de los equipos.

11.2.5 Salida de activos fuera de las dependencias de la empresa.

11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.

11.2.8 Equipo informático de usuario desatendido.

Seguridad en la Operatividad: Este Dominio tiene como propósito proteger toda información desde la creación de usuarios, ambientes de desarrollo, prueba y producción, controles contra el código malicioso, registro y gestión de eventos de actividad. (Camelo, 2010) [2]

12.1.1 Documentación de procedimientos de operación.

12.1.2 Gestión de cambios.

12.1.3 Gestión de capacidades.

12.1.4 Separación de entornos de desarrollo, prueba y producción.

12.2.1 Controles contra el código malicioso.

12.4.1 Registro y gestión de eventos de actividad.

12.4.3 Registros de actividad del administrador y operador del sistema.

12.6.1 Gestión de las vulnerabilidades técnicas.

12.6.2 Restricciones en la instalación de software.

12.7.1 Controles de auditoría de los sistemas de información.

Seguridad en las telecomunicaciones: Este Dominio tiene como propósito establecer políticas de seguridad en las redes y telecomunicaciones, acuerdos de intercambio de información con proveedores externos, acuerdo de confidencialidad para evitar fugas de datos. (Camelo, 2010) [2]

13.1.1 Controles de red.

13.1.2 Mecanismos de seguridad asociados a servicios en red.

13.1.3 Segregación de redes

13.2.1 Políticas y procedimientos de intercambio de información.

13.2.2 Acuerdos de intercambio.

13.2.4 Acuerdo de confidencialidad y secreto.

Adquisición, desarrollo y mantenimiento de los sistemas de Información: Este Dominio busca asegurar toda la infraestructura que soporta la información de la Organización, proporcionándoles controles adecuados para proteger toda la información de propiedad de la Organización. (Camelo, 2010) [2]

14.2.3 Recisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.

Relaciones con proveedores: Este Dominio tiene como propósito establecer procedimientos de documentación de datos de proveedores y revisión de servicios prestados para que no afecte la operativa en caso de un fallo en los sistemas. (Camelo, 2010) [2]

15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.

15.2.1 Supervisión y revisión de los servicios prestados por terceros.

15.2.2 Gestión de cambios en los servicios prestados por terceros.

Gestión de Incidentes en la seguridad de la información: La gestión de incidentes es un insumo de increíble valor para el SGSI, pues contribuye a robustecer cualquier área que se vea afectada con un incidente, de allí la importancia de que este Dominio este aplicado en la Organización con una estructura muy fuerte de trabajo, respuesta y gestión de incidentes. (Camelo, 2010) [2]

16.1.2 Notificación de los eventos de seguridad de la información.

16.1.3 Notificación de puntos débiles de la seguridad.

Aspecto de seguridad de la información en la gestión de la continuidad del negocio: Este dominio busca que la información de la Organización siempre esté disponible, y cuando no pueda estarlo, su tiempo de no disponibilidad sea lo más reducido posible para no afectar las operaciones, al cliente, etc. (Camelo, 2010) [2]

17.1.1 Planificación de la continuidad de la seguridad de la información.

17.1.2 Implementación de la continuidad de la seguridad de la información.

17.1.3 Verificación, revisión y evaluación de la continuidad de la

seguridad de la información.

17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

5.2.4.1 PLANIFICACIÓN

La definición de las tareas, estimación, duración, costos, calendarización y presupuesto estará a cargo del personal de la institución de acuerdo a su planificación interna.

5.2.4.2 EJECUCIÓN

La ejecución será realizada por la institución buscando la permanente compatibilidad entre las diferentes fases del proyecto cumpliendo con los requerimientos ajustado a la realidad de la institución.

Para verificar su calidad se realizarán auditorías internas de los procesos cuyo resultado dará oportunidades de mejoras en los procedimientos.

La conformación del equipo de desarrollo estará a cargo de la institución con el personal más idóneo para estas tareas.

Adicionalmente se deberá de ser el caso elaborar

contratos con los proveedores seleccionados, así como un calendario de recursos con el fin de gestionar los mismos.

5.2.4.3 SEGUIMIENTO Y CONTROL

Se deberá considerar que pueden ocurrir cambios que modifiquen la ejecución del proyecto, sean por factores de personas, tecnológicos o normativos, por lo cual se deberá manejar un control de cambios formal que incluya un proceso de revisión y verificación de entregables.

Se sugiere medir el rendimiento del trabajo y obtener un indicador horas-hombres que permitan un adecuado control de presupuesto.

5.2.4.4 CIERRE

La información aprendida del proyecto, deberá ser documentada y formará parte de la información histórica de la institución con el objeto que sea referencia para futuros proyectos.

La aceptación formal por contratos, formularios, entre otros será parte de la información histórica.

CAPÍTULO 6

ANÁLISIS Y RESULTADOS

6.1 RESUMEN EJECUTIVO

En el trabajo realizado, se identificaron serias deficiencias en el control interno de la institución, basados en los procesos de gestión de usuario y del monitoreo de la seguridad.

La institución está operando sin una guía clara de lineamientos de seguridad de la información, encontrando casos de ausencia de planes de contingencia de TI.

Se detectaron tres factores relevantes que influyen en el riesgo operativo institucional y no son administrados adecuadamente, procesos, personas y tecnologías de la información.

El riesgo reputacional, es el más importante para la institución, ya que depende mucho de la imagen que proyecte a sus clientes y la confianza

que genere.

Los dominios de seguridad de la información donde más deficiencias se han encontrado, radican en políticas de seguridad, seguridad física y ambiental y seguridad en las operaciones.

Respecto al cumplimiento normativo, la institución tiene la predisposición para cumplir con las normativas vigentes evidenciado en la gestión realizada para este trabajo, sin embargo, se deben unificar esfuerzos de todas las áreas y no hacerlo de forma aislada.

La administración de riesgos actual se realiza de forma subjetiva, es decir que no se ejecuta una valoración holística con los dueños de los procesos, por lo cual pueden existir riesgos que no se hayan considerado.

La institución, dispondrá de la implementación de los proyectos sugeridos en relación a sus recursos considerando una nueva evaluación de riegos debido a cambios en los factores de riesgos asociados.

Los controles sugeridos a implementar, son los mínimos requeridos para disponer de una seguridad razonable en la institución y para el cumplimiento normativo.

La institución deberá este ahondar esfuerzos en reforzar y establecer un área de Seguridad de la Información independiente del área de sistemas que son los ejecutores, minimizando así un potencial conflicto de

intereses.

Las formas de transaccionar cambian con la llegada de nuevas tecnologías y con ellos asociados nuevos riesgos para los cuales la institución debe estar preparada con una base sólida de seguridad para no dar en lo posible ventajas en la captación de clientes.

La seguridad no es estática y no proviene solo del exterior, por lo cual se debe considerar avanzar con el análisis de riesgos e implementación de controles que ayuden a complementar el ecosistema de seguridad.

6.2 RESUMEN DE CUMPLIMIENTO DE CONTROLES

Después de la implementación de los controles por medio de los proyectos definidos, estos deben ser evaluados por auditorias independientes para el cumplimiento de los requisitos normativos.

Se debe encontrar en el siguiente avance de acuerdo a las cláusulas de la norma ISO/IEC 27001:2013:

Tabla 25

Controles Sugeridos

DOMINIO	Controles Actuales	Controles Implementar
Políticas de Seguridad de la Información	2	10
Seguridad ligada a los recursos humanos.	3	14
Gestión de Activos.	2	12
Control de Accesos.	3	31
Cifrado.	0	1
Seguridad Física y Ambiental.	8	53
Seguridad Operativa.	9	42
Seguridad en las Telecomunicaciones.	4	18
Adquisición, desarrollo y mantenimiento de los sistemas de información.	0	1
Relaciones con proveedores.	3	9
Gestión de Incidentes en la Seguridad de la Información.	2	4
Aspectos de la Seguridad de la Información en la Gestión de la Continuidad del Negocio.	1	12

Fuente: Creación Propia

El 82% de los controles sugeridos, no existen en la institución y solo un 18% existen, pero son pocos efectivos para mitigar el riesgo asociado y necesitan rediseñarse.

Los controles actuales deberán ser evaluados en el momento que se inicie la implementación de los controles sugeridos, con el objeto de analizar su impacto en la seguridad de la institución.

Los controles a implementar, deben estar personalizados a la realidad de la institución, cumpliendo las normativas vigentes.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1 El Sistema de Gestión de Seguridad de Información se define de forma personalizada de acuerdo a los riesgos de la institución, es decir a su realidad de forma estructurada, sistemática y metódica.

2 La definición clara y oportuna de los responsables de cada uno de los activos de información es primordial, siendo conveniente delimitar el área de responsabilidad de cada uno.

3 El monitoreo del uso de los recursos permite establecer potenciales retrasos que derivarían en fallos del sistema y de seguridad, otorgando tiempo para realizar un plan de administración de capacidad.

4 Al no disponer de recursos suficientes la institución, no debe extender el SGSI a toda la organización, sino deberá enfocar sus esfuerzos en los

procesos donde se realizan la mayor parte de las actividades Core del negocio.

5 Con el objeto de responder de forma precisa a incidencias de seguridad, es vital tener especificado un proceso de comunicación de incidencias, el cual debe ser difundido a todos los empleados de la organización, minimizando así la probabilidad de recurrencia en un mismo problema.

6 La seguridad es una actividad permanente y la aplicación de la propuesta para requiere el soporte de toda la organización.

7 EL SGSI no se debe considerar como un fin, sino como un medio de apoyo para la consecución de los objetivos institucionales.

8 La concientización en la institución es un pilar fundamental, por lo cual se debe buscar y adoptar prácticas que permitan activar el interés y compromiso por parte de todos los empleados.

9 El eslabón más vulnerable de la cadena operativa radica en las personas, por lo cual el análisis y evaluación del riesgo del SGSI se hará énfasis en este ítem, aplicando el principio del mínimo conocimiento.

10 La institución actualmente, adolece de serias deficiencias en la gestión de usuarios y de monitoreo de seguridad cumpliendo solo parcialmente la normativa vigente y expuesta a fraudes internos y externos.

11 La ESPOL por medio de la realización de este trabajo, confirma su vínculo de colaboración con el sector privado.

RECOMENDACIONES

1 Estructurar un área de independiente de Seguridad de la Información, que será la encargada del monitoreo de seguridad y de la gestión de usuarios, evitando así un potencial conflicto de interés con el área de Sistemas.

2 Revisar que los controles a dispuestos en el documento acorde al momento en que se decida a implementar, debido a cambios en factores de costos, tecnológicos, normativas y externos, puedan quedar obsoletos o deficientes para la función que fueron diseñados.

3 Realizar análisis periódicos de los riesgos por cambios interno o externos, reduciendo así la posibilidad de que algún evento no considerado pueda afectar la operatividad del negocio,

4 Documentar formalmente los procedimientos, independientemente de su origen, detallando sus requerimientos, evitando que estos queden de forma informal y no se puedan establecer responsabilidades por el incumplimiento del mismo.

5 Definir el comité de contingencias, donde se establezca de forma clara las funciones y responsabilidades de cada uno de los miembros y estar preparados normativa y operativamente ante eventuales siniestros

6 Considerar el cumplimiento de las normas y leyes vigentes en el sistema de gestión de seguridad de información por temas de corresponsales bancarios, es importante desde el punto de vista reputacional ante los demás.

7 Considerar como un proceso de mejoramiento continuo al SGSI, en donde

los cambios actuales estén soportados en requerimientos de seguridad, caso contrario es posible que muchos procesos queden obsoletos y a su vez puedan generar brecha de seguridad respecto a la confidencialidad, integridad y disponibilidad de la información que dispone la institución.

BIBLIOGRAFÍA

[1] BINARIA, E. (16 de 3 de 2012). EXPRESIÓN BINARIA. Obtenido de http://www.expresionbinaria.com/la-seguridad-de-informacion-tratada-en-capas/

[2] Camelo, L. (28 de Junio de 2010). SEGU.INFO. Obtenido de Noticias sobre seguridad de la información: http://blog.segu-info.com.ar/2010/06/dominios-de-iso-27001-e-iso-27002.html?m=1

[3] Ecuador, S. d. (2 de Febrero de 2014). Superbancos. Obtenido de Superbancos: http://www.superbancos.gob.ec/practg/p_index?

[4] Furnell, S. (2005). Computer Insecurity: Risking the System. UK: Springer Science & Business Media.

[5] Info, S. (15 de 02 de 2013). Seguridad y auditoria de sistemas. Obtenido de Seguridad en la nube: http://seguridadenlanube.blogspot.com/2013/02/cambios-en-la-nueva-iso-27001-2013.html

[6] ISACA. (4 de 8 de 2013). www.isaca.org. Obtenido de Asociación de auditores de sistemas: https://www.isaca.org/pages/default.aspx

[7] ISO27000. (5 de 6 de 2016). www.iso27000.es. Obtenido de Portal de ISO 27001 en español: http://www.iso27000.es/

[8]Lean, S. (11 de 7 de 2015). http://senseilean.blogspot.com/2015/07/ciclo-sdca-y-pdca-controlar.html. Obtenido de http://senseilean.blogspot.com/2015/07/ciclo-sdca-y-pdca-controlar.html: http://senseilean.blogspot.com/2015/07/ciclo-sdca-y-pdca-controlar.html

[9]Orué, N. B. (2015). Mejora Continua en el Servicio de Atención al Cliente de ANDE.

[10]Solidaria, S. d. (5 de 2 de 2015). www.seps.gob.ec. Obtenido de SEPS: http://www.seps.gob.ec/

[11]Standardization, I. O. (16 de 7 de 2016). iso.org. Obtenido de ISO: https://www.iso.org/home.html

ANEXO 1

Tabla 20

POLÍTICAS DE SEGURIDAD.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Hardware Portátil	A7	V7	Falta de control de protección de derechos de software	5.1.2	Inconvenientes legales	S	Revisión de las políticas de derecho de software.
	A10	V10	No se encuentran definidos	5.1.1	Fácil acceso a violaciones de seguridad	S	Emisión y verificación de las políticas de seguridad de la información
	A11	V11	No se encuentran definidos	5.1.2	Fácil acceso a violaciones de seguridad	S	Revisión de las políticas de privacidad
	A12	V12	Falta de políticas	5.1.1	Copias no autorizadas de software	S	Emisión y verificación de las políticas de seguridad de la información
	A13	V13	Falta de políticas	5.1.2	Copias no autorizadas de software	S	Revisión de las políticas de privacidad

Computador de escritorio	A11	V11	Falta de políticas	5.1.1	Copias no autorizadas de software	S	Emisión y verificación de las políticas de seguridad de la información
	A12	V12	Falta de políticas	5.1.2	Copias no autorizadas de software	S	Revisión de las políticas de privacidad
Contrato de Proveedores	A4	V4	Errores de los empleados	5.1.2	Errores de los empleados	S	Evaluación de almacenamiento digital de la información de los proveedores.
	A8	V8	Falta de documentación actualizada del sistema	5.1.2	Falta de argumentos ante alguna eventualidad contractual	S	Evaluación de almacenamiento digital de la información de los proveedores.
Procedimiento	A4	V4	Errores de los empleados	5.1.2	Errores de los empleados	S	Evaluación de almacenamiento digital de la información de los procedimientos.
	A8	V8	Falta de documentación actualizada	5.1.2	Falta de argumentos ante alguna eventualidad en los aplicativos	S	Establecer y/o mejorar procedimiento
	A9	V9	Falta de control para el establecimiento del procedimiento	5.1.2	Falta de argumentos ante alguna eventualidad laboral	S	Establecer un procedimiento
	A11	V11	Insuficiente entrenamiento de los empleados	5.1.2	Elaboración de procedimientos no viables o complejos de implementar	S	Establecer un procedimiento de continuidad del negocio

Canal de Internet	A5	V5	Situación local donde los recursos pueden ser afectados por desastres	5.1.2	Operaciones basadas en este canal no puedan estar disponibles	S	Establecer un procedimiento de continuidad del negocio
Correo electrónico	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	5.1.2	La comunicación respecto al envió de documentación de soporte normativo no esté disponible, incumpliendo.	S	Establecer un procedimiento de continuidad del negocio
	A6	V6	Falta de control de acceso	5.1.2	Acceso no autorizado al servicio		Realizar una revisión de las políticas de seguridad de acceso a este servicio
Red LAN	A1	V1	Falta de conocimiento del uso del servicio	5.1.2	Uso no adecuado del servicio	S	Realizar una revisión de las políticas de seguridad de acceso a este servicio
	A1	V1	Falta de conocimiento del uso del servicio	5.1.2	Uso no adecuado del servicio	S	Realizar una revisión de las políticas de seguridad de acceso a este servicio

Tabla 21

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Hardware Portátil	A7	V7	Falta de conocimiento de protección de derecho de software	7.2.2	Incumplimiento normativo y de leyes vigentes	S	Inducción al personal sobre las normativas vigentes
	A8	V8	Falta de políticas aplicadas	7.2.2	Uso del recurso para tareas no propias del negocio	S	Inducción al personal sobre seguridad de la información
	A9	V9	Desconocimiento por parte del personal en temas de seguridad.	7.2.2	Incumplimiento de las normas	S	Inducción al personal sobre seguridad de la información
				7.2.3	Incumplimiento de las normas	S	Definición e implementación de la política de proceso disciplinario
Computador de escritorio	A8	V8	Falta de políticas aplicadas	7.2.2	Uso del recurso para tareas no propias del negocio	S	Inducción al personal sobre seguridad de la información

Tabla 21

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A11	V11	Desconocimiento por parte del personal en temas de seguridad.	7.2.2	Potencial contravención a los controles de seguridad	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Potencial contravención a los controles de seguridad	S	Definición e implementación de la política de proceso disciplinario
Impresoras	A6	V6	Falta de políticas	7.2.2	Uso del recurso para tareas no propias del negocio	S	Inducción al personal sobre seguridad de la información.
Equipos de red	A6	V6	Falta de políticas	7.2.2	Uso del recurso para tareas no propias del negocio	S	Inducción al personal sobre seguridad de la información.
Contrato de Proveedores	A4	V4	Errores de los empleados	7.2.2	Pérdida total o parcial de la información	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Pérdida total o parcial de la información	S	Definición e implementación de la política de proceso disciplinario.
	A6	V6	Almacenamiento no protegido	7.2.2	Divulgación de la información de los contratos	S	Inducción al personal sobre seguridad de la información.
	A7	V7	Falta de conocimiento de los empleados	7.2.2	Incumplimiento de las normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Incumplimiento de las normas	S	Definición e implementación de la política de proceso disciplinario.
Procedimiento	A4	V4	Errores de los empleados	7.2.2	Pérdida total o parcial de la información	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario

Tabla 21

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Usuarios Internos	A6	V6	Almacenamiento no protegido	7.2.2	Divulgación de la información de los procedimientos	S	Inducción al personal sobre seguridad de la información.
	A7	V7	Falta de conocimiento de los empleados	7.2.2	Incumplimiento de las normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
	A8	V8	Falta de documentación actualizada	7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
	A9	V9	Falta de control para el establecimiento del procedimiento	7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
	A1	V1	Falta de conocimiento	7.2.2	Uso de recursos de forma no adecuada	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
	A2	V2	Falta de acuerdos definidos para reemplazo de empleados	7.3.1	Degradación o retrasos en los procesos	S	Establecimiento de procedimiento de reemplazos al menos en puestos críticos.
	A3	V3	Falta de acuerdos de confidencialidad	7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.

Tabla 21

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Operadores de Monitoreo	A1	V1	Falta de conocimiento	7.2.2	Uso de recursos de forma no adecuada	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
	A2	V2	Falta de acuerdos definidos para reemplazo de empleados	7.3.1	Degradación o retrasos en los procesos	S	Establecimiento de procedimiento de reemplazos al menos en puestos críticos.
	A3	V3	Falta de acuerdos de confidencialidad	7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Operadores de Infraestructura	A1	V1	Falta de conocimiento	7.2.2	Uso de recursos de forma no adecuada	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
	A2	V2	Falta de acuerdos definidos para reemplazo de empleados	7.3.1	Degradación o retrasos en los procesos	S	Establecimiento de procedimiento de reemplazos al menos en puestos críticos.
	A3	V3	Falta de acuerdos de confidencialidad	7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Proveedores	A1	V1	Falta de conocimiento y entrenamiento oportuno	7.2.2	Uso de recursos de forma no adecuada	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas		Definición e implementación de la política de proceso disciplinario.
	A2	V2	Falta de acuerdos definidos para reemplazo de empleados	7.3.1	Degradación o retrasos en los procesos	S	Establecimiento de procedimiento de reemplazos al menos en puestos críticos.
	A3	V3	Falta de acuerdos de confidencialidad	7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.

Tabla 21

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Correo electrónico	A5	V5	Falta de conocimiento del administrador	7.2.2	Mal funcionamiento del medio	S	Inducción al personal sobre seguridad de la información.
	A7	V7	Falta de políticas	7.2.2	Incumplimiento de las normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Sistema de gestión de base de datos	A7	V7	Falta de políticas de seguridad	7.2.2	Incumplimiento de las normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Sistema de monitoreo de seguridad	A7	V7	Falta de políticas de seguridad	7.2.2	Incumplimiento de las normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Cableado	A4	V4	Ausencia de seguridad fisica adecuada	7.2.2	Incumplimiento de normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Red LAN	A4	V4	Falta de políticas de seguridad	7.2.2	Incumplimiento de normas	S	Inducción al personal sobre seguridad de la información.
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.
Red WAN	A4	V4	Falta de políticas	7.2.2	Incumplimiento de normas	S	Inducción al personal sobre seguridad de la información.

Tabla 21

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS							
ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				7.2.3	Infracciones en las normas	S	Definición e implementación de la política de proceso disciplinario.

Tabla 22

GESTIÓN DE ACTIVOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A11	V11	Desconocimiento por parte del personal en temas de seguridad.	8.1.3	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de uso aceptable de los activos

Tabla 22

GESTIÓN DE ACTIVOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Contrato de Proveedores	A4	V4	Errores de los empleados	8.2.1	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de clasificación de la información.
				8.2.2	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de etiquetado de la información
	A6	V6	Almacenamiento no protegido	8.2.2	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de etiquetado de la información
				8.2.3	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de manipulación de activos
Procedimiento	A4	V4	Errores de los empleados	8.2.1	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de clasificación de la información.
				8.2.2	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de etiquetado de la información

Tabla 22

GESTIÓN DE ACTIVOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A6	V6	Almacenamiento no protegido	8.2.2	Perdida o fuga de información de los equipos	S	Definición, implementación y difusión del procedimiento de etiquetado de la información.
				8.2.3	Perdida o fuga de información de los equipos	S	Defunción, implementación y difusión del procedimiento de manipulación de activos
Canal de Internet	A6	V6	Almacenamiento no protegido	8.13	Perdida o fuga de información de los equipos	S	Defunción, implementación y difusión del procedimiento de manipulación de activos
Correo electrónico	A6	V6	Almacenamiento no protegido	8.13	Perdida o fuga de información de los equipos	S	Defunción, implementación y difusión del procedimiento de manipulación de activos
Sistema de gestión de base de datos	A4	V4	Falta de copias de Backus	8.3.1	Perdida de información y falta de registro histórico normativo	S	Definición, implementación y difusión del procedimiento de uso aceptable de activos
Sistema de monitoreo de seguridad	A4	V4	Falta de copias de Backus	8.3.1	Perdida de información y falta de registro histórico normativo	S	Definición, implementación y difusión del procedimiento de uso aceptable de activos

Tabla 22

GESTIÓN DE ACTIVOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Red LAN	A2	V2	Falta de control de acceso	8.1.3	Uso de equipos externos no autorizados por la institución	S	Defunción, implementación y difusión del procedimiento de uso aceptable de activos
Red WAN	A2	V2	Falta de control de acceso	8.1.3	Uso de equipos no autorizados por la institución	S	Definición, implementación y difusión del procedimiento de uso aceptable de activos

Tabla 23

CONTROL DE ACCESOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Hardware Portátil	A8	V8	Uso del recurso para tareas no propias del negocio	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios
				9.2.5	Cambio no autorizado en las configuraciones	U	Revisar los derechos de accesos de los usuarios
				9.2.6	Cambio no autorizado en las configuraciones	U	Adaptación de los derechos de los usuarios de acuerdo a sus funciones
				9.4.1	Cambio no autorizado en las configuraciones	U	Restricción del acceso a la información de acuerdo a la clasificación de la información
Computador de escritorio	A8	V8	Uso del recurso para tareas no propias del negocio	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios
				9.2.5	Cambio no autorizado en las configuraciones	U	Revisar los derechos de accesos de los usuarios
				9.2.6	Cambio no autorizado en las configuraciones	U	Adaptación de los derechos de los usuarios de acuerdo a sus funciones

Tabla 23

CONTROL DE ACCESOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				9.4.1	Cambio no autorizado en las configuraciones	U	Restricción del acceso a la información de acuerdo a la clasificación de la información
Servidores	A10	V10	Falta de control de acceso	9.2.2	Cambios en las configuraciones no autorizados	U	Gestionar los derechos de accesos de los usuarios
				9.2.3	Cambios en las configuraciones no autorizados	U	Gestionar los derechos de accesos de los usuarios especiales (admin, super usuarios)
				9.4.1	Cambios en las configuraciones no autorizados	U	Restricción del acceso a la información de acuerdo a la clasificación de la información
				9.2.2	Cambio no autorizado en las configuraciones	S	Gestionar los derechos de accesos de los usuarios
Impresoras	A6	V6	Falta de políticas	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios

Tabla 23

CONTROL DE ACCESOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Equipos de red	A6	V6	Falta de políticas	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios
				9.2.5	Cambio no autorizado en las configuraciones	U	Revisar los derechos de accesos de los usuarios
				9.2.6	Cambio no autorizado en las configuraciones	U	Adaptación de los derechos de usuarios de acuerdo a sus funciones
Correo electrónico	A6	V6	Falta de control de acceso	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios
				9.2.3	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios especiales (admin, super usuarios)
				9.2.5	Cambio no autorizado en las configuraciones	U	Revisar los derechos de accesos de los usuarios
Sistema de gestión de base de datos	A8	V8	Falta de control de acceso	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de los usuarios

Tabla 23

CONTROL DE ACCESOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				9.2.3	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de usuarios especiales (Amin, supe usuarios)
				9.2.5	Cambio no autorizado en las configuraciones	U	Revisar los derechos de accesos de los usuarios
				9.2.6	Cambio no autorizado en las configuraciones	U	Adaptación de los derechos de usuarios de acuerdo a sus funciones
Sistema de monitoreo de seguridad	A8	V8	Falta de control de acceso	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de acceso de los usuarios
				9.2.3	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de accesos de usuarios especiales (Amin, supe usuarios)
				9.2.5	Cambio no autorizado en las configuraciones	U	Revisar los derechos de accesos de los usuarios

Tabla 23

CONTROL DE ACCESOS

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				9.2.6	Cambio no autorizado en las configuraciones	U	Adaptación de los derechos de usuarios de acuerdo a sus funciones
Red LAN	A2	V2	Falta de control de acceso	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de acceso de los usuarios
				9.2.3	Cambio no autorizado en las configuraciones	U	Gestionar el derecho de acceso a los usuarios (admin, superusuarios)
Red Wan	A2	V2	Falta de control de acceso	9.2.2	Cambio no autorizado en las configuraciones	U	Gestionar los derechos de acceso de los usuarios
				9.2.3	Cambio no autorizado en las configuraciones	U	Gestionar el derecho de acceso a los usuarios (admin, superusuarios)

Tabla 24

CIFRADO

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A10	V10	Falta de control de acceso	10.1.2	Uso de claves comunes entre personal del área de administración de servidores	U	Establecer un procedimiento de gestión de clave que considere al menos antigüedad, complejidad, longitud.

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Hardware Portátil	A1	V1	Falta de protección contra el fuego	11.1.4	Daño del equipo	S	Establecer e implementar controles de fuego para áreas seguras

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Perdida de información del equipo	S	Establecer e implementar controles de acceso y sobre los recursos contenidos en las oficinas
				11.1.5	Robo de información	S	Diseño de normas para trabajar en áreas seguras
	A4	V4	Falta de protección por desatención de equipos	11.2.5	Robo de información	S	Diseño e implementación de un procedimiento para la salida de equipos
				11.2.8	Robo de información	S	Informar a los usuarios del uso adecuado de las contraseñas y en la desatención de los equipos.
	A5	V5	Mal funcionamiento del up	11.2.4	Daño en el equipo	S	Implementar un plan de mantenimiento funcional de equipos
	A6	V6	Falta de control de acceso	11.1.3	Acceso por personal no autorizado	S	Establecer e implementar controles de acceso y sobre los recursos contenidos en las oficinas.

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A11	V11	Falta de mantenimiento	11.2.4	Falla o insuficiencia en el uso de los recursos	S	Implementar un plan de mantenimiento preventivo de los equipos
	A14	V14	Ausencia de seguridad fisica adecuada	11.2.5	Robo del equipo	S	Diseño, implementación y difusión de un procedimiento para salida de equipos.
				11.2.6	Robo del equipo	S	Diseño, implementación y difusión de un procedimiento para uso de los equipos fuera de la institución.
Computador de escritorio	A1	V1	Falta de protección contra el fuego	11.1.4	Daño del equipo	S	Establecer control de fuego para áreas seguras
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Perdida de información del equipo	S	Establecer e implementar controles de acceso y sobre los recursos contenidos en las oficinas.
	A4	V4	Falta de protección por desatención de equipos	11.1.5	Robo de información	S	Diseñar normas para trabajar en áreas seguras

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A5	V5	Funcionamiento no confiable de UPS	11.2.4	Daño en el equipo	S	Implementar un plan de mantenimiento funcional de equipos
	A6	V6	Falta de control de acceso	11.1.3	Acceso por personal no autorizado	S	Establecer e implementar control de acceso y sobre los recursos contenidos en las oficinas
	A7	V7	Falta de control de protección de derechos de software	11.2.4	Inconvenientes legales	S	Dentro del plan de mantenimiento considerar la revisión del software autorizado en el equipo
	A10	V10	Falta de mantenimiento	11.2.4	Falla o insuficiencia en el uso de los recursos	S	Implementar un plan de mantenimiento funcional de equipos
	A13	V13	Ausencia de seguridad física	11.2.5	Robo del equipo	S	Diseño, implementación y difusión de un procedimiento para salida de equipos
				11.2.6	Robo del equipo	S	Diseño, implementación y difusión de un

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
							procedimiento para uso fuera de la institución
Servidores	A1	V1	Falta de protección contra el fuego	11.1.4	Daño del equipo	S	Establecer control de fuego para áreas seguras
	A2	V2	Ausencia de seguridad fisica adecuada	11.2.5	Robo/daño del equipo	S	Diseño, implementación y difusión de un procedimiento para salida de equipos
				11.2.6	Robo del equipo	S	Diseño, implementación y difusión de un procedimiento para uso fuera de la institución.
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Perdida de información del equipo	S	Establecer e implementar control de acceso y sobre los recursos contenidas en las oficinas
	A7	V7	Funcionamiento no adecuado del aire acondicionado	11.2.4	Daño en el equipo	S	Implementar un plan funcional de manteniendo de los equipos

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A9	V9	Falta de mantenimiento adecuado	11.2.4	Fallas en el Hardware	S	Implementar un plan funcional de manteniendo de los equipos
	A15	V15	Ausencia de seguridad fisica	11.1.4	Destrucción o inhabilitación del equipo	S	Establecer un control de fuego para áreas seguras
				11.1.6	Destrucción o inhabilitación del equipo	S	Establecer áreas de acceso restringido
Impresoras	A1	V1	Falta de protección contra el fuego	11.1.4	Daño en el equipo	S	Establecer un control de fuego para áreas seguras
	A4	V4	Falta de mantenimiento	11.2.4	Fallas en el Hardware	S	Implementar un plan funcional de manteniendo de los equipos
Equipos de red	A1	V1	Falta de protección contra el fuego	11.1.4	Daño en el equipo	S	Establecer un control de fuego para áreas seguras
	A2	V2	Ausencia de seguridad fisica adecuada	11.1.6	Destrucción o inhabilitación del equipo	S	Establecer áreas seguras de acceso restringido

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Perdida de información del equipo	S	Establecer e implementar control de acceso y sobre los recursos contenidas en las oficinas
	A4	V4	Falta de mantenimiento	11.2.4	Fallas en el Hardware	S	Implementar un plan funcional de manteniendo de los equipos
Equipos de monitoreo	A1	V1	Falta de protección contra el fuego	11.1.4	Daño en el equipo	S	Establecer un control de fuego para áreas seguras
	A2	V2	Ausencia de seguridad fisica adecuada	11.1.6	Destrucción o inhabilitación del equipo	S	Establecer áreas seguras de acceso restringido
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Perdida de información del equipo	S	Establecer e implementar control de acceso y sobre los recursos contenidas en las oficinas
	A4	V4	Falta de mantenimiento	11.2.4	Fallas en el Hardware	S	Implementar un plan funcional de manteniendo de los equipos

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A5	V5	Ausencia de seguridad fisica	11.1.6	Destrucción o inhabilitación del equipo	S	Establecer áreas seguras de acceso restringido
Contrato de Proveedores	A1	V1	Falta de protección contra el fuego	11.1.4	Pérdida total o parcial de la información	S	Establecer un control de fuego para áreas seguras
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Pérdida total o parcial de la información	S	Establecer e implementar control de acceso y sobre los recursos contenidas en las oficinas
Procedimiento	A1	V1	Falta de protección contra el fuego	11.1.4	Pérdida total o parcial de la información	S	Establecer un control de fuego para áreas seguras
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Pérdida total o parcial de la información	S	Establecer e implementar control de acceso y sobre los recursos contenidas en las oficinas
Edificio	A1	V1	Falta de protección contra el fuego	11.1.4	No operatividad del edificio	S	Establecer un control de fuego.
Edificio	A3	V3	Falta de políticas	11.1.3	Robo de bienes	S	Establecer e implementar control de acceso y sobre

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
							los recursos contenidos en las oficinas
	A5	V5	Situación local donde los recursos pueden ser afectados por desastres	11.1.3	Inoperatividad del edificio	S	Establecer e implementar control de acceso y sobre los recursos contenidos en las oficinas.
Canal de Internet	A1	V1	Falta de protección contra el fuego	11.1.4	Interrupción en el uso de los servicios provistos por este canal	S	Establecer un control de fuego para áreas seguras
Correo electrónico	A1	V1	Falta de protección contra el fuego	11.1.4	Interrupción en el uso de los servicios provistos por este canal	S	Establecer un control de fuego para áreas seguras
	A2	V2	Ausencia de seguridad fisica adecuada	11.1.3	Daño o robo	S	Establecer e implementar control de acceso sobre los recursos del correo electrónico
Servicio de energía eléctrica	A1	V1	Falta de protección contra el fuego	11.1.4	Interrupción en todos los servicios	S	Establecer un control de fuego para áreas seguras

Tabla 25

SEGURIDAD FÍSICA Y AMBIENTAL

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Aire acondicionado en el centro de datos	A1	V1	Falta de protección contra el fuego	11.1.4	Degradación y/o fallos de los servidores y equipos del CC	S	Establecer un control de fuego para áreas seguras
Cableado	A1	V1	Falta de protección contra el fuego	11.1.4	Degradación y/o fallos en los servicios	S	Establecer un control de fuego para áreas seguras
	A2	V2	Ausencia de seguridad fisica adecuada	11.1.3	Robo de los cables	S	Establecer e implementar control de acceso sobre estos recursos
	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	11.2.3	Daño total de los cables de datos y comunicación no disponible con el CC	S	Establecer procedimientos de seguridad del cableado en la institución, considerando su ubicación, y normativas internacionales que la rigen

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A4	V4	Falta de protección de los archivos de registro	12.1.4	Fallo por corrupción de servicios	S	Establecer ambientes de desarrolló, preproducción, calidad y producción para desarrollo de pruebas de software.
				12.4.3	Inconsistencia u omisión en la configuración	S	Establecer logs de auditoría para registrar actividad del operador y administrador del sistema.
				12.6.1	Recursos no estén disponibles	S	Configuración de seguridad en el servidor, garantiza mayor control en el uso y recursos.
	A5	V5	Incapacidad de distinguir entre una petición real de una falsa	12.4.1	Daños en el equipo	S	Establecer registros y logs de autoría
				12.1.3	Degradación en los servicios provistos por la base de datos	S	Auditar los programas instalados en el servidor de base de datos.

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				12.2.1	Fallos en los equipos y sus servicios	S	Desarrollar mantenimientos preventivos de equipos.
	A8	V8	Código malicioso desconocido	12.4.1	Daños en el equipo	S	Desarrollar mantenimientos preventivos de equipos.
				12.6.2	Instalación de virus malicioso en la red interna	S	Implementación de un software que prevenga y detecte software malicioso, como virus, troyanos y scripts, para minimizar los riesgos con paralizaciones del sistema o la pérdida de información.
	A14	V14	Falta de monitoreo de servidores	12.4.1	Daños en el equipo	S	Establecer el plan de mantenimiento de servidores.
				12.1.2	Inoperatividad del servicio	S	Adquisición de herramientas para

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
							monitoreo de red y servidores.
				12.7.1	Manipulación de datos sin registro alguno en el log de auditoría	S	Establecer registros y logs de autoría
Canal de Internet	A5	V5	Situación local donde los recursos pueden ser afectados por desastres	12.1.2	Inoperatividad del servicio	S	Seleccionar el proveedor de internet de la compañía en base a la calidad del servicio.
				12.4.1	Daños en el equipo	S	Acceso a Internet para permitir intercambiar información con seguridad vía Internet.
Correo electrónico	A3	V3	Situación local donde los recursos pueden	12.1.2	Inoperatividad del servicio	S	Creación de alertas para notificar fallas de correo.

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
			ser afectados por desastres	12.4.1	Daños en el equipo	S	Utiliza certificados digitales para garantizar el sigilo de las informaciones y software para filtro de contenido, y proteger a la empresa de aplicaciones maliciosas que llegan por ese medio.
	A4	V4	Falta de mantenimiento adecuado	12.4.1	No disponibilidad del servicio.	S	Utiliza certificados digitales para garantizar el sigilo de las informaciones y software para filtro de contenido, y proteger a la empresa de aplicaciones maliciosas que llegan por ese medio.
				12.4.3	Inconsistencia u omisión en la configuración	S	Revisión de configuración de correo electrónico.

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				12.4.3	Inconsistencia u omisión en la configuración	S	Revisión de configuración de correo electrónico.
Sistema de gestión de base de datos	A1	V1	Capacidad no adecuada de recursos	12.1.3	Degradación en los servicios provistos por la base de datos	S	Revisión de indicadores de BD y planes de ejecución de consultas que abarcan más recursos en el BD.
				12.4.1	No disponibilidad del servicio.	S	Creación de alertas para notificar al operador/dba fallas en la base de datos.
	A2	V2	Administador sin la capacitación adecuada	12.4.3	Inconsistencia u omisión en la configuración	S	Revisión periódica de la configuración de la BD. Establecer permiso sysadmin para los usuarios que tienen autorización de administrador.
	A3	V3	Falta de protección actualizada	12.2.1	Degradación del servicio y robo de información	S	Implantación de aplicaciones y dispositivos para la prevención contra

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
							accesos indebidos y el robo de información.
				12.4.1	No disponibilidad del servicio.	S	Habilitar firewall funciona al aislar el acceso a la red de servidores críticos, minimizando los riesgos de invasiones internas a servidores y aplicaciones de misión crítica.
				12.6.2	Instalación de virus malicioso en la red interna	S	Implementación de un software que prevenga y detecte software malicioso, como virus, troyanos y scripts, para minimizar los riesgos con paralizaciones del sistema o la pérdida de información.

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
	A4	V4	Falta de copias de backups continuas	12.1.3	Pérdida total o parcial de información de transacciones ante alguna eventualidad	S	Crear Jobs de backup diario de base de datos.
	A5	V5	Actualizaciones incorrectas	12.1.1	No adecuado funcionamiento del servicio y posibles puntos de vulnerabilidad	S	Crear control para auditar los programas instalados en el servidor. Desactivas las actualizaciones automáticas.
				12.1.2	Inoperatividad del servicio	S	Creación de alertas para notificar la inoperatividad.
				12.4.3	Inconsistencia u omisión en la configuración	S	Definir checklist para la revisión de la configuración de la base.
Sistema de monitoreo de seguridad	A1	V1	Capacidad no adecuada de recursos	12.1.3	Creación de brechas de seguridad	S	Establecer revisiones periódicas de brechas de seguridad por compañía certificada.

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				12.4.1	No disponibilidad del servicio	S	Definir plan de continuidad del negocio bajo este escenario
	A2	V2	Administador sin la capacitación adecuada	12.4.3	Inconsistencia u omisión en la configuración	S	Creación de checklist para la revisión de la configuración
				12.2.1	Degradación del servicio y robo de información	S	Implantación de aplicaciones y dispositivos para la prevención contra accesos indebidos y el robo de información.
	A3	V3	Falta de protección actualizada	12.4.1	No disponibilidad del servicio	S	Creación de alertas para notificar la inoperatividad.
				12.6.2	Instalación de virus malicioso en la red interna	S	Implementación de un software que prevenga y detecte software malicioso, como virus, troyanos y scripts, para minimizar los riesgos con paralizaciones del

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
							sistema o la pérdida de información.
	A4	V4	Falta de copias de backups continuas	12.1.3	Pérdida total o parcial de información de monitoreo	S	Crear Jobs de backup diarios
				12.1.1	No adecuado funcionamiento del servicio y posibles puntos de vulnerabilidad	S	Establecer revisiones periódicas de brechas de seguridad por compañía certificada.
	A5	V5	Actualizaciones incorrectas	12.1.2	Inoperatividad del servicio	S	Definir plan de continuidad del negocio bajo este escenario
				12.4.3	Inconsistencia u omisión en la configuración	S	Revisión periódica de configuración

Tabla 26

SEGURIDAD EN LA OPERATIVA

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servicio de energía eléctrica	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	12.1.2	Interrupción en todos los servicios	S	Revisión periódica de instalaciones eléctricas.
Aire acondicionado en el centro de datos	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	12.1.2	Degradación y/o fallos de los servidores y equipos del CC	S	Mantenimiento periódico de CC
Red Lan	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	12.4.1	No disponibilidad del servicio	U	Establecer e implementar plan de continuidad del negocio.
Red Wan	A3	V3	Situación local donde los recursos pueden ser afectados por desastres	12.4.1	No disponibilidad del servicio	S	Establecer e implementar plan de continuidad del negocio.

Tabla 27

SEGURIDAD EN LAS TELECOMUNICACIONES.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A13	V13	Falta de establecimiento de una conexión segura	13.1.1	Acceso no autorizado para escuchar en la red	S	Establecer cifrados de la conexión
				13.1.2	Acceso no autorizado para escuchar en la red	S	Establecer conexiones seguras para que solo el servidor de destino reciba la información.
				13.1.3	Acceso no autorizado para escuchar en la red	S	Definir políticas de seguridad para conexiones seguras
				13.2.1	Falta de seguridad en el intercambio de información	S	Establecer mecanismos de seguridad en la conexión.
				13.2.2	Falta de seguridad en el intercambio de información.	S	Establecer acuerdos de intercambio de información.
Equipos de red	A13	V13	Falta de establecimiento de una conexión segura	13.1.2	Acceso no autorizado para escuchar en la red	S	Definir políticas de seguridad para conexiones seguras

Tabla 27

SEGURIDAD EN LAS TELECOMUNICACIONES.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Canal de Internet	A3	V3	Falta de políticas	13.1.1	Uso de este servicio para fines no autorizados	S	Establecer cifrados de la conexión
				13.1.2	Acceso no autorizado para escuchar en la red	S	Establecer conexiones seguras para que solo el servidor de destino reciba la información.
				13.2.1	Falta de seguridad en el intercambio de información.	S	Establecer mecanismos de seguridad en la conexión.
				13.2.4	Falta de seguridad en el intercambio de información.	S	Establecer acuerdo de confidencialidad
Red LAN	A3	V3	Falta de establecimiento de una conexión segura	13.1.1	Uso de herramientas externas como sniffers para capturar tráfico	S	Establecer cifrados de la conexión

Tabla 27

SEGURIDAD EN LAS TELECOMUNICACIONES.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				13.1.2	Acceso no autorizado para escuchar en la red	S	Establecer conexiones seguras para que solo el servidor de destino reciba la información.
				13.2.1	Falta de seguridad en el intercambio de información.	S	Establecer mecanismos de seguridad en la conexión.
				13.2.2	Falta de seguridad en el intercambio de información.	S	Establecer acuerdos de intercambio de información.
Red Wan	A3	V3	Falta de establecimiento de una conexión segura	13.1.1	Uso de herramientas externas como sniffers para capturar tráfico	S	Establecer cifrados de la conexión
				13.1.2	Acceso no autorizado para escuchar en la red	S	Establecer conexiones seguras para que solo el servidor de destino reciba la información.

Tabla 27

SEGURIDAD EN LAS TELECOMUNICACIONES.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
				13.2.1	Falta de seguridad en el intercambio de información.	S	Establecer mecanismos de seguridad en la conexión.
				13.2.2	Falta de seguridad en el intercambio de información.	S	Establecer acuerdos de intercambio de información.

Tabla 28

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad

Servidores	A14	V14	Falta de monitoreo en el servidor	14.2.3	Falla en la operatividad del servidor	S	Agregar a la lista de revisión, las aplicaciones una vez actualizado el sistema operativo.

Tabla 29

RELACIONES CON SUMINISTRADORES.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A9	V9	Falta de control para la revisión de contratos	15.1.3	Demora en los servicios prestados por el proveedor	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.
Contrato de Proveedores	A9	V9	Falta de control para la revisión de contratos	15.2.1	Demora en los servicios prestados por el proveedor	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.
				15.2.1	Falla en los servicios soportados por no tener respaldos	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.
Servicio de energía eléctrica	A9	V9	Falta de control para la revisión de contratos	15.2.1	Falla en los servicios	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los

					soportados por no tener respaldos		servicios prestados por el proveedor.
Aire acondicionado en el centro de datos	A9	V9	Falta de control para la revisión de contratos	15.2.1	Falla en los servicios soportados por no tener respaldos	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.
Red Lan	A5	V5	Falta de acuerdos definidos con terceras partes	15.2.1	Falla en los servicios soportados por no tener respaldos	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.
				15.2.2	Demora en los servicios prestados por el proveedor	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.
Red Wan	A5	V5	Falta de acuerdos definidos con terceras partes	15.2.1	Falla en los servicios soportados por no tener respaldos	S	Establecer un contrato donde se expongan los acuerdos, garantías, sanciones sobre los servicios prestados por el proveedor.

Tabla 30

GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Correo electrónico	A6	V6	Los equipos y servidores quedan expuestos sin seguridades de ingreso	16.1.2	Información confidencial expuesta	S	Establecer e implementar control de acceso al área de servidores
	A8	V8	No se cuenta con un área de servidores asegurada que resguarde los equipos y servidores.	16.1.3	Posibles ataques a servidores de correos	S	Diseñar un área de centro de datos
Sistema de gestión de base de datos	A8	V8	Alta de control de acceso	16.1.3	Información confidencial expuesta	S	Establecer e implementar control de acceso al área de servidores
Sistema de monitoreo de seguridad	A8	V8	Los equipos y servidores quedan expuestos sin seguridades de ingreso	16.1.3	Información confidencial expuesta	S	Implementar sistema de monitoreo de red.

Tabla 31

ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Servidores	A6	V6	Funcionamiento confiable del suministro	17.1.1	Degradación del servicio	S	Mantenimiento preventivo a los servidores
				17.1.2	Degradación del servicio	S	Establecer control de acceso a área de servidores
				17.1.3	Degradación del servicio	S	Implementar herramientas de monitoreo
	A12	V12	Falta de planes de continuidad del negocio	17.1.1	Pérdida total o parcial del servicio	S	Implementar plan de mantenimiento funcional de los equipos.
				17.1.2	Pérdida total o parcial del servicio	S	Verificación de aplicaciones instaladas en los servidores.
				17.1.3	Pérdida total o parcial del servicio	S	Implementar herramientas de monitoreo
				17.2.1	Pérdida total o parcial del servicio	S	Elaborar plan de contingencia TI
Equipos de monitoreo	A3	V3	Funcionamiento confiable del suministro	17.2.1	Pérdida total o parcial del servicio	S	Implementar herramientas de monitoreo

Tabla 31

ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

ACTIVO	ID AMENAZA	ID Vulnera	Vulnerabilidad	Control ISO 27002	Riesgo	Gestión	Actividad
Sistema de gestión de base de datos	A5	V5	Pérdida de servicio	17.2.1	Pérdida del servicio, afecta la continuidad del negocio	S	Elaborar plan de contingencia TI
Sistema de monitoreo de seguridad	A5	V5	Pérdida de servicio	17.2.1	Pérdida del servicio, afecta la continuidad del negocio	S	Elaborar plan de contingencia TI
Red Lan	A5	V5	Pérdida de servicio	17.2.1	Pérdida del servicio, afecta la continuidad del negocio	S	Establecer e implementar plan de continuidad del negocio.
Red Wan	A5	V5	Pérdida de servicio	17.2.1	Pérdida del servicio, afecta la continuidad del negocio	S	Establecer e implementar plan de continuidad del negocio.

ANEXO 2

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

ISO27000.es PATROCINADO POR:

GES CONSULTOR
GOBIERNO T.I. - RIESGO - CUMPLIMIENTO