UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERIA DE SISTEMAS Y ADMINISTRACION DE EMPRESAS

CARRERA PROFESIONAL DE INGENIERIA DE SISTEMAS

"IMPLEMENTACION DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA LA CONTINUIDAD DEL NEGOCIO EN BASE A LA NORMA ISO 27002 EN EL AREA DE SISTEMAS DE LA EMPRESA CORPORACION LA SIRENA"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

LAOR FLORES, NATALY SUSAN

Villa El Salvador
2016

DEDICATORIA

Dedico esta tesis a Jehová Dios porque en su infinita bondad y amor me da las fuerzas para seguir tras mis metas, a mis padres Jesús y Bertha por sus consejos, el ánimo y su guía, a mis hermanas Helen y Karen Laor por su apoyo y buen ejemplo día a día.

AGRADECIMIENTO

Agradezco a la empresa Corporación La sirena y a mi Jefe de Sistemas Wolfang Zdenko Lojas Ávila por permitirme aplicar mi proyecto en la empresa, compartir sus conocimientos y facilitarme los días necesarios para la investigación.

A mi asesor Teodoro Díaz Leiva por su guía, consejos, motivación y estar siempre presto a guiarme en mi investigación.

A mi asesor Mg. Ing. Hernán Ochoa Carbajal, por ayudarme a aclarar mis dudas y guiarme en la metodología de mi proyecto de tesis.

Agradezco a mis compañeros de esta casa de estudios por sus consejos, por siempre compartir conocimientos y motivarme en la especialidad que tanto me gusta, Seguridad de la Información.

A mi profesor José Escajadillo, por su guía a la hora de elegir y definir mi título de proyecto de tesis.

Agradezco a mi primo Rony Hanco por sus explicaciones interesantes y sencillas para mi proyecto de tesis.

INDICE

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

El presente proyecto la inicie con la necesidad de poder darle una mayor seguridad a la valiosa información del centro donde laboro, para ello implementaré un Plan de Seguridad de la información que le permita a la empresa Corporación La Sirena en su área de Sistemas y su proceso Administración de servidores, mitigar sus riesgos y continuar con sus procesos de negocio pese a incidentes.

La información es un activo sumamente importante en una organización y requiere en consecuencia una protección adecuada y tener un Plan de seguridad de la información, permite reaccionar de forma adecuada ante incidentes; en esta investigación, en base a la Norma ISO 27002 y su Dominio 17 “Aspectos de la seguridad de la información en la gestión de la continuidad del negocio” nos permite implementar un Plan que se amolde a la necesidad de la organización y le permita la continuidad del negocio.

Para el logro de los objetivos de este proyecto se gestionara un plan de seguridad de la información que tiene como característica principal resguardar la integridad, confidencialidad e integridad de los activos de información en la empresa, Para ello atreves de un minucioso análisis de los riesgos a los que está expuesto los activos de información y un plan de tratamiento del riesgo ayudaran a proteger estos activos de los procesos críticos y operativos del negocio frente a eventos inesperados la cual interrumpe la operación de la empresa.

El presente proyecto consta de 3 capítulos. Ellos son:

En el capítulo I: se presenta el planteamiento del problema, justificación del Problema, limitación del Proyecto, Formulación del Problema con los Objetivos Generales y Específicos.

En el capítulo II: muestra el Marco teórico, en el que están planteadas las bases teóricas relacionadas con un plan de Continuidad de la seguridad de la Información, definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación.

En el capítulo III: Se especifican los materiales, métodos y herramientas utilizadas para el desarrollo del trabajo de investigación. También se define la metodología a emplear, la cual es la resultante de un estudio de distintas metodologías, también está destinado a la presentación de la pruebas y resultados del trabajo de investigación.

CAPÍTULO I

1. PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la Realidad Problemática

La empresa Corporación La Sirena es una empresa peruana distribuidora local y nacional de productos ferreteros, cuenta con distintas áreas de operación como Área de Sistemas, ventas, compras, logística, marketing, tienda y almacén surquillo. Cada proceso realizado genera un flujo de información tales como guías, facturas, correos corporativos, fichas entre otros la cual son de vital importancia para la funcionalidad de la empresa. Esta información en la mayoría de los casos, es almacenado en diferentes medios tanto físicos como electrónicos, además es puesta a disposición del personal que requiere hacer uso de esta información para la toma de decisiones, realizar planes, reportes, inventarios, entre otros.

El acceso no autorizado a la información se ha vuelto más fácil debido a los tantos métodos existentes y nuevos para extraer información, esto ha permitido que sea más difícil salvaguardar la información y sus métodos

de transmisión; ya sean estos comunicados verbales, archivos, documentos, base de datos, entre otros.

Por otra parte día a día la empresa se enfrenta a amenazas, desde un robo informático por el personal interno o externo, modificación de información intencional y no intencional, cortes de luz, inundaciones, terremotos, incendios, falta de personal adecuado, entre otros, todos estos influyen significativamente en los procesos de la empresa y sobre todo al proceso critico de Administración de los servidores del Área de Sistemas.

Por lo anterior mencionado es necesaria la implementación un Plan De Seguridad de la Información que contenga procedimientos, controles, normas, que permitan asegurar la confidencialidad, disponibilidad e integridad de la información; con ello garantizar un adecuado acceso a la información a quien corresponda, esté disponible cuando se requiera y permanezca tal como fue creada por sus propietarios esta de un Plan de Seguridad de la Información

1.2. Justificación del Problema

Debido a los riesgos que están expuestos los activos de la información, el impacto que la interrupción de estos puede causar es preponderante; por tanto definir de normas y metodologías que ayuden a reducir y mitigar estos riesgos.

Por ello se propone implementar un plan de seguridad de la información para la continuidad del negocio de la empresa en base a la

ISO 27002 Dominio 17 la cual nos brinda procedimientos, lineamientos necesarios para identificar y evaluar los riesgos, amenazas, vulnerabilidades de los activos de la Información, implementar controles en los procesos que son implicados en el área de sistemas y así mantener y mejorar la continuidad del negocio.

1.3. Delimitación del Proyecto

Espacial El Proyecto se ejecuto en el proceso de Administración de Servidores en el Área de Sistemas de la empresa Corporación La Sirena.

Temporal El Proyecto se ejecutó desde el mes Junio de 2015 hasta mes de Noviembre del año 2015.

1.4. Formulación del Problema

¿Cómo la implementación de un plan de seguridad de la información en base a la Norma ISO 27002 Dominio 17 permitirá la continuidad del negocio en el Área Sistemas de Corporación La Sirena?

1.5. Objetivos

1.5.1. Objetivo General

Implementación de un plan de la seguridad de la información en base a la Norma ISO 27002 Dominio 17 que permita la continuidad del negocio en el Área Sistemas de Corporación La Sirena.

1.5.2. Objetivos Específicos

- Reconocimiento de la situación actual de la seguridad de la Información en el área de sistemas para contribuir con la continuidad del negocio de la empresa Corporación La Sirena.
- Analizar y Gestionar el riesgo de la Seguridad de la Información a los activos del área de Sistemas en la Administración de los servidores que permitan la continuidad del negocio en el área de sistemas de Corporación La Sirena.
- Realizar un Plan de tratamiento de los Riesgos que permitirá la continuación del negocio en el área de sistemas de Corporación La Sirena.

CAPÍTULO II

MARCO TEÓRICO

2.1. Antecedentes de la Investigación

NACIONAL:

"Diseño e Implementación de un Sistema de Gestión de seguridad de Información en Procesos Tecnológico" presentado por Barrantes Porras Carlos Eduardo y Hugo Herrera Javier Roberto (2014).

La Siguiente investigación aplicada en la empresa CardPerú S.A. en sus procesos tecnológicos no cuenta con controles, medidas, procedimientos de seguridad necesarios para resguardar sus activos de información, tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicio, están expuestas a altos niveles de riesgo frente a las diversas amenazas. Su objetivo es de reducir y mitigar los riesgos de los activos de información, que ponen en peligro los recursos, servicios y continuidad de los procesos tecnológicos. Para el logro de sus objetivos sea tomado distintas metodologías y como base la ISO 17799:2005 (versión anterior a la ISO 27002), partiendo de esta

se siguen otras más como Alexander: 2007 sus buenas prácticas permiten el análisis y evaluación de los riesgos y MAGERIT mediante un análisis y gestión de los riesgos permite planificar medidas para mitigar riesgos manteniendo el control de estos.

Este trabajo de investigación me resulta importante ya que plantea metodologías en base a la NORMA ISO 17799-2005 (Versión similar a la ISO 27002) para conseguir un plan para la seguridad de la información mitigando los riesgos en el área tecnológica.

NACIONAL:

"Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo" presentada por Hans Ryan Espinoza Aguinaga (2013).

Para el caso del presente proyecto de tesis, se realizó un enfoque en la seguridad de una empresa del rubro de producción y distribución de alimentos de consumo masivo, donde existe la necesidad de proteger la información. Como objetivo del presente proyecto es analizar y diseñar un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 27001:2005 lo que implica utilizar diferentes herramientas y metodologías como MAGERIT, con un previo reconocimiento de los activos de información.

Para garantizar la seguridad de esta información, las empresas deben dejar de actuar reactivamente en respuesta a los incidentes y problemas relacionados con la seguridad de información y empezar a realizar un conjunto de acciones como identificar, analizar y gestionar los activos y definir su impacto, por último la alta gerencia debe decidir qué acciones se tomarán para mitigar los riesgos.

Esta tesis es interesante ya que muestra cómo implementar un sistema de gestión de seguridad de la información en base a la Norma ISO 27001 y los controles de la ISO 27002, partiendo de la identificación, análisis y gestión de riesgos de la seguridad de la información aplicando la metodología MAGERIT la cual será usando para mi investigación.

INTERNACIONAL:

"Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial" presentada por María Gabriela Hernández Pinto (2006), Guayaquil-Ecuador.

Este trabajo de investigación tiene como objetivo obtener un nivel considerable de seguridad y para lograrlo realiza una propuesta, "Diseño de un Plan Estratégico de Seguridad de Información" en base a normas y estándares internacionales como la ISO 17799 incluyendo el Dominio "Continuidad del Negocio" (versión anterior a la ISO 27002).

Este proyecto de investigación me permite tener un enfoque específico de cómo puedo definir y clasificar los activos de información, los riesgos en base a Normas siendo de mi interés la Norma ISO 27002 (ISO 17799 versión anterior) armando un Plan de seguridad de Información en el área de sistemas en la Administración de Servidores.

2.2. Bases teóricas

2.2.1. Seguridad de la Información

La Seguridad de la Información es la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información.[1]

Seguridad de la Información sería la disciplina que se encargaría de proporcionar, evaluar los riesgos y las amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, bajo normativa o buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad en el manejo de la información (activos).

[1] Julián Gonzales. (2012 - 2014). ¿Seguridad Informática o Seguridad de la Información?, de Seguridad para Todos, Sitio web: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

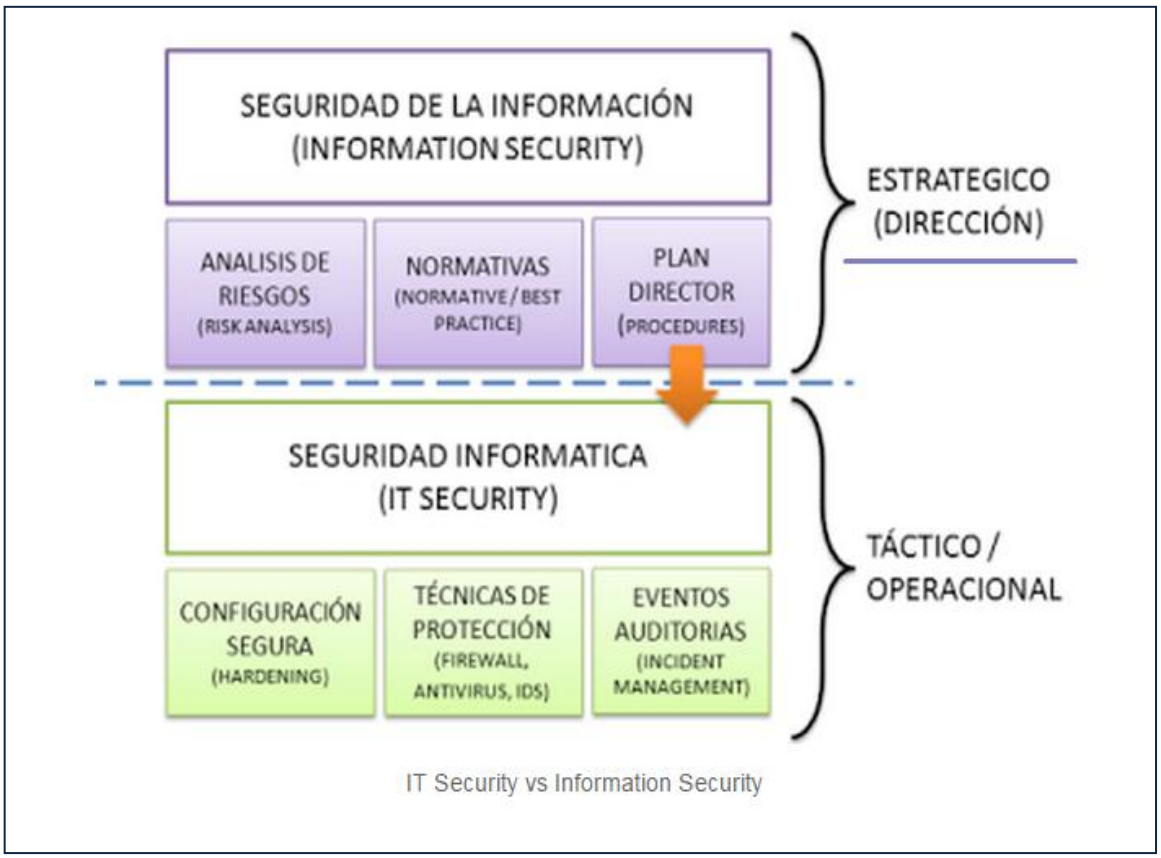


FIGURA 01: SEGURIDAD DE LA INFORMACION-SEGURIDAD INFORMATICA

Julián Gonzales. (2012 - 2014). ¿Seguridad Informática o Seguridad de la Información?, de Seguridad para Todos, Sitio web: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html

La Seguridad de la Información se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para alcanzar el objetivo se apoya en la Seguridad Informática (que estaría gobernada por las directrices de la Seguridad de la Información), es decir, a pesar de ser disciplinas diferentes, la una no puede "ir" sin la otra. De modo que la Seguridad de la Información será la encargada de "regular" y establecer las pautas a seguir para la protección de la información.[2]

Bases de la Seguridad de la Información, un sistema será seguro o fiable si podemos garantizar tres aspectos:

- **Confidencialidad**: acceso a la información solo mediante autorización y de forma controlada.
- **Integridad**: modificación de la información solo mediante autorización.
- **Disponibilidad**: la información del sistema debe permanecer accesible mediante autorización.

[2]Elvira Mifsud. (2012-2015). Introducción a la Seguridad Informática/Seguridad de la Información. España, Madrid, de Gobierno de España Sitio web: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

FIGURA 02: PILARES DE LA SEGURIDAD DE LA INFORMACION

Extraída de: página web http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1
(2012-2015)

2.2.2. Confidencialidad

Es la accesibilidad a los sistemas y datos, solo para su uso autorizado. Es un requisito necesario para garantizar que el sistema trabaje puntualmente, con prontitud y que no se desvíe el servicio a ningún usuario autorizado. La disponibilidad protege al sistema contra determinados problemas contra los intentos deliberados o accidentales de realizar un borrado no autorizado de datos, de causar cualquier tipo de denegación del servicio o de acceso a los datos y de los intentos de utilizar el sistema o los datos para propósitos no autorizados.

2.2.3. Integridad

Se encarga de garantizar que la información del sistema no haya sido alterada por usuarios no autorizados, evitando la perdida de consistencia. Presenta dos fases:

- *Integridad de datos,* Es la propiedad de que los datos no hayan sido alterados de forma no autorizada, mientras se almacena, procesan o transmiten.
- *Integridad del Sistema.* Es la cualidad que posee un sistema cuando realiza la función deseada, de manera no deteriorada y libre de manipulación no autorizada. La integridad es el objetivo de seguridad más importante después de la disponibilidad.

2.2.4. Disponibilidad

Es el requisito que intenta que la información privada o secreta no se revele a individuos no autorizados. La protección de la confidencialidad se aplica a los datos almacenados durante su procesamiento, mientras se transmiten y se encuentran en tránsito. Para muchas organizaciones, la confidencialidad se encuentra, frecuentemente, detrás de la disponibilidad y de la integridad, en términos de importancia, para algunos sistemas y para tipos específicos de datos como los autenticadores, la disponibilidad es de extrema importancia.

2.2.5. Análisis de Riesgo

El proceso de gestión de riesgos identifica y prioriza los peligros inherentes al desarrollo de un producto, sistema u organización. La gestión del riesgo es una parte importante de la gestión de la seguridad y se define como el proceso que se encarga de identificar y cuantificar la probabilidad de que se produzcan amenazas y de establecer un nivel aceptable de riesgo para la organización, considerando el impacto potencial de un incidente no deseado. La valoración de riesgos es el proceso consistente en identificar los problemas antes de que aparezcan.[3]

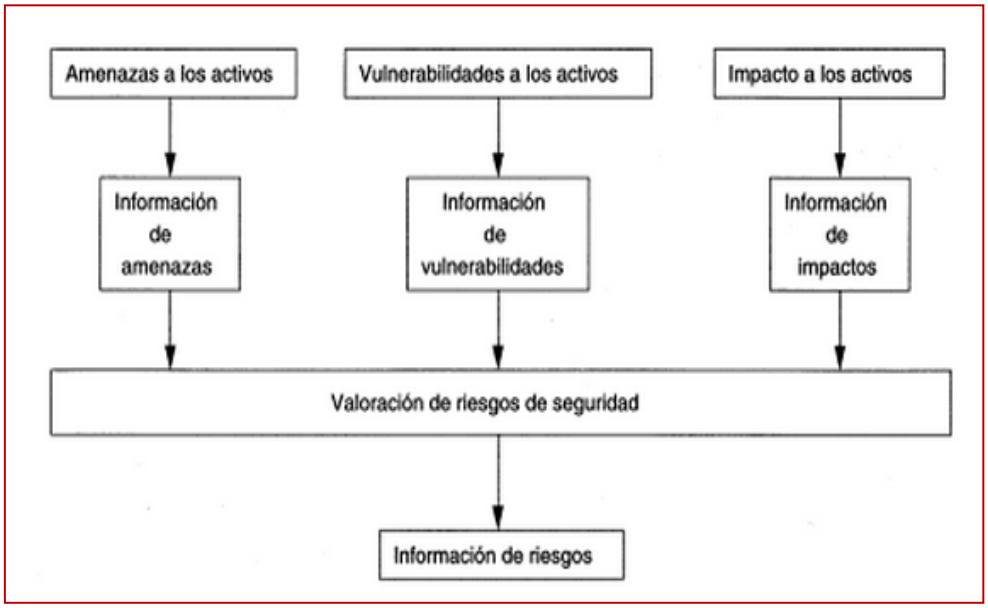


FIGURA 03: COMPONENTES DEL PROCESO DE RIESGO
Extraída del libro: Javier Areitio Bertolín. (2008)Seguridad de la información. Redes, informática y sistemas de información.

[3]Javier Areitio Bertolín. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Magallanes.

2.2.6. Amenazas

Se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información.

Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información.

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas de ingeniería social, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales.

Tipos de Amenazas:

Las amenazas pueden clasificarse en dos tipos:

- Intencionales, en caso de que deliberadamente se intente producir un daño (por ejemplo el robo de información aplicando la técnica de trashing, la propagación de código malicioso y las técnicas de ingeniería social).
- No intencionales, en donde se producen acciones u omisiones de acciones que si bien no buscan explotar una vulnerabilidad,

ponen en riesgo los activos de información y pueden producir un daño (por ejemplo las amenazas relacionadas con fenómenos naturales).[4]

2.2.7. Vulnerabilidad

La Vulnerabilidad es la capacidad, las condiciones y características del sistema mismo (incluyendo la entidad que lo maneja), que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacitad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.[5]

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño. Dependiendo del contexto de la institución, se puede agrupar las vulnerabilidades en grupos característicos:

Ambiental, Física, Económica, Social, Educativo

Institucional y Política.

[4]Departamento de Seguridad Informática. (2012). Amenazas a la Seguridad de la Información. Buenos Aires, Argentina, de Universidad Nacional de Luján Sitio web: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12

[5]Ing. Carlos Ormella Meyer. (2014). Normas ISO de SI. Madrid, España, de Red Informática de criptografía y seguridad de la información Sitio web: http://www.criptored.upm.es/descarga/normas_segu_info_marzo_2014.pdf

FIGURA 04: Vulnerabilidades

Ing. Carlos Ormella Meyer. (2014). Normas ISO de SI. Madrid, España, de Red Informática de criptografía y seguridad de la información Sitio web: http://www.criptored.upm.es/descarga/normas_segu_info_marzo_2014.pdf

2.2.8. NORMA ISO 27002

Es una guía de recomendaciones de buenas prácticas para la gestión de la seguridad de la información.

Las norma ISO/IEC 27002 está enfocada a todo tipo de organizaciones (por ejemplo empresas comerciales, agencias, gubernamentales, organizaciones sin ánimo de lucro), tamaños (pequeña, mediana o gran empresa), tipo o naturaleza.

Está organizado en base a los 14 dominios, 35 objetivos de control y 114 controles.[6]

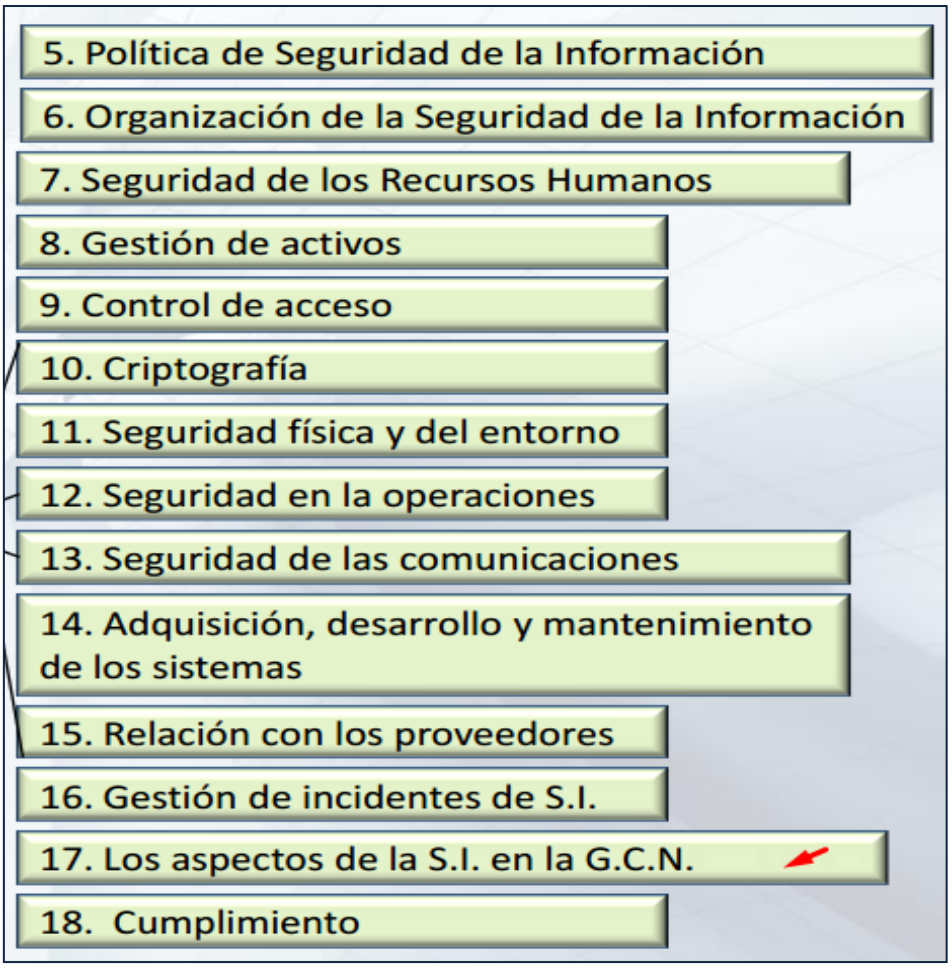


FIGURA 05: DOMINIOS DE LA ISO 27002-2013

Ing. Manuel Collazos Vallager, Colegio de Ingenieros del Perú, (2014). La nueva versión ISO:27001-2013, Lima, Perú.

[6] Ing. Manuel Collazos Vallager, Colegio de Ingenieros del Perú, (2014). La nueva versión ISO: 27001: 2013, Lima, Perú.

2.2.9. NORMA ISO 27002 Clausula 8.1

Activos relacionados con las instalaciones de procesamiento de información y la información deben ser identificados y un inventario de los activos deberá estar redactado y mantenido.[7]

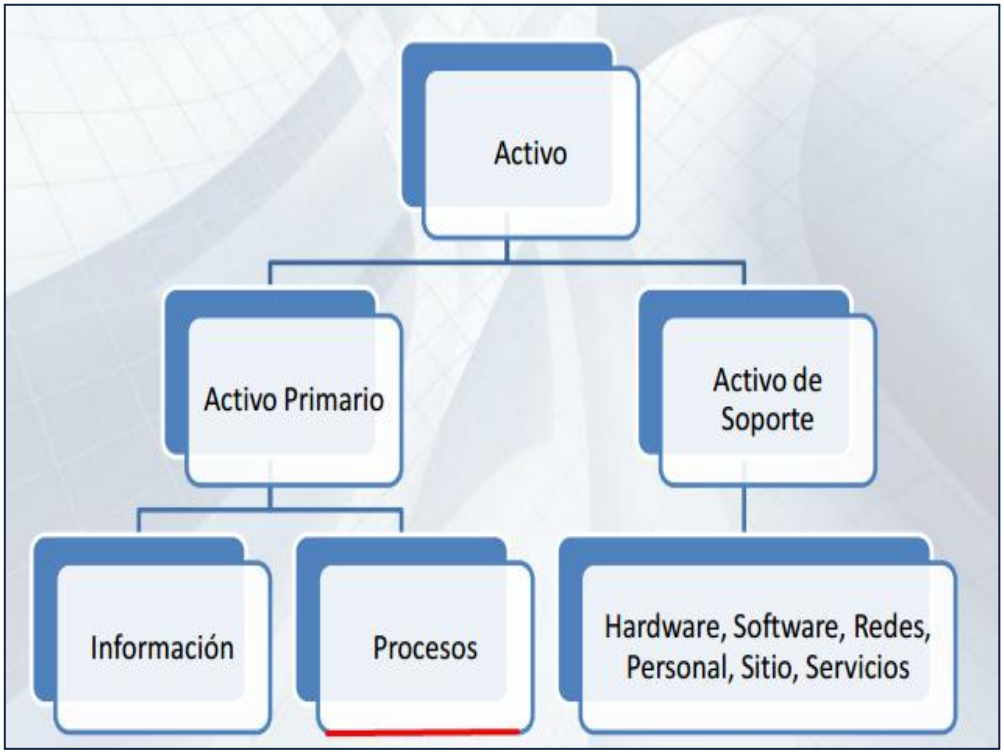


FIGURA 06: ACTIVOS DE SEGURIDAD DE INFORMACION

Luis Gómez Fernández Ana Andrés Álvarez (2012) "Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes" 2° edición, AENOR, Madrid-España

[7] Luis Gómez Fernández Ana Andrés Álvarez (2012) "Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes" 2° edición, AENOR, Madrid-España

2.2.10. Dominio 17 “Aspectos de la Seguridad de la Información para la Continuidad del negocio”

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se debería integrar dentro de los procesos críticos de negocio, aquellos requisitos de gestión de la seguridad de la información con atención especial a la legislación, las operaciones, el personal, los materiales, el transporte, los servicios y las instalaciones adicionales, alternativas y/o que estén dispuestos de un modo distinto a la operativa habitual.

Las organizaciones deberían verificar la validez y la efectividad de las medidas de continuidad de la seguridad de la información regularmente, especialmente cuando cambian los sistemas de información, los procesos, los procedimientos y los controles de seguridad de la información, o los procesos y soluciones establecidas para la gestión de la continuidad de negocio.

Instruir al personal involucrado en los procedimientos de reanudación y recuperación en relación a los objetivos del plan,

los mecanismos de coordinación y comunicación entre equipos (personal involucrado), los procedimientos de divulgación en uso, los requisitos de la seguridad, los procesos específicos para el personal involucrado y responsabilidades individuales[8].

- **CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN**

Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

Las organizaciones deberían verificar la validez y la efectividad de las medidas de continuidad de la seguridad de la información regularmente, especialmente cuando cambian los sistemas de información, los procesos, los procedimientos y los controles de seguridad de la información, o los procesos y

[8]DRI International. (2013). El portal de ISO 27002 en Español. España, de ISO 27002.ES Sitio web: http://www.iso27000.es/iso27002_17.html

soluciones establecidas para la gestión de la continuidad de negocio.

- Actividades de control del riesgo

Planificación de la continuidad de la seguridad de la información: La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.

Implantación de la continuidad de la seguridad de la información: La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.

Verificación, revisión y evaluación de la continuidad de la seguridad de la información: La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas[9].

[9] Versión ISO 27002 (2013). ISO 27002.es – El anexo de ISO 27001 en Español. España, web: http://www.iso27002.es/

2.2.11. Área de Sistemas

El área de Sistemas está compuesta de cuatro procesos como la Administración de Servidores, Desarrollo de Sistemas, Administración de BD y Administración de Infraestructura.

Para este estudio se ha escogido el proceso más Crítico del área, la Administración de los Servidores siendo este el que alberga los sistemas principales de la empresa.

2.2.12. Metodología de Gestión de Riesgos (Alexander: 2007)

A. Análisis de riesgo

El objetivo del análisis de riesgo es identificar riesgos, amenazas y vulnerabilidades basados en la identificación de activos (procesos).

El análisis y evaluación de riesgo y las decisiones que se tomen en reacción con el tratamiento del riesgo en la empresa gira alrededor del proceso crítico en el área de sistemas.[10]

Este proceso clave le permite a la organización continuar con el negocio por tanto se requiere asegurar su protección, su correcta operación y continuidad.

[10]Javier Areitio Bertolín. (2008). Seguridad de la información. Redes, informática y sistemas, Editorial Alfaomega, Lima, Perú.

De acuerdo a la metodología el alcance de la evaluación de riesgo son los activos implicados a la Administración de los Servidores del área de Sistemas de la empresa Corporación La Sirena.

El Administrador de Servidores es el responsable de la administración de los mismos, tanto hardware como software, seguridad perimetral, seguridad de la Información, supervisión de la infraestructura del cableado estructurado de red de internet y telefonía.

B. Identificación de Activos

El análisis y evaluación del riesgo y las decisiones que se tomen en relación con el tratamiento del riesgo en el área de sistemas giran alrededor de los activos de información identificados.

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones y su continuidad. Por esta razón, necesitan tener protección para asegurar una correcta operación del negocio y continuidad en sus operaciones

La administración de los servidores abarca los siguientes activos.

- Activos de Hardware: como Servidores AS400, Proxy/Firewall, Samba, SIDIGE, NEXTEL (Pedidos), AVAYA, etc.
- Activos de Software: Aplicaciones SPEED, Consulta/venta, Cotización, Gestión de compra, programas, etc. Infraestructura de RED Internet/datos y telefonía.
- Activos de Información: Manuales (datos, usuarios, contraseñas, procedimientos) normas establecida.
- Activos Humanos: Responsables de las actividades.

Teniendo claro el activo (proceso) se podrá aplicar de forma correcta el análisis y gestión de riesgo y por ende establecer las buenas prácticas de la norma ISO 27002 DOMINIO 17 Aspectos de la seguridad de la Información para la Continuidad del Negocio.

La tasación de los activos se debe realizar por un grupo compuesta por personas involucradas en el proceso que abarca el alcance del modelo. Es de suma importancia que los dueños de los activos es decir la persona que tiene una responsabilidad por el control, desarrollo, mantenimiento, el uso y seguridad de los activos aprobada por autoridades jefe de sistemas y Gerencia.

Estos activos ya correctamente identificados serán tasados para visualizar su impacto en la empresa por su deterioro o por sus fallas en (1) Confidencialidad, (2) Integridad, (3) Disponibilidad.

C. Tasación de los Activos

Cada activo se taza, utilizando una escala de Likert Donde el valor 1 significa muy poco y 5 muy alto. La pregunta que debe efectuarse para utilizar la escala es: ¿Cómo una pérdida o falla en un determinado activo afecta la confidencialidad, la Integridad y disponibilidad? [11]

Scala de Likert	
5	Muy alto
4	Alto
3	Medio
2	Bajo
1	Muy bajo

TABLA 01: Escala de Likert

Fuente el Autor

El responsable de los activos debe definir apropiadamente la clasificación de seguridad y los derechos de acceso a los activos y mantener una revisión periódica de los derechos de

[11]Luz Marina Méndez Hinojosa, José Armando Peña Moreno (2007).Manual práctico para el diseño de la escala de likert, México.

accesos y la clasificación de seguridad. A demás debe de ser útil definir, documentar e implementar reglas para el uso aceptable de activos, describiendo acciones permitidas y prohibidas en el uso cotidiano de los activos. Las personas que utilizan los activos, deben estar conscientes de estas reglas como parte de su descripción del puesto.

D. Identificación de Amenazas y Vulnerabilidades

Una vez realizada la tasación, se efectúa la identificación de la Amenazas. Una amenaza para poder causar daño a un activo debe de estar asociado a una vulnerabilidad en el sistema, aplicación o servicio. Un incidente es cuando coincide una vulnerabilidad y una amenaza afectando el funcionamiento de la organización es decir es la concreción de una amenaza.

Para la definición de la Amenazas y vulnerabilidades se realizó reuniones con las personas encargadas de estos activos, con la finalidad de explorar las principales amenazas para cada activo de información.

- ✓ Amenazas:

Una amenaza puede causar un incidente no deseado, que puede provocar daños o perdidas de todo tipo en la organización. Los ataques son principalmente en forma de

revelación, de destrucción, de modificación no autorizada, de indisponibilidad o de pérdida de información.[12]

Clasificación de Amenazas:

- Amenazas naturales (inundaciones, sismos, incendios, tormentas, etc.)
- Amenazas a instalaciones (energía, explosión, fuego, fallas, etc.)
- Amenazas humanas (Transporte, renuncias, huelgas, accidentes, etc.)
- Acceso no autorizado
- Amenazas tecnológicas (virus, hacking, red, fallas de software, hardware)
- Amenazas operacionales (crisis, legal, fallas, equipos, proveedores)

✓ Vulnerabilidad:

Una amenaza para poder causar algún tipo de daño a un activo, tendrá que explotar la vulnerabilidad del sistema, aplicación o servicio.

Una vulnerabilidad por sí misma no causa daño alguno; es, simplemente una condición o un conjunto de condiciones que pueden permitir que una amenaza afecte a un activo.

[12]Javier Areitio Bertolín. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Magallanes.

Clasificación de Vulnerabilidades:

- Seguridad de los recursos humanos, (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, carencia de procedimientos que aseguren la entrega de activos al término del contrato del contrato de trabajo, empleados desmotivados)
- Control de acceso, (Segregación inapropiada de redes, falta de políticas sobre escritorio y pantalla limpia, políticas incorrectas para el control de acceso, pasword sin modificarse)[13]
- Seguridad física y ambiental, (control de acceso físico inadecuado a la oficina, ubicación en áreas sujetas a inundaciones, carencias de programas para sustituir equipos, susceptibilidad de equipos a variaciones de voltaje)[14].
- Gestión de operaciones y comunicaciones, (Complicadas interfaces para usuarios, Gestión de red inadecuada, carencia de control de copiado de información, falta de protección en redes).
- Mantenimiento, adquisición de sistemas de información, (protección inadecuada de claves criptográficas, carencia de

[13] Ecu Red conocimiento con todos y para todos. (2015). Ciencias informáticas y tecnologías. Cuba, web: http://www.ecured.cu/Sistemas_de_control_de_acceso.

[14] Jose Luis Ortiz Barrios, Prezi (2013).Seguridad Física y ambiental. web: Jhttps://prezi.com/c_c7ejl9r9hv/seguridad-fisica-y-ambiental/.

validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos)[15].

Una vez identificadas las vulnerabilidades, para cada una de ellas, se debe evaluar la posibilidad de que sean explotadas por las amenazas.

Se debe de entender que las vulnerabilidades y amenazas deben presentarse juntas, para poder causar incidentes que pudiesen dañar los activos

E. Calculo de las Amenazas y Vulnerabilidades

Una vez identificadas la Amenazas y Vulnerabilidades, es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. “El riesgo es la posibilidad de que se produzca un impacto determinado en un activo en toda una organización y explote una vulnerabilidad en particular”[16]

Conviene calcular la posibilidad de la presencia de amenazas se deben de considerar los siguientes aspectos de la amenaza:

[15] Versión ISO 27002 (2013). ISO 27002.es – El anexo de ISO 27001 en Español. España, web: https://iso27002.wiki.zoho.com/12AdquisicionDesarrolloMantenimiento.html

[16] Javier Areitio Bertolín. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Magallanes.

- ✓ Amenazas deliberadas. La posibilidad de amenazas deliberadas en la motivación, capacidad y recursos disponibles para posibles atacantes.
- ✓ Amenazas accidentales. La posibilidad de amenazas accidentales puede estimarse utilizando la experiencia y las estadísticas.
- ✓ Incidentes del pasado. Los incidentes ocurridos en el pasado ilustran los problemas en el actual sistema de protección.
- ✓ Nuevos desarrollos y tendencias. Esto incluye informes, novedades y tendencias obtenidas de diferentes medios, como internet.

F. Análisis del Riesgo y su Vulnerabilidad

El tratamiento del riesgo se define, como el conjunto de decisiones tomadas con cada activo de información. De ahí que el objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos y en el cálculo de las amenazas y vulnerabilidades.

Los Riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad, y disponibilidad y del cálculo de la posibilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Para el cálculo del riesgo se tomara el más apropiado para el área de sistemas y sus requerimientos de seguridad. Los niveles de riesgo calculados proveen un medio para poder priorizarlos riesgos e identificar aquellos otros que son más problemáticos para el Área de Sistemas.

2.2.13. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT)

Es una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

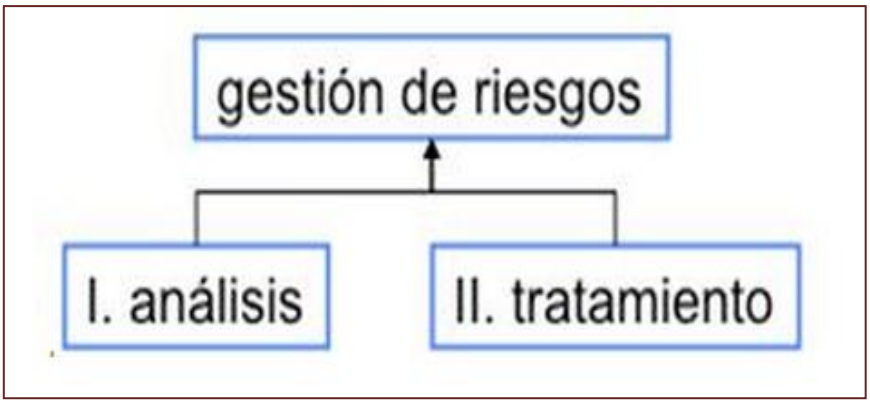


FIGURA 07: GESTION DE RIESGO

Extraída de: Portal de Administración Electrónica. (2012). MAGERIT v. 3.Metodologia de análisis y gestión de riesgos de los SI. España, de Gob. España Sitio web: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.ViR6s9Ivfct

ONBJETIVOS

MAGERIT persigue los siguientes objetivos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
4. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.[17]

A. Análisis y Gestión de los Riesgos en MAGERIT

Las tareas de análisis y gestión de riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de gestión de riesgos permiten

[17]Portal de Administración Electrónica. (2012). MAGERIT v. 3.Metodologia de análisis y gestión de riesgos de los SI. España, de Gobierno de España Sitio web: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.ViR6s9Ivfct

elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que se acepta la Dirección.

La implantación de los controles de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.

Este esquema de trabajo debe ser repetitivo pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto. El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.

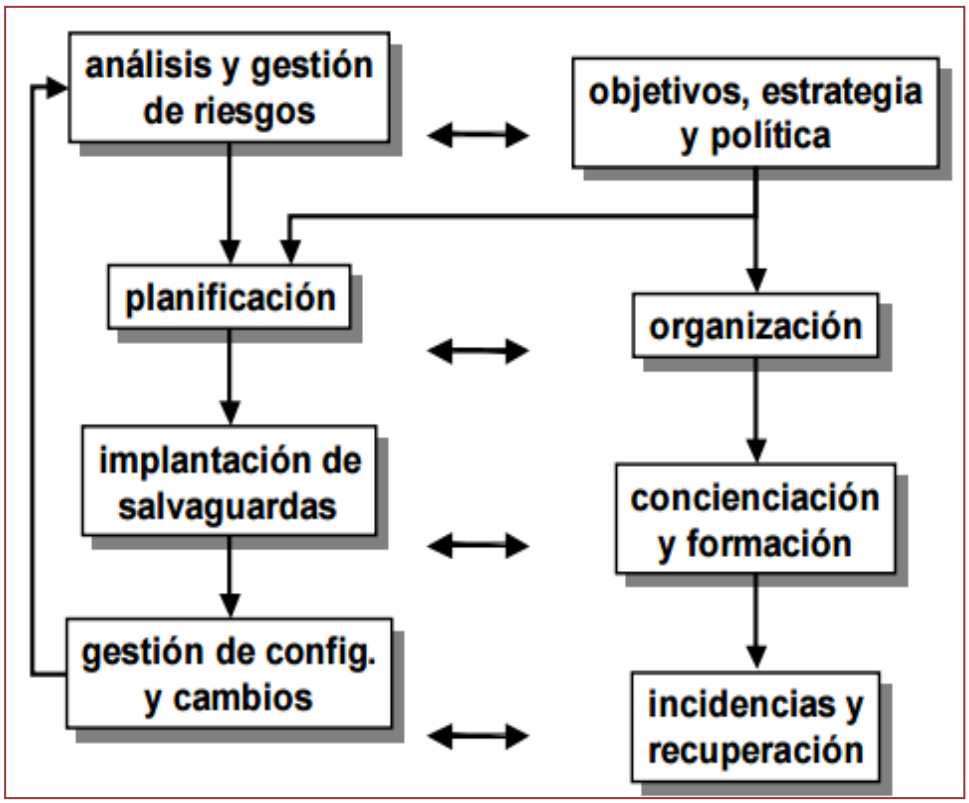


FIGURA 08: ANALISIS Y GESTION DE LOS RIESGOS

Alexander, G. (2007) Diseño de un Sistemas de Gestión de Seguridad de la Información (Primera edición), Alfaomega, Colombia. Pag.8.

B. Evaluación, Certificación, Auditoria y Acreditación

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. En análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué

salvaguardas se ha dotado. Es pues el análisis de riesgos paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:

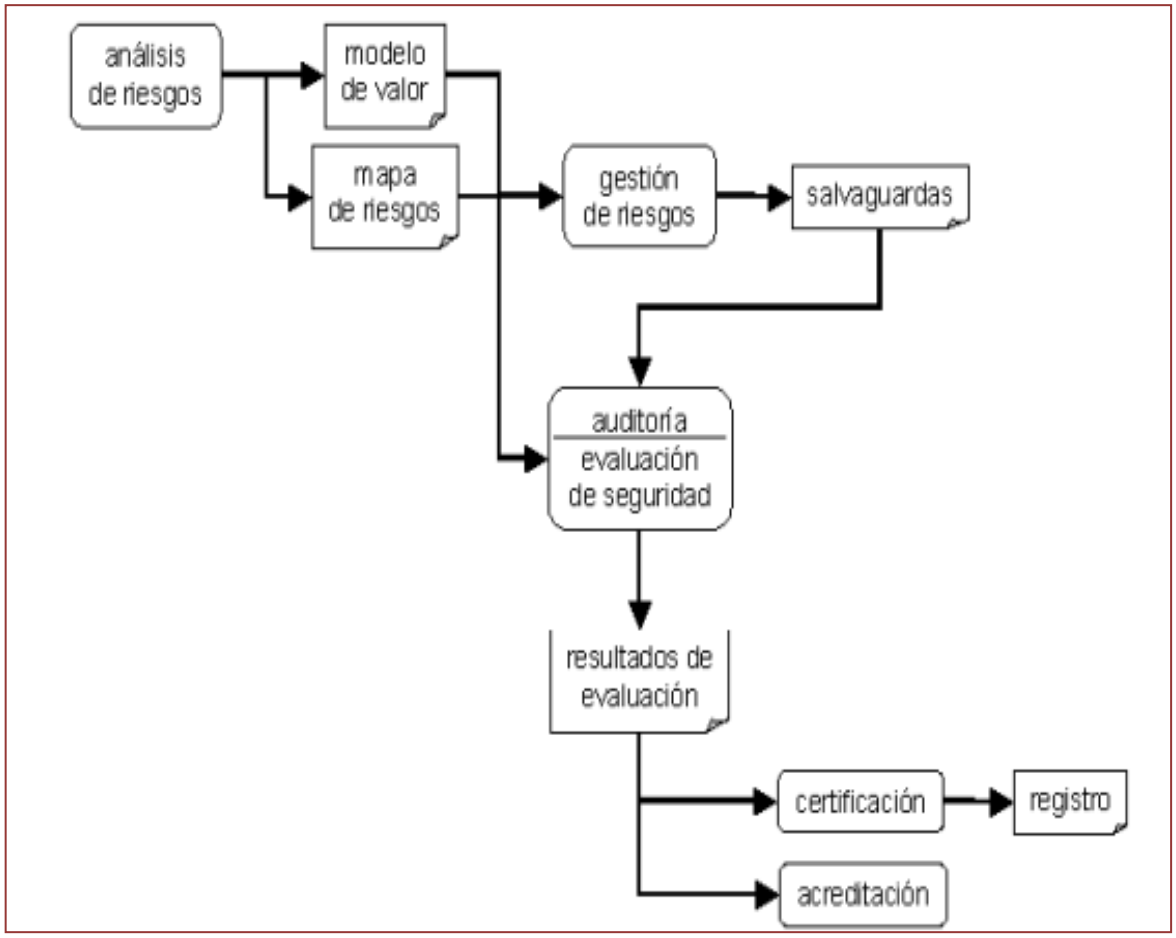


FIGURA 09: ANALISIS DE RIESGO

Alexander, G. (2007) Diseño de un Sistemas de Gestión de Seguridad de la Información (Primera edición), Alfaomega, Colombia. Pag.12.

C. Realización del Análisis de la Gestión

- ***Análisis de riesgos***, que permite determinar qué tiene la Organización y estimar lo que podría pasar.

  Elementos:

  - ✓ Activos, que no son sino los elementos del sistema de información (o estrechamente relacionados con este) que aportan valor a la Organización
  - ✓ Amenazas, que no son sino cosas que les pueden pasar a los activos causando un perjuicio a la Organización
  - ✓ Salvaguardas (o contra medidas), que no son sino elementos de defensa desplegados para que aquellas amenazas no causen [tanto] daño.

  Con estos elementos se puede estimar:

  - ✓ el impacto: lo que podría pasar
  - ✓ el riesgo: lo que probablemente pase

  El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento.

- ***Gestión de riesgos***, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando

en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume. Si el impacto y el riesgo residuales son despreciables, se ha terminado. Si no, hay que hacer algo.

D. Implementación de los Valores de Impacto y Riesgo Residual

Impacto y riesgo residual son una medida del estado presente, entre la inseguridad potencial (sin salvaguarda alguna) y las medidas adecuadas que reducen impacto y riesgo a valores despreciables. Son pues una métrica de carencias. Los párrafos siguientes se refieren conjuntamente a impacto y riesgo. Si el valor residual es igual al valor potencial, las salvaguardas existentes no valen para nada, típicamente no porque no haya nada hecho, sino porque hay elementos fundamentales sin hacer. Si el valor residual es despreciable, ya está. Esto no quiere decir descuidar la guardia; pero si afrontar el día con cierta confianza.

E. Selección de Salvaguarda

Las amenazas hay que conjurarlas, por principio y mientras no se justifique lo contrario. Hay que planificar el conjunto de salvaguardas pertinentes para atajar tanto el impacto como el riesgo, reduciendo bien la degradación del activo (minimizando

el daño), bien reduciendo la frecuencia de la amenaza (minimizando sus oportunidades).

F. Pérdidas y Ganancias

Es de sentido común que no se puede invertir en salvaguardas más allá del valor de los propios activos a proteger. Aparecen en la práctica gráficos como el siguiente que ponen uno frente al otro el coste de la inseguridad (lo que costaría no estar protegidos) y el coste de las salvaguardas.

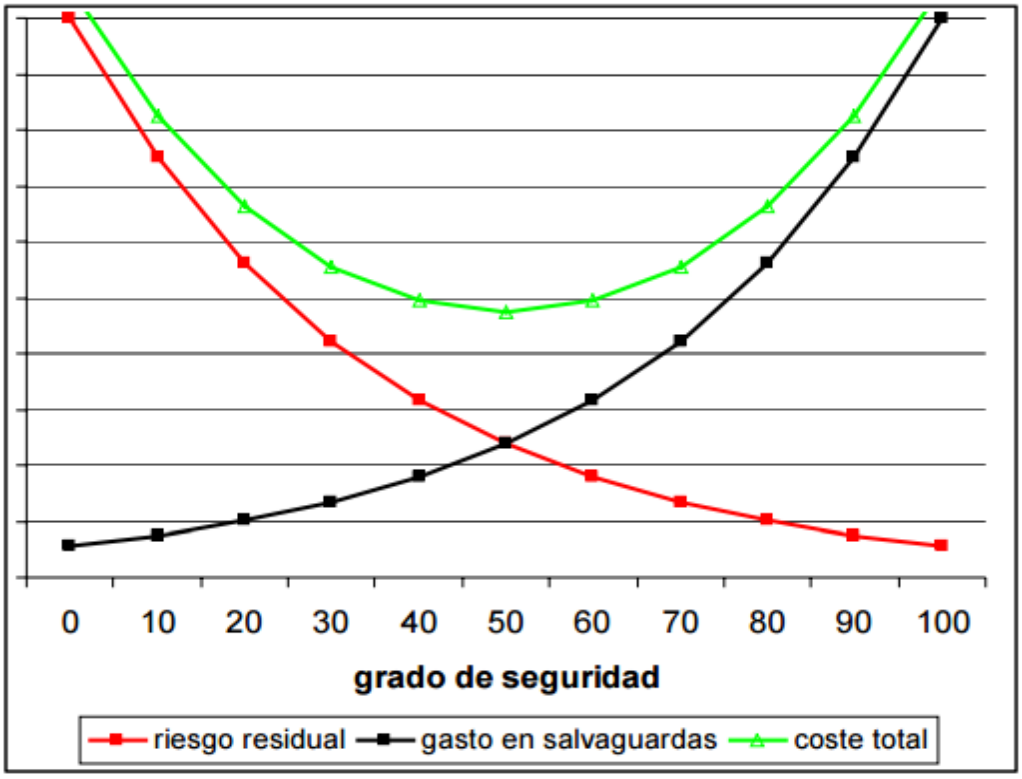


FIGURA 10: PERDIDAS Y GANANCIAS

Alexander, G. (2007) Diseño de un Sistemas de Gestión de Seguridad de la Información (Primera edición), Alfaomega, Colombia. Pag.28.

G. Cambio de Actitud en la Organización

La dirección de la Organización sometida al análisis de riesgos debe determinar el nivel de impacto y riesgo aceptable. Más propiamente dicho, debe aceptar la responsabilidad de las insuficiencias. Esta decisión no es técnica. Puede ser una decisión política o gerencial o puede venir determinada por ley o por compromisos contractuales con proveedores o usuarios. Estos niveles de aceptación se pueden establecer por activo o por agregación de activos (en un determinado departamento, en un determinado servicio, en una determinada dimensión, etc.)

H. Desarrollo del Proyecto MAGERIT

- ❖ PLANIFICACION
  - Se establecen las consideraciones necesarias para arrancar el proyecto AGR.
  - Se investiga la oportunidad de realizarlo.
  - Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará.
  - Se planifican los medios materiales y humanos para su realización.
  - Se procede al lanzamiento del proyecto.

❖ ANALISIS DE RIESGOS

- Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen.
- Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado.
- Se identifican las salvaguardas existentes y se valora la eficacia de su implantación.
- Se estima el impacto y el riesgo al que están expuestos los activos del sistema.
- Se interpreta el significado del impacto y el riesgo.

❖ GESTION DE RIESGOS

- Se elige una estrategia para mitigar impacto y riesgo.
- Se determinan las salvaguardas oportunas para el objetivo anterior.
- Se determina la calidad necesaria para dichas salvaguardas.
- Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Se lleva a cabo el plan de seguridad.

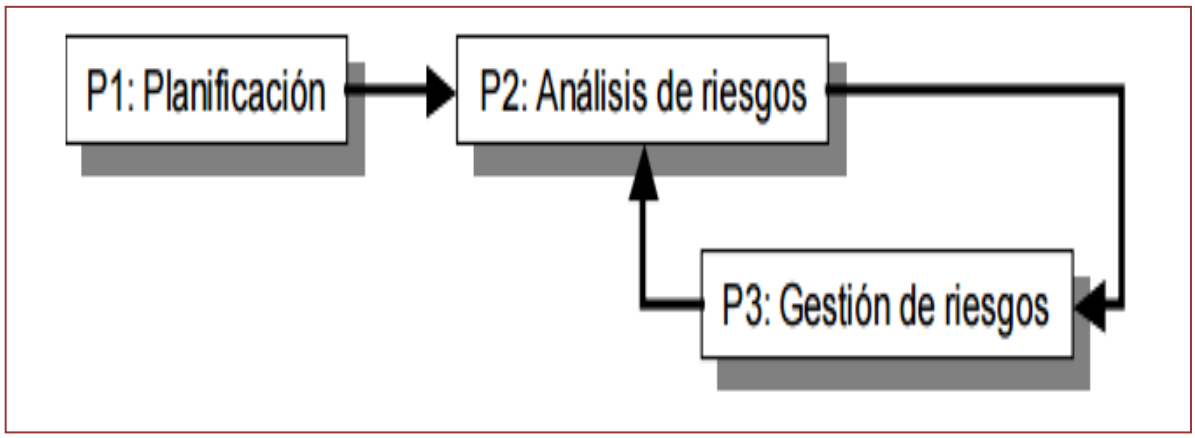


FIGURA 11: PLAN DE SEGURIDAD

Alexander, G. (2007) Diseño de un Sistemas de Gestión de Seguridad de la Información (Primera edición), Alfaomega, Colombia. Pag.36.

2.3 Marco Conceptual

- ✓ INFORMACION

La información es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Para sus actividades diarias, operaciones de su trabajo, para cumplir con sus funciones, el cual puede equivocarse o no, o hacer el bien o el mal. La información tiene estructuras que modificará las sucesivas interacciones del ente que posee dicha información con su entorno.

La información es uno de los principales activos de las organizaciones. La defensa de este activo es una tarea esencial para asegurar la continuidad y el desarrollo del negocio, así como también es una exigencia legal (protección de la propiedad intelectual,

protección de datos personales, servicios para la sociedad de la información), y además traslada confianza a los clientes y/o usuarios.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o malintencionada.

- ✓ SEGURIDAD DE LA INFORMACION

La información es un recurso que, como el resto de los activos, tiene valor para una organización y por consiguiente debe ser debidamente protegida. La seguridad de la información protege ésta de una amplia gama de amenazas, a fin de garantizar la continuidad del negocio, minimizar el daño al mismo y maximizar el retorno sobre las inversiones y las oportunidades.

La información puede existir en muchas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por un medio electrónico, presentada en imágenes, o expuesta en una conversación. Cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada.

- ✓ VULNERABILIDAD

Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Una amenaza a un sistema informático es una circunstancia que tiene el potencial de causar un daño o una pérdida. Es decir, las amenazas pueden materializarse dando lugar a un ataque en el equipo.

Como ejemplos de amenaza están los ataques por parte de personas, al igual que los desastres naturales que puedan afectar a su computadora. También se pueden considerar amenazas los fallos cometidos por los usuarios al utilizar el sistema, o los fallos internos tanto del hardware o cómo del software.

- ✓ RIESGOS

El riesgo es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

El riesgo se utiliza sobre todo el análisis de riesgos de un sistema informático. Esté riesgo permite tomar decisiones para proteger mejor al sistema. Se puede comparar con el riesgo límite que acepte para su equipo, de tal forma que si el riesgo calculado es inferior al de referencia, éste se convierte en un riesgo residual que podemos considerar cómo riesgo aceptable.

CAPÍTULO III

IMPLEMENTACION DE LA METODOLOGIA

3.1. Situación actual de la Seguridad de la Información

3.1.1. Definición de la Empresa Corporación la Sirena

Corporación La Sirena es una organización dedicada a brindar soluciones estratégicas de abastecimiento, suministrando las mejores marcas nacionales e importadas que conciernen a las líneas de: acabados de construcción, eléctricos, ferretería.

La Sirena ha experimentado una gran expansión en su gestión comercial logrando cobertura a nivel nacional y contando con una cartera de clientes de primer nivel. Brinda atención, garantía y servicio permanente y se posiciona como una empresa con amplio conocimiento y experiencia en el rubro ferretero, lo cual le permite competir con amplia solidez.

Esta organización está compuesta por un equipo de ejecutivos en el área de compras y ventas, especializados por líneas, manejando más de 20,000 artículos, garantizando en ellos, calidad, precios competitivos y puntualidad en la entrega del material. Está orientado hacia los clientes con una atención personalizada, por

ello, se cuanta con 4 canales de atención ubicado en Jr. Gonzales Prada 420, Surquillo – Lima, Perú.

Misión

Asegurar un servicio de asesoramiento y abastecimiento especializado en ferretería y afines a nuestros clientes, aprendiendo de ellos y adaptándonos a sus necesidades creando valor para sus proyectos.

Visión

Ser una empresa líder en el sector ferretero, reconocida por la creación de valor para sus clientes, colaboradores y accionistas.

3.1.2. Situación Actual de la Seguridad de la Información en el Área de Sistemas

El Área de sistemas de la empresa Corporación La Sirena es fundamental dentro de la organización, ya que de ella depende el funcionamiento correcto de varias de las tecnologías de la información y la información que manejan dentro de la organización, razón por la cual se requiere que la información y la seguridad de la misma sea tratada de forma organizada ya que actualmente no existe un plan que permita responder mitigando riesgos ante amenazas.

3.1.3. Estructura Organizacional de la empresa Corporación la Sirena

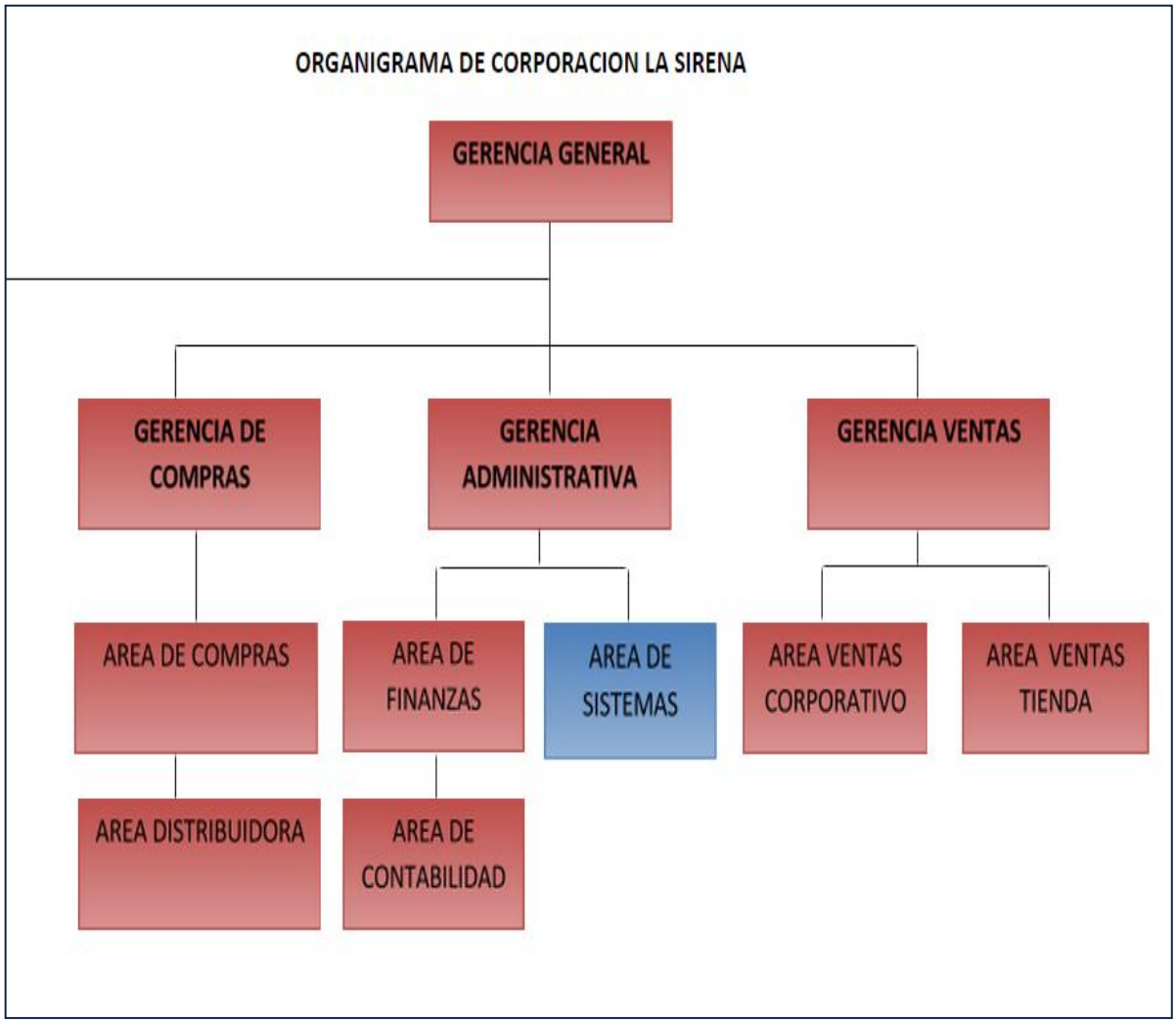


FIGURA 12: Organigrama Corporación la Sirena

(Fuente: Autor)

3.1.4. Mecanismos de Seguridad de la información actual

En La actualidad para la Administración de Servidores del Área de Sistemas se cuentan con ciertos mecanismos de protección para la seguridad de la información de forma independiente y no planificada en el mayor de sus casos, las cuales están a cargo de los siguientes responsables:

Procesos de seguridad:

- Copias de Seguridad de los procesos críticos en el servidor AS400 de forma manual en Cintas diarias.
- Restauración de Información de las cintas de respaldo Cintas del AS400.
- Solo se cuenta con proveedores principales de soporte para la infraestructura de Red y electricidad y los equipos informáticos.

  Estos son los siguientes proveedores:

  - TRAVI Soporte y revisión de la infraestructura cableado de Internet y electricidad.
  - IBM, Soporte y servicios para el servidor AS400.
  - PERU CONSULT SISTEM SAC, Proveedor de equipos informáticos de distintas marcas, brinda servicio de mantenimiento, soporte.
  - PRESICION SERVICE (Centro de servicios especializados), brinda servicios en mantenimientos, reparación de equipos informáticas.

- FUJITA COMUNICACIONES S.A. Reparación y mantenimiento de teléfonos y Central AVAYA.

- Políticas de uso del servicio de Conexión a Internet.
- Se cuenta con un proveedor de telecomunicaciones:
  - Internet que es Claro.
  - Telefonía siendo AVAYA.
- Solamente se cuenta con capacitación de Inserción laboral.
- Explicación y reconocimiento breve de las funciones de Administrador de Servidores.

Responsables:

- Jefe de Sistemas: Lojas Avila Wolfgang Zdenko
- Asistente de Sistemas: Laor Flores Nataly Susan
- Practicante de Sistemas: Álvarez Carguayo Jhulian

3.1.5. Procesos del área de sistemas

En la siguiente tabla se muestran cuatro procesos del área de sistemas de las cuales el resaltado con color es el proceso tomado para el estudio de este proyecto por ser crítico.

Ítem	AREA RESPONSABLE	PROCESOS
1	Área de sistemas	Administración de servidores.
2		Desarrollo de Sistemas.
3		Administración de Base de Datos.
4		Administración de la infraestructura.

TABLA 02: Procesos del área de sistemas

Fuente: Autor

3.2 Metodología

3.2.1 Metodología para el Plan de Seguridad de la Información

Para el plan de Seguridad de la Información, la siguiente metodología a implementar está basada en la Norma ISO 27002 DOM 17, tomando como referencias a la metodología de análisis y gestión de los riesgos de Sistemas de Información (MAGERIT) y la metodología de análisis gestión de los riesgos en el libro de Alexander, 2007.

Por tanto para la elaboración del plan de seguridad de la Información se determina siguiendo las buenas prácticas plasmadas en el dominio 17 de la ISO 27002 según gráfico:

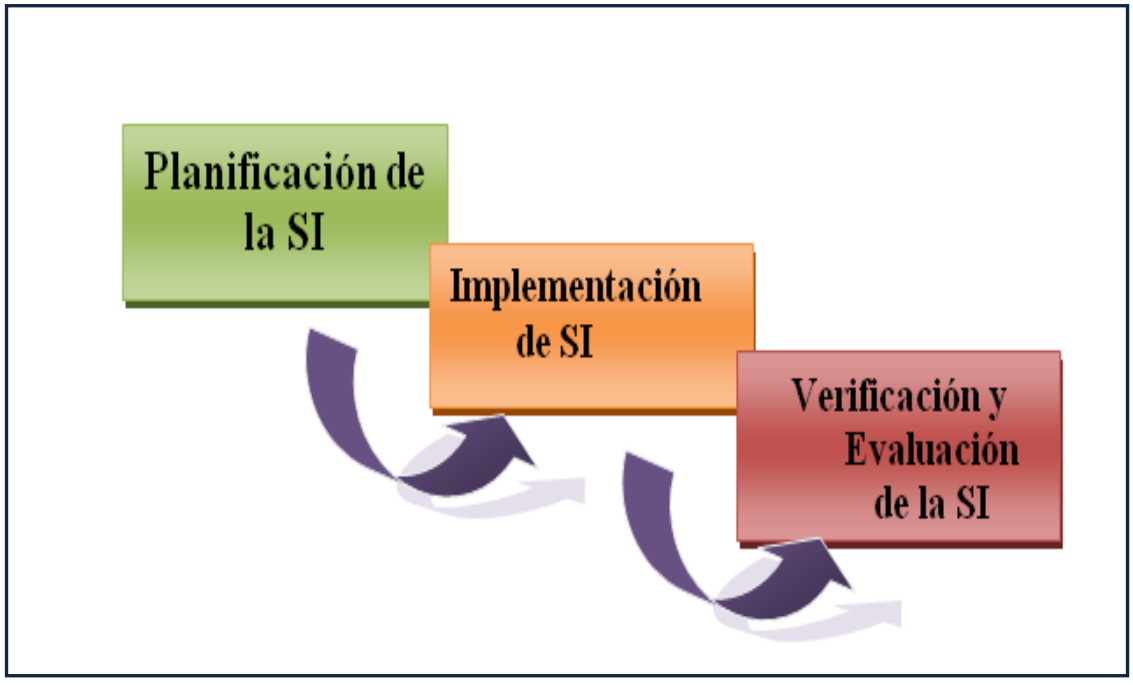


FIGURA 13: Actividades del Control del Riesgo; Proceso del Plan de Seguridad de la Información
Elaborado por el Autor

3.2.2 Plan de Seguridad de la Información

Para realizar la planificación se deberá determinar los requisitos para la seguridad de la información y para su gestión durante situaciones adversas se relazara un análisis y evaluación de los riesgos lo que implica los siguientes pasos:

- ✓ Análisis y Evaluación de Riesgos

El análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- Determinar los activos relevantes en el proceso crítico Administración de servidores en el área de sistemas de la empresa.
- Determinar a qué amenazas y vulnerabilidades están expuestos aquellos activos.
- Determinar que salvaguardas hay dispuestas y cuan eficaces son frente al riesgo.
- Estimar el impacto, definido como daño sobre el activo derivado de la materialización de la amenaza.
- Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (expectativa de materialización) de la amenaza.

Para alcanzar el objetivo de hacer un plan para la seguridad de la información y se asegure la continuidad del negocio de la empresa.

Según el grafico muestra los pasos de un impacto y riesgo.

FIGURA 14: Elementos del riesgo

Gobierno Informático. (2010). Administración de Riesgos. España, de Seguridad Informática Sitio web: http://cata-seguridaddelainformacion.blogspot.pe/2010/03/administracion-de-riesgos.html

A. Identificación del proceso critico

En el primer paso se identifica el proceso crítico a estudiar fijado dentro del alcance, mediante reuniones de 1 hora con los responsables estos son planificadas mediante fichas, se define el proceso crítico a estudiar.

B. Identificación de activos

Para determinar con precisión los activos de información del proceso crítico se utiliza el método de la Elipses.

El primer paso es determinar la elipse concéntrica, el proceso critico incluidos dentro del alcance.

En la elipse intermedia se identifican las distintas interacciones entre el proceso crítico con los otros procesos del área de sistemas. Seguidamente en la elipse externa, se identifican las demás áreas de la empresa que guardan interacción entre los procesos del área de sistemas incluyendo el proceso crítico definido.

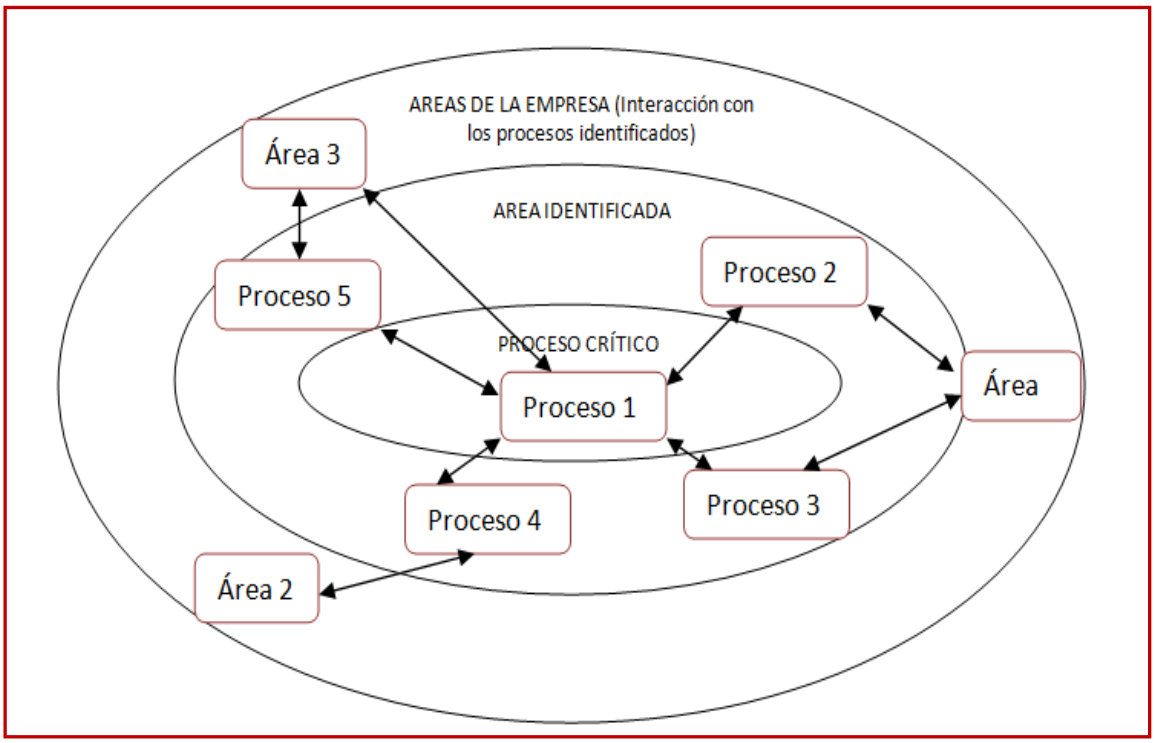


FIGURA 15: INTERACCIONES DE PROCESOSOS

Elaborada por el Autor

Este método le elipse será como punto de partida para los siguientes documentos de Análisis de identificación de los activos, y al analizar el proceso crítico y el flujo de información entre los demás procesos del Área de Sistemas y las demás áreas de la empresa, se procede a determinar los activos de información para realizar el análisis de los riesgos y su impacto por ende obtener el Plan de seguridad de Información para la continuidad del negocio de la empresa.

C. Inventario de los Activos

Para la elaboración del documento de activos de seguridad de la información, se debe tener en consideración lo siguiente, para la categorización de los activos.

TIPO	CODIGO	CATEGORIA	EJEMPLO
Activos de informacion	I1	Informacion electronica	Base de datos, documentos creados y conservados en medios electronicos(correo electronico, audio, video, Disco externo, etc.)
	I2	Informacion escrita	Documentos creados y o conservados en papel
	I3	Informacion hablada	Conversaciones precenciales, tecnicas, presentaciones orales o medios virtuales.
	I4	Otro tipo de informacion	-
Activos de software	S1	Software de sistemas operativos	Software de BD, windows 2007, windowws server, XP, server Linux, Unix, ETC.
	S2	Software comercial o heramientas, utilitarios	Office, Adobe; ect.
	S3	Software desarrollado por terceros	Sap, ORACLE, etc.
	S4	Software desarrollado internamente	Sistemas integrados, aplicativo, modulo de sistemas, etc.
	S5	Software de administracion de base de datos	SQL, Oracle, DB/2, etc.,
Activos de hardware	H1	Equipo de procesamiento	Servidores, computadoras, laptops, etc.
	H2	Equipo de comunicaciones	Routers, centrales digitales, Switch, etc.
	H3	Medio de almacenamiento	Discos, Cintas, CD, DVD, etc.
	H4	Mobiliario y equipamiento	Estantes, rack, archivadores, etc.
	H5	Otros equipos	-
Servicios (Terceros)	T1	Procesamiento y comunicaciones	Servicio de procesamiento de la informacion, de mensajeria, telefonia, etc.
	T2	Servicios generales	Energia electrica , aire acondicionado, etc.
	T3	Otros servicios	Servicio de intermediacion laboral, entre otros.

TABLA 03: Inventario de Activos

Elaborado por el autor

D. Análisis y Evaluación de riesgos

- Identificación de Amenazas

Partiendo de la definición la amenaza es un anuncio de un mal o peligro, algo que ocurre, interesa lo que pueda pasarle a nuestros activos de información y causar un daño. Una amenaza puede causar incidentes no deseados que pueden generar daño a una organización y sus activos.

Pueden ser de distintos tipos:

VALOR DEL ACTIVO	ALTO	Cuando la destrucción, modificación, revelamiento o interrupción de la información **afecta seriamente** la operación, competitividad, rentabilidad.
	MEDIO	Cuando la destrucción, modificación, revelamiento o interrupción de la información **afecta considerablemente** la operación, competitividad, rentabilidad.
	BAJO	Cuando la destrucción, modificación, revelamiento o interrupción de la información **no afecta considerablemente** la operación, competitividad, rentabilidad.

TABLA 04: VALORACION DEL ACTIVO

(Elaborado por el autor)

- Clasificación de Amenazas
    - Amenazas naturales (inundaciones, sismos, incendios, tormentas, etc.)
    - Amenazas a instalaciones (energía, explosión, fuego, fallas, etc.)

- Amenazas humanas (Transporte, renuncias, huelgas, accidentes, etc.)

  Acceso no autorizado
- Amenazas tecnológicas (virus, hacking, red, fallas de software, hardware)
- Amenazas operacionales (crisis, legal, fallas, equipos, proveedores)Identificación de amenazas y mecanismos de protección

- Identificación de amenazas y mecanismos de protección

  Determinando que una amenaza puede perjudicar a un activo, hay que estimar si afecta a la confidencialidad, Integridad y disponibilidad de acuerdo a las bases de la seguridad de la información.

  La organización mediante mecanismos de protección las cuales reducen la probabilidad de ocurrencia de dichas amenazas. Se deben identificar los mecanismos de protección clasificadas en:

  - Preventivos: Mecanismos de protección que previene a que la amenaza se materialice.
  - Detectivos: Mecanismo de protección que detecta cuando una amenaza se materializa.

- Correctivos: Mecanismo de protección que ejecutara después que la amenaza se haya materializado.

- Identificación de Vulnerabilidades

Par tiendo también de la definición de vulnerabilidad, es una condición o un “conjunto de condiciones que pueden permitir que una amenaza afecte a un activo” de una organización.

La mejor manera de definidillos es pensar en las debilidades de sistema de seguridad. Por ello es bueno entender que las vulnerabilidades y las amenazas deben presentarse juntas, para poder causar daño a los activos. Podríamos preguntarnos ¿Qué amenaza pudiese explotar cuál de las vulnerabilidades?

- Clasificación de vulnerabilidades
  - Seguridad lógica
  - Seguridad de recursos humanos
  - Seguridad física y ambiental
  - Seguridad de gestión de operaciones y comunicaciones
  - Mantenimiento, desarrollo y adquisición de sistemas de información.

- Determinación del Impacto y probabilidad

Impacto es la medida del daño sobre el activo derivado de la materialización de una amenaza. Identificando ya los activos del proceso crítico y sobre el las amenazas, se deriva el impacto que estas tendrían sobre el sistemas.

El impacto mide el daño causado por un incidente en el supuesto de que ocurriera.

Tomando en consideración las amenazas, mecanismos de protección actuales y vulnerabilidades del sistema para todos los activos de información del proceso crítico de debe definir:

- La ***Valoración*** de los activos, que es la sumatoria del impacto del activo en la Confidencialidad, Integridad y Disponibilidad de acuerdo a las bases de la seguridad de la información, en una escala de (1) Muy bajo, (5) Muy alto.
- La ***Probabilidad*** que las amenazas se materialicen, usando la siguiente clasificación:

5: MUY ALTO	**Ocurrencia diaria**
4: ALTO	**Ocurrencia Semanal**
3: MEDIO	**Ocurrencia Mensual**
2: BAJO	**Ocurrencia Anual**
1: MUY BAJO	**Ocurrencia en dos año a mas**

TABLA 05: Probabilidad de materialización de amenazas

Elaborada por el autor

- ***Impacto*** que ocasionaría el que las amenazas de materialicen, usando la siguiente clasificación:

5: MUY ALTO	**Afecta a más de un área**
4: ALTO	**Afecta a un área**
3: MEDIO	**Afecta a un usuario, no hay posibilidad de trabajo alterno**
2: BAJO	**Afecta a un usuario, hay posibilidad de trabajo alterno**
1: MUY BAJO	**No afecta a la productividad**

TABLA 06: Impacto que ocasiona una amenaza al materializarse

Elaborada por el autor

Determinación del Riesgo

El objetivo del análisis del riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y

disponibilidad y del cálculo de la probabilidad de que amenazas y vulnerabilidades relacionadas se junten y causen un incidente.

Teniendo ya el Impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la frecuencia de ocurrencia. El riesgo crece con el impacto y con la frecuencia.

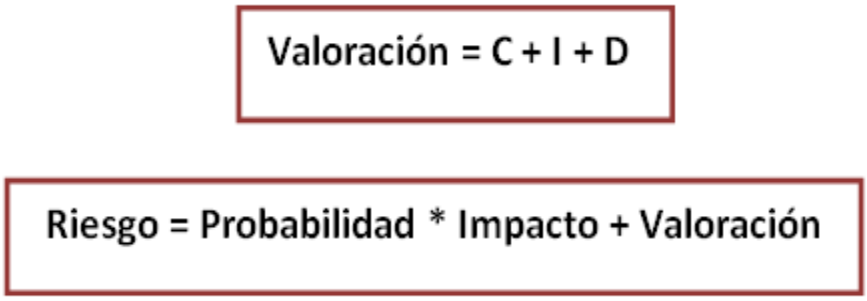


FIGURA 16: VALORACION Y RIESGO

Elaborado por el Autor

Los riesgos no se pueden eliminar, solo mitigar, de ahí que se establece un nivel de tolerancia de riesgos, expresados en:

Totalmente Tolerante: TT	**4-15**
Regularmente Tolerante: RT	**16-25**
No Tolerable: NT	**26-40**

TABLA 07: NIVEL DE TOLERANCIA

Elaborada por el Autor

Para activos que tienen mínimo un riesgo que resulte regularmente tolerable o no tolerable se debe redefinir salvaguardas.

Los riesgos que resulten Totalmente Tolerables, son opcionales para ser tratados.

- Definición de Salvaguardas

Se definen salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se evitan simplemente organizándose adecuadamente, otras requieren elementos técnicos, otra seguridad física o políticas al personal.

Las salvaguardas se caracterizan por su eficiencia frente al riesgo que pretenden mitigar. La salvaguarda ideal es 100% eficaz, lo que implica:

- Teóricamente idónea
- Esta perfectamente desplegada, configurada y mantenida
- Se emplea siempre
- Existen procedimientos claros de su uso normal y en caso de incidencias
- Existen controles que avisan de posibles fallos

Las estrategias para el tratamiento de las salvaguardas pueden ser:

- *Reducción del riesgo*(R): Para todos aquellos riesgos don de la opción de reducirlos se ha tomado, se deben implementar controles apropiados para poder reducirlos a un nivel aceptable.
- *Aceptar el riesgo (A):* Muchas veces se presentas situaciones en el cual la empresa no cuenta con controles para mitigar el riesgo, o en la cual la implantación de controles tiene un costo mayor que las consecuencias del riesgo. En estas circunstancias, la decisión de aceptar el riesgo y vivir con las consecuencias es la más adecuada.
- *Transferencia del riesgo* (T): La transferencia del riesgo es una opción cuando para la empresa es difícil reducir o controlar el riesgo a nivel aceptable. Esta alternativa de tercerizar es muchas veces más económica ante estas circunstancias.
- *Evitar el riesgo* (E): Es cualquier acción orientada a cambiar las actividades, o la manera de desempeñar una actividad en particular, para así evitar la presencia del riesgo.

- Por cualquiera de las estrategias que se opte, todas las salvaguardas incurren en un costo y tiempo que estarán gestionados por los responsables de implementación.
- Para dimensionar el Costo aproximado de la implementación de la salvaguarda elegida, se considera:

3	Alto Costo
2	Medio Costo
1	Bajo Costo
D	Desconocido

TABLA 08: DIMENSIONAR COSTOS

Elaborado por el Autor

- Para dimensionar *el tiempo aproximado* de la implementación de la salvaguarda elegida, se considera:

C	Corto Plazo (Menos de 1 mes)
M	Mediano Plazo (Menos de 1 a 2 mes)
L	Largo Plazo (Mas de 3 meses)
D	Desconicido

TABLA 09: DIMENSIONAR TIEMPO

Elaborado por el Autor

- Determinación del Riesgo Residual

Hechos todos los deberes a la perfección, el riesgo residual debe ser despreciable.

Si son hechos a medias hacer (normas imprecisas, procedimientos incompletos, salvaguardas inadecuadas o insuficientes o controles que no controlan) entonces se dice que el sistemas permanece sometido a un riesgo residual.

Como no han cambiado los activos, ni sus dependencias, se repiten los cálculos de riesgos usando el impacto residual y la nueva tasa de ocurrencia.

Riesgo Residual = Probabilidad R * Impacto R + Valoración

Totalmente Tolerante: TT	**4-15**
Regularmente Tolerante: RT	**16-25**
No Tolerable: NT	**26-40**

TABLA 10: Medición del Impacto y probabilidad del Riesgo

Elaborada por el Autor

Para los riesgos que resulten nuevamente “regularmente tolerables” o “no tolerables” se debe definir nuevamente salvaguardas.

Los riesgos que resulten “totalmente tolerables**”**, son considerados “despreciables**”,** y no requieren más condiciones, que el monitoreo periódico.

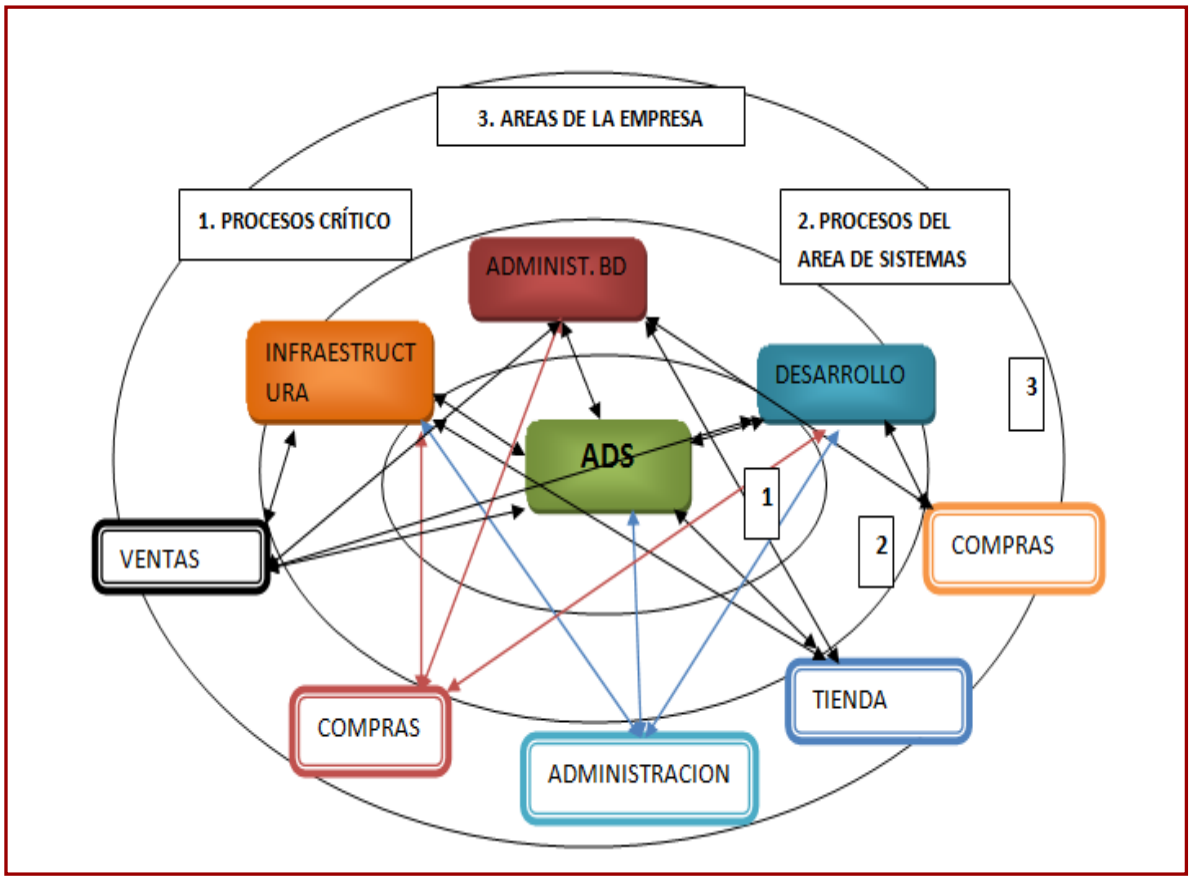
E. Plan Estratégico de Riesgos

El área realizara lo siguiente:

- Formular el plan de tratamiento de riesgo que identifique las acciones, los recursos, las responsabilidades y prioridades para manejar los riesgos de la seguridad de información.
- Implementar el plan de tratamiento de riesgos para lograr los objetivos, los cuales incluyen tener en consideración el financiamiento y asignación de roles y responsabilidades.

3.3. Aplicación de la Metodología

3.3.1. Identificación de los Activos del proceso Administración de Servidores



FIGUA 17: INTERACCION ENTRE EL PROCESO ADMINISTRACION DE SERVIDORES Y LOS DEMAS PROCESOSO, AREAS DE LA EMPRESA

Elaborado por el autor

3.3.2. Inventario de Activos Administración de Servidores

ACTIVO DE INFORMACION			
ITEM	NOMBRE DEL ACTIVO	CATEGO	UBICACIÓN
1	Manuales de instalación 2010	I1	servidor de archivo
2	Lista de usuarios y contraseñas 2010	I1	servidor de archivo
3	Archivadores de facturas	I2	Encargado. Infraestructura
4	tos de tecnologías archivados den folders	I2	Encargado. Infraestructura
5	Inventarios HW y SW 2014	I1	servidor de archivo
6	Licencias de tecnología	I1	Encargado. Infraestructura
ACTIVOS DE SOFTWARE			
7	DB/2	S1	Servidor AS/400
8	MS office	s2	Computador
9	Antivirus Karpesky	s2	Computador
10	Windows server 2003	S1	Servidores
11	server Ubuntu	S1	Servidores Linux
12	Servidor Proxy	S1	Servidores Linux
13	server Centos	S1	Servidores Linux
14	SQL 0.6	S1	Servidores
15	SPEED Advance	S1	Servidores
16	SIDIGE	S1	Servidores
17	SERVER WAP	s2	Servidores
	ACTIVOS DE HARDWARE		
17	Servidor AS/400	H1	Servidores
18	servidor AVAYA	H1	Servidores
19	SERVIDOR SIDIGE	H1	Servidores
20	SERVER WAP	H1	Servidores
21	SERVIDOR SAMBA	H1	Servidores
22	Teléfonos	H1	INFRAESTRUCTURA
23	Computadoras	H1	INFRAESTRUCTURA
24	Laptop	H1	INFRAESTRUCTURA
25	Route	H2	INFRAESTRUCTURA
26	Switch	H2	INFRAESTRUCTURA
27	Central telefónica AVAYA	H1	Servidores
28	Servidor de cámara de vigilancia	H1	Servidores
29	Unidad de Cintas diarias	H3	INFRAESTRUCTURA
30	UPS de duración 1 hora	H5	INFRAESTRUCTURA
31	Disco duro externo	H3	INFRAESTRUCTURA
SERVICIO (TERCEROS)			
32	Internet Claro	T1	INFRAESTRUCTURA

33	Correo Corporativo Google	T1	INFRAESTRUCTURA
34	Cableado estructurado TRAVI	T2	TRAVI Terceros
35	Cableado eléctrico TRAVI	T2	TRAVI Terceros
36	Mantenimiento a equipos de información	T2	PRESICION SERVERVICE
COLABORADORES			
37	Usuarios	C1	Toda la empresa colaboradora
38	Gerente de Administración	C1	Área de administración
39	Encargado de Infraestructura	C1	Área de infraestructura
40	Jefe de Sistemas	C1	Área de sistemas
41	Administrador de BD	C1	Área de sistemas
42	Desarrollo de sistemas	C1	Área de sistemas

TABLA 11: INVENTARIO DE ACTIVOS EN ADMINISTRACION DE SERVIDORE

Elaborado por el autor

Análisis y evaluación del riesgo

Área de sistemas – Administración de Servidores

RIESGO DEL PROCESO								CONTROLES EFECTIVOS	RIESGO EFECTIVO			
ID	ACTIVOS DE INFORMACION	AMENAZAS	C	I	D	VAL.	VULNERAVILIDAD	MECANISMOS DR PROTECCION EXISTENTES	PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA
R1	Daños en el centro de cómputo (destrucción y/o deterioro de los equipos como, ambiente de monitoreo y alojamiento de los equipos informáticos como servidores)	Desastres(fuego, inundación, sismo, explosión, disturbios, y otras formas de desastre natural y hechas por el hombre)	1	4	4	9	No se cuenta con Normas y planes que permitan dar continuidad al negocio. No existe un área alterna con equipos para la generación de backup de los procesos críticos del área de sistemas. No se cuenta con proveedores de servicio de Infraestructura de Red y Electricidad de emergencia para casos de interrupciones o falta de disponibilidad de proveedores principales. No existe un Soporte y mantenimiento periódico planificado en prevención de fallas de hardware. No cuenta con adecuado y exclusivo UPS. No cuenta con equipos de información de respaldo.	Copias de Seguridad de los procesos críticos en el servidor AS400 de forma manual.	2	5	19	RT
		Fallas en Hardware (equipos de procesamiento de datos y telecomunicación).						Solo se cuenta con proveedores principales de soporte para la infraestructura de Red y electricidad.	3	4	21	RT
		Daños en la infraestructura de red y electricidad del área de Sistemas.						Llamadas a proveedores de soporte técnico cuando ocurren las fallas de Hardware.	2	5	19	RT
	Perdida de registros vitales, Información (software y hardware, base de datos, manuales informes, etc.)	Desastres naturales	1	3	3	7	No cuenta con un control de accesos adecuado sobre la documentación, archivos informáticos, código fuente, etc. No existen normas, documentación que evidencie confidencialidad de Información(a excepción de políticas de Conexión a internet). No se cuenta con procedimiento	Políticas de uso del servicio de Conexión a Internet.	2	5	17	RT
		Fuga/divulgación de información por parte del personal interno						Copias de Seguridad de los procesos críticos en el servidor AS400 de forma manual.	3	5	22	RT
		Acceso no autorizado personal interno y externo. Ruptura de claves de acceso(tanto a los servidores AS/400, Nextel,						Restauración de Información de las cintas de respaldo OLT del AS400.	4	5	27	NT

R 2		SIDIGE, AVAYA, servidores administradores de Red datos, correo electrónico). Intromisión por curiosidad					de actualización de la información de manuales de seguridad. Los documentos físicos e informáticos son fácilmente extraíbles. Falta de compromiso de los usuarios en cumplimiento de la política existente (Políticas de Conexión a Internet). No existe seguridad perimetral como un Firewall/Proxy para que le brinde protección a la Red. No existen normas y planes de continuidad para los procesos que le permitan salvaguardar su información. No existe un área alterna con equipos para la generación de backup de los procesos críticos del área de sistemas.					
		Ataques informáticos, Infección por código malicioso, virus, troyanos, gusanos y personas externas con USB, CD/DVD infectados.						Solo se cuenta con proveedores principales de soporte para la infraestructura de Red y electricidad.	3	5	22	RT
		Modificación de información accidental/intencional.						Llamadas a proveedores de soporte técnico cuando ocurren las fallas de Hardware.	5	5	32	NT
	Daño en la infraestructura de Red(Conexión de red Internet, telefonía o cualquier problema físico que detenga las operaciones de los equipos de Red de internet y telefonía)	Desastres (fuego, inundación, sismo, explosión, disturbios, y otras formas de desastre natural y hechas por el hombre).	2	3	3	8	No se cuenta con proveedores de servicios de Infraestructura de Red de Internet, telefonía y equipos de emergencia para casos de interrupciones o falta de disponibilidad de proveedores principales. Falta de Revisión, Soporte y mantenimiento (HW y SW) por parte de terceros para la conexión de red de internet, Telefonía y sus equipos de forma periódica. No existe un respaldo de otro operador de internet y telefonía en caso de incidencia.	Solo se cuenta con proveedores principales de soporte para la infraestructura de Red de Internet, Telefonía y sus equipos. Se cuenta con un proveedor de Internet que es Claro y telefonía siendo AVAYA.	5	5	33	NT
		Fallas en Hardware (equipos Accespoint, Switch, Route de Red de Internet y telefonía como Servidor Avaya).							3	4	20	RT

							No se cuenta con Normas y planes que permitan dar continuidad al negocio.					
R 3	Falta de prestación de servicios tercer izados (central de comunicaciones, redes de Internet y Los Sistemas para procesos de negocio)	No se cuenta con proveedores de emergencia para casos de interrupciones o falta de disponibilidad de proveedores principales.	3	3	3	9	Falta de registros de emergencia para el servicio de soporte y mantenimiento.	Solo se cuenta con proveedores principales de soporte para la infraestructura de Red de Internet, Telefonía y demás sistemas de procesos. Solo se cuenta con proveedores principales de soporte para la infraestructura de Red de Internet, Telefonía y demás sistemas de procesos.	3	5	24	RT
R 4	Daños en los activos de software (Herramientas y entornos de implementación como Server Centos, Server Ubuntu, Server R2, etc.)	Mala instalación, configuración, actualización de software. Cambio de versión de las herramientas y entornos(versión obsoleta) Falta de licencias y renovación para software.	4	3	3	10	Falta de Revisión, Soporte y mantenimiento (HW) por parte de terceros para los servidores donde se aloja la información de forma periódica.	Revisión, Soporte y mantenimiento (HW) por parte de terceros para los servidores donde se aloja la información.	3	5	25	RT
R 5	Personal Inadecuado	Personal con poca experiencia y conocimientos en tema de administración de servidores y lo que implica.	1	2	2	5	Desconocimiento de las funciones y responsabilidades inherentes al cargo. Falta de experiencia en funciones vitales como administrador de servidores. Nivel de compromiso del colaborador con la empresa. Falta de capacitación periódica.	Únicamente se cuenta con capacitación de Inserción laboral.	5	4	25	RT
		Personal indispuesto.						Explicación y reconocimiento breve de las funciones de Administrador de Servidores	4	2	13	TT
		No definir personal alternativo en caso de no encontrar con el directo.							5	4	25	RT
		Personal alternativo no capacitado							5	5	30	NT

		para restauración de operaciones.										

TABLA 11: ANALISIS Y GESTION DE LOS RIESGOS

Elaborado por el Autor

Gestión del riesgo

Área de sistemas – Administración de Servidores

			RIESGO EFECTIVO									RIESGO RESIDUAL				
ID	AMENAZAS		VALORACION	PROB.	IMPAC	RIESGO	TOLERANCIA	MECANISMOS DE PROTECCION PROPUESTOS	TIPO DE CONTROL	COSTO APROX.	TIEMPO APROX.	PROBABILIDAD	IMPACTO	RIESGO	TOLERANCIA	RESPONSABLE
R1	Daños en el centro de cómputo(destrucción y/o deterioro de los equipos como, ambiente de monitoreo y alojamiento de los equipos informáticos como servidores)	Desastres(fuego, inundación, sismo, explosión, disturbios, y otras formas de desastre natural y hechas por el hombre)	9	2	5	19	RT	Implementación extintores apropiados para equipos informáticos.	Reducir	**1**	**C**	2	1	11	TT	SUM ASIS
								Capacitación en uso de seguridad física.	Reducir	**1**	**C**					
								Implementar detectores de aniego y fuego.	Reducir	**1**	**C**					
								Reubicar el Data center.	Reducir	**2**	**L**					
		Fallas en Hardware (equipos de procesamiento de datos y telecomunicación).		3	4	21	RT	Contar con stock mínimo de repuestos, PC, laptop y otros equipos.	Reducir	**2**	**C**	3	1	12	TT	INF ASIS PSIS
								Implementar programa de mantenimiento preventivo.	Reducir	**2**	**M**					
								Capacitación de uso, cuidado y seguridad de equipos de información.	Reducir	**1**	**C**					
								Corregir las instalaciones eléctricas.	Reducir	**1**	**C**					
								Seguimiento a las garantías.	Reducir	**1**	**C**					
								Mantener relaciones comerciales con proveedores principales y mantener lista de proveedores secundarios.	Reducir	**1**	**C**					

								Establecer inventario de los equipos de información y una actualización periódica.	Reducir	**2**	**M**					
		Daños en la infraestructura de red y electricidad del área de Sistemas.		2	5	19	RT	Adquirir e Independizar UPS para los equipos de información. Mantenimiento preventivo de la infraestructura de Red de internet, telefonía y electricidad.	Reducir Transfe rencia	**1** **1**	**C** **C**	1	5	14	RT	INF ASIS PSIS
R 2	Perdida de registros vitales, Información (software y hardware, base de datos, manuales informes, etc.)	Desastres naturales	7	2	5	17	RT	Respaldos periódicos de información como archivos físicos e informáticos. Definir tiempos de backup.	Reducir Reducir	**1** **1**	**M** **C**	3	1	10	RT	INF ASIS
		Fuga/divulgación de información por parte del personal interno		3	5	22	RT	Implementación de Capacitación para los usuarios en seguridad en información. Restablecer información de respaldo.	Reducir Reducir	**1** **2**	**C** **M**	3	2	13	TT	INF ASIS JSIS
		Acceso no autorizado personal interno y externo. Ruptura de claves de acceso (tanto a los servidores AS/400, Nextel, SIDIGE, AVAYA, servidores administradores de Red datos, correo electrónico). Intromisión por curiosidad		4	5	27	NT	Elaboración de procedimientos de acceso a los equipos de información y programas, aplicaciones y correos corporativos. Configurar usuarios y claves a los equipos de información, programas,	Reducir Reducir	**1** **1**	**M** **M**	5	1	12	TT	INF ASIS PSIS

								aplicaciones y correos corporativos. Implementar y actualizar periódicamente manuales y listas de claves y usuarios de acceso. Mejorar la seguridad del data center.	Reducir Reducir	**1** **2**	**M** **M**					
		Ataques informáticos, Infección por código malicioso, virus, troyanos, gusanos y personas externas con USB, CD/DVD infectados.		3	5	22	RT	Seguimiento sobre el estado del antivirus. Administración y mantenimiento adecuada de los servidores Proxy/firewall.	Reducir Reducir Transferir	**1** **2**	**M** **M**	5	1	12	TT	INF ASIS
		Modificación de información accidental/intencional.		4	5	27	NT	Elaboración de procedimientos en caso de pérdida de la información original. Respaldo periódico de archivos físicos y informáticos.	Reducir Reducir	**2** **1**	**M** **C**	1	3	10	NT	INF ASIS
R 3	Daño en la infraestructura de Red(Conexión de red Internet, telefonía o cualquier problema físico que detenga las operaciones de los equipos de Red de internet y telefonía)	Desastres (fuego, inundación, sismo, explosión, disturbios, y otras formas de desastre natural y hechas por el hombre).	8	5	5	33	NT	Equipos de información situados en otro lugar. Implementar contingencia de red Internet.	Reducir Transferir	**3** **3**	**L** **L**	3	1	11	TT	
		Fallas en Hardware (equipos Accespoint, Switch, Routers de Red de Internet y telefonía como Servidor Avaya).		3	4	20	RT	Contar con stock mínimo de repuestos para equipos de internet y telefonía. Mantener relaciones comerciales con	Reducir Reducir	**2** **1**	**M** **C**	3	1	11	TT	INF ASIS JSIS

								proveedores principales y mantener lista de proveedores secundarios.									
R 4	Falta de prestación de servicios tercer izados (central de comunicaciones, redes de Internet y Los Sistemas para procesos de negocio)	No se cuenta con proveedores de emergencia para casos de interrupciones o falta de disponibilidad de proveedores principales.	9	3	5	24	RT	Mantener relaciones comerciales con proveedores principales. Elaborar y actualizar de forma constante una lista con proveedores principales y secundarios en caso no estar disponible los principales.	Reducir Reducir	**1** **1**	**C** **M**	3	1	12	TT	ASIS PSIS
R 5	Daños en los activos de software (Herramientas y entornos de implementación como Server Centos, Server Ubuntu, Server R2, etc.)	Mala instalación, configuración, actualización de software. Cambio de versión de las herramientas y entornos(versión obsoleta) Falta de licencias y renovación para software.	10	3	5	25	RT	Revisiones periódicas de nuevas actualizaciones. Implementar revisiones y controles mensuales para la renovación de licencias.	Reducir Reducir	**1** **2**	**C** **M**	2	1	12	TT	INF ASIS PSIS
	Personal Inadecuado	Personal con poca experiencia y conocimientos en tema de administración de servidores y lo que implica.	5	5	4	25	RT	Elaborar un plan de inducción por el área personal nuevo). Entrenamiento del personal. Evaluar y capacitar al personal responsable. Programar capacitación de actualización contaste.	Reducir Reducir Reducir Transfe rir	**1** **1** **1** **1**	**C** **C** **C** **C**	2	1	7	TT	INF ASIS JSIS

R 6								Asignar personal adecuado.	Reducir	**1**	**C**							
		Personal indispuesto.		4	2	13	TT	Programar capacitación y motivación de concientización en seguridad de la información.	Reducir	**1**	**C**	2	1	7	TT	ASIS PSIS
		No definir personal alternativo en caso de no encontrar con el directo.		5	4	25	RT	Planificar lista de personal alternativo en caso no encontrar al directo.	Reducir	**1**	**C**	2	1	7	TT	ASIS PSIS
		Personal directo y alternativo no capacitado para restauración y administración de operaciones.		4	5	25	NT	Capacitación periódicas externas respecto a las funciones implicadas en el proceso.	Reducir	**1**	**C**	2	1	7	TT	ASIS PSIS

TABLA 12: GESTION DE LOS RIESGOS

Elaborada por el Autor

Plan de Tratamiento del Riesgo

PLAN DE TRABAJO PARA EL TRATAMIENTO DE RIESGOS-ADMINISTRACION DE SERVIDORES						
			Plazo			
Nro.	Mecanismos de protección	Actividades	Inicio	Fin	Avance %	Responsable
1.	Implementar programa de capacitación y sensibilización al personal en seguridad de Información	1.1 Elaborar capacitación en seguridad de información.	06/05/15	16/05/15	100%	ASIS
		1.2 Elaborar boletines de seguridad de información	12/05/15	17/05/15	100%	PSIS
		1.3 Ejecutar capacitación en seguridad de información.	18/05/15	28/05/15	100%	ASIS
2.	Implementar lista de personal alternativo asignado en caso no encontrar el directo. Elaborar un plan de capacitación anual (nuevas tecnologías)	2.1 Evaluar personal para administración de servidores.	01/05/15	15/05/15	100%	JFSIS
		2.2 Asignar personal adecuado para la restauración administración del data center.	15/05/15	29/05/15	100%	JFSIS
		Programación anual de capacitación	01/06/15	04/06/15	100%	JFSIS GADM
3.	Implementar capacitación de personal directo y alternativo en administración y restauración del data center.	3.1 Elaborar un plan de capacitación en administración y restauración del data center.	15/05/15	20/05/15	100%	JFSIS Y GADM
		3.1 Capacitación por instituciones externas en administración y restauración del data center (As400, Linux, otros).	15/05/15	20/05/15	100%	JFSIS Y GADM

4.	Implementar pruebas periódicas de restauración	4.1 Programación de pruebas	20/05/15	26/05/15	100%	JFSIS
		4.2 Elaborar instructivos técnicos	26/05/15	02/06/15	100%	JFSIS
		4.3 Aperturar archivos físico de cronograma de programación	02/06/15	09/06/15	100%	JFSIS
5.	Corrección de instalación y actualización de software Versiones	5.1 Elaborar inventario de software.	01/06/15	30/06/15	100%	ASIS
		5.2 Programar reunión de coordinación para actualización de versiones de SW.	01/07/15	12/07/15	100%	ASIS Y JFSIS
		5.3 Definición de un Plan de actualización de versión ANUAL 2015-2016	12/07/15	27/07/15	100%	ASIS Y JFSIS
6.	Corrección de instalación y actualización de software Licencias	6.1 Elaborar inventario de software.	01/06/15	15/06/16	100%	ASIS Y JFSIS
		6.2 Definición de un Plan de actualización de Licencias ANUAL 2015-2016	15/06/15	30/06/15	100%	ASIS Y JFSIS
7.	Mantener relaciones comerciales con proveedores estratégicos	7.1 Elaborar lista de proveedores diferenciando los principales como los secundarios (en caso de ausencia de los principales)	08/06/15	12/06/15	100%	PSIS
8.	Planificar los trabajos de mantenimiento de terceros	8.1 Elaborar inventario de contratos	03/08/15	14/08/15	100%	Coordinación con INF
		8.2 Programación de fechas de mantenimiento de equipos de	17/08/15	29/08/15	100%	Coordinación con INF

		información por terceros.				
9. Daño en la infraestructura (fallas en hardware)	Implementar mecanismos de control a los contratos de mantenimiento con terceros	9.1 Elaborar lineamiento para el mantenimiento de cableado y equipos de red internet(Red Claro)	15/06/15	19/06/15	100%	JFSIS
10. Daño en la infraestructura (fallas en hardware)	Contar con un stock mínimo de repuestos y equipos de Red (switch, route, accespoint, otros)	10.1 Evaluar stock mínimo de repuestos y equipos de red.	01/06/15	03/06/15	100%	PSIS
		10.2 Adquisición de stock de repuestos y equipos de Red.	04/06/15	9/06/15	100%	PSIS
		10.3 Inventariar repuestos y equipos.	12/06/15	14/06/15	100%	PSIS
11. Daño en la infraestructura (fallas en hardware)	Contar con un stock mínimo de repuestos y equipos de Red (switch, route, accespoint, otros)	11.1 Evaluar stock mínimo Teléfonos.	01/06/15	03/06/15	100%	PSIS
		11.2 Adquisición de stock de Teléfonos.	04/06/15	7/06/15	100%	PSIS
		11.3 Inventariar repuestos y equipos.	8/06/15	13/06/15	100%	PSIS
12. Daño en la infraestructura (desastres)	Implementar contingencia de internet	12.1 Cotizar servicio de internet con contingencia	15/06/15	26/06/15	100%	JFSIS
		12.2 Análisis comparativo	29/06/15	03/07/15	100%	JFSIS
		12.3 Elaboración de propuesta	6/07/15	7/07/15	100%	JFSIS
		12.4 Presentación de propuesta	07/07/15	070/07/15	100%	JFSIS
		12.5 Aprobación de propuesta	08/07/15	08/07/15	100%	JFSIS
		12.6 Envío de orden de compra	08/07/15	09/07/15	100%	JFSIS
		12.7 Planificación e implementación	10/07/15	16/07/15	100%	JFSIS

		del servicio de internet de contingencia				
13. Perdida de registros vitales, Información (software y hardware, base de datos, manuales informes, etc.)	Elaborar procedimiento ante la pérdida de Información	13.1Elaborar procedimiento ante la pérdida o robo de Información.	01/07/15	01/07/15	100%	ASIS
		13.2 Revisión y aprobación de procedimiento.	10/07/15	20/07/15	100%	ASIS
14. Perdida de registros vitales, Información (software y hardware, base de datos, manuales informes, etc.)	Implementar informes mensuales sobre el estado del Antivirus	14.1 Coordinar con Infraestructura	01/07/15	15/05/15	100%	Coordinación INF
		14.2 definir procedimientos de trabajo	15/07/15	21/07/15	100%	Coordinación INF
		14.3 elaborar procedimientos de antivirus	21/07/15	28/07/15	100%	Coordinación INF
15.	Implementar controles para visitas externas	15.1 Elaborar un cheklist de controles para visitas externas	15/07/15	22/07/15	100%	Coordinación INF
		15.2 Implementar controles para visitas externas	22/07/15	22/07/15	100%	Coordinación INF
		15.3 Elaborar procedimiento para la recepción de proveedores.	22/07/15	26/07/15	100%	Coordinación INF
16.	Implementar controles para prevenir el acceso físico del personal o lugares restringidos	16.1 prevenir acceso físico de personal a lugares restringidos.	01/06/15	07/06/15	100%	Coordinación INF
		16.2 Implementar controles para prevenir acceso físico de personal a lugares restringidos.	07/06/15	07/06/15	100%	Coordinación INF
		16.3 Elaborar lineamientos par ingreso a lugares	7/06/15	13/06/15	100%	Coordinación INF

		restringidos.				
17.	Implementar controles/mecanismos de encriptación	17.1 Evaluar mecanismos de encriptación de datos para los equipos	20/06/15	30/06/15	100%	ASIS
		17.2 Implementar mecanismo de encriptación para laptop, Pc, Servidores, otros.	30/06/15	30/06/15	100%	ASIS
18.	Implementar control de claves a los servidores	18.1 Elaborar inventario de usuarios y claves	08/06/15	12/06/15	100%	ASIS
		18.2 Asegurar ubicación de inventario	12/06/15	12/06/15	100%	ASIS
19.	Implementar herramientas de monitoreo	19.1 Adquirir herramientas de monitoreo de trafico de red.	22/06/15	27/06/15	100%	ASIS
		19.2 Implementar herramientas de monitoreo de trafico de red	27/06/15	05/07/15	100%	ASIS
20.	Renovación tecnológica	20.1 Programación anual de renovación tecnológica	15/06/15	19/06/15	100%	Coordinación INF
21.	Digitalizar contratos físicos	21.1 Inventario de contratos	22/06/15	27/06/15	100%	PSIS
		21.2Digitalización de contratos	27/06/15	02/07/15	100%	PSIS
22.	Implementar mecanismos de control para renovación de contratos	22.1 Elaborar inventario de contratos y fechas de renovación	06/07/15	10/07/15	100%	PSIS
		22.2 Establecer mecanismos de alertas de fecha de renovación	10/07/15	17/07/15	100%	PSIS
23.	Implementar extintores apropiados para equipos de	23.1 Selección de tipos y cantidad de extintores	13/07/15	17/07/15	100%	Coordinación SUM

	información	23.2 Adquisición e implementación de extintores	17/07/15	17/07/15	100%	Coordinación SUM
24.	Capacitación en uso de extintores	24.1 Capacitación en uso de extintores	17/07/15	21/07/15	100%	Coordinación SUM
25.	Implementar detectores de aniegos	25.1 Adquirir detectores de aniego	13/07/15	13/07/15	100%	Coordinación INF
		25.2 Definir zonas e implementar e implementar detectores de aniego.	14/07/15	17/07/15	100%	Coordinación INF
26.	Implementar detectores de Fuego	26.1 Implementar detectores de fuego	13/07/15	13/07/15	100%	Coordinación INF
		26.1 Definir zonas e implementar detectores de fuego.	14/07/15	17/07/15	100%	Coordinación INF
27.	Mejorar la seguridad del data center	27.1 Definir solución para la seguridad del data center.	03/08/15	06/08/15	100%	JSIS
28.	Implementar contingencia de servidores	28.1 Adquisición de servidores físicos, licencias, storage y software de aplicación.	03/08/15	01/09/15	100%	JSIS Y ASIS
		28.2 Instalación y configuración de equipos.	01/09/15	03/09/15	100%	JSIS Y ASIS
		28.3 Ejecutar pruebas de contingencia.	05/09/15	31/09/15	100%	JSIS y ASIS
29.	Adquisición de UPS exclusivamente para el Data Center	29.1 Cotización y adquisición de UPS	03/09/15	04/08/15	100%	Coordinación con INF
		29.1 Instalación de UPS	05/08/15	05/08/15	100%	Coordinación con INF
30.	Elaborar instructivos, políticas y procedimientos de operación y	30.1 Elaborar Instructivos, políticas y procedimientos	03/08/15	17/08/15	100%	ASIS Y JFSIS

	mantenimiento	para la operación y mantenimiento de Firewall				
		30.2 Elaborar Instructivos, políticas y procedimientos para la operación y mantenimiento de DNS	17/08/15	21/08/15	100%	ASIS Y JFSIS
		30.3 Elaborar Instructivos, políticas y procedimientos para la operación y mantenimiento del Server SAMBA (Archivos)	24/08/15	04/09/15	100%	ASIS Y JFSIS
		30.4 Elaborar Instructivos, políticas y procedimientos para la operación y mantenimiento de AS400	07/09/15	31/09/15	100%	ASIS Y JFSIS
		30.5 Elaborar Instructivos, políticas y procedimientos para la operación y mantenimiento AVAYA	01/09/15	11/09/15	100%	ASIS Y JFSIS
		30.6 Elaborar Instructivos, políticas y procedimientos para la operación y mantenimiento de Nextel (Server de Pedidos)	14/09/15	23/09/15	100%	ASIS Y JFSIS
		30.7 Elaborar Instructivos, políticas y procedimientos	24/09/15	02/10/15	100%	ASIS Y JFSIS

		para la operación y mantenimiento de SIDIGE (Asistencia)				

TABLA 13: PLAN DE TRATAMIENTO DEL RIESGO

Elaborado por el Autor

3.4. Análisis y Consolidación de Resultados

Para la mediación de los resultados de la implementación del Plan de seguridad de la Información sobre el proceso de Administración de Servidores del Área de Sistemas en la Empresa Corporación La Sirena, se tomó como referencia dos escenarios:

- Inventario de activos de información.
- Nivel de Mitigación de los Riesgos de los activos de información.
- Nivel de tolerancia en los riesgos en los activos de información.
- Plan de seguridad

Objetivos	Indicadores (%)	Formula	Meta
Reconocimiento de la situación actual de la seguridad de la Información en el área de sistemas para contribuir con la continuidad del negocio de la empresa Corporación La Sirena.	Inventario de activos de información	Cuadro de Inventario -	100%
Analizar y Gestionar el riesgo de la Seguridad de la Información a los activos del área de Sistemas en la Administración de los servidores que permitan la continuidad del negocio en la empresa Corporación La Sirena.	Nivel de mitigación de los riesgos de los activos de información	**RIESGO EFESTIVO>RIESGO RESIDUAL**	100%
	Nivel de tolerancia en los riesgos en los activos de información	• **NTR<NTE** • **RTR<RTE** • **TTR>TTE**	100%
Realizar un Plan de tratamiento de los Riesgos que permitirá la continuación del negocio en la empresa Corporación La Sirena.	Plan de Seguridad	Cuadro Plan de Seguridad	100%

TABLA14: OBJETIVOS VS INDICADORES

Elaborado por el autor

3.4.1. Nivel de Mitigación de los riesgos en los Activos de Información

En el desarrollo del modelo, para el Plan de Seguridad de la Información se hizo un análisis y gestión de los riesgos (Riesgos Efectivos/ Riesgos Residuales) en los activos de información, y mediante el Plan de tratamiento de riesgos varían estos valores para mitigar los riesgos.

Para la siguiente comparación se abarca todos los activos implicados en el proceso.

ACTIVOS DE INFORMACION	NIVEL DE RIESGO EFECTIVO	NIVEL DE RIESGO RESIDUAL
Daños en el Centro de Computo	59	37
perdida de registros vitales	110	57
Daños en la Infraestructura de red	53	31
Falta servicios Tercerizados	24	12
Daños en los activos de Software	25	12
Personal Inadecuado	88	28

TABLA 15: NIVEL DE MITIGACION DE RIESGOS

Elaborado por el autor

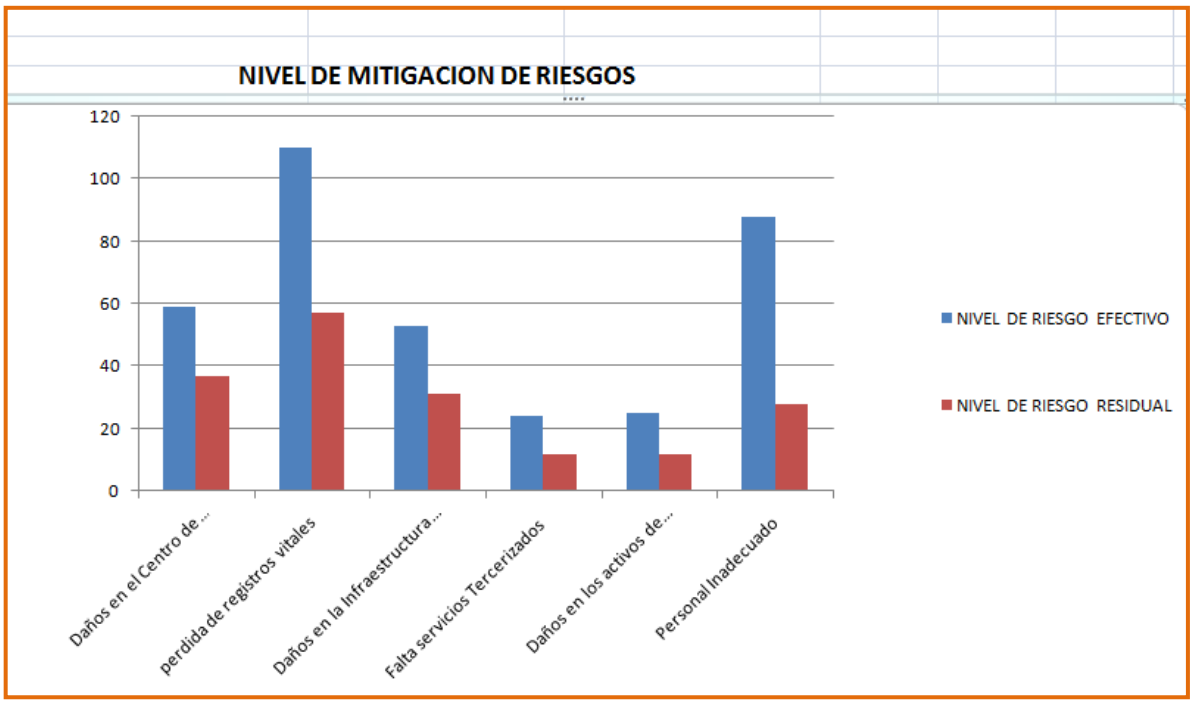


FIGURA 18: NIVEL DE MITIGACION DE RIESGOS

Elaborado por el autor

Este análisis demuestra que el riesgos residual (riesgos actual) en comparación al riesgo efectivos (anteriores), ha disminuido sobre los activos de información al implementar el plan de seguridad permitiendo la continuidad del negocio.

3.4.2. Nivel de Tolerancia en el riesgo de los Activos de Información

Aquí se analizara el impacto de cuan tolerable es un riesgo frente a una amenaza en un activo de la Información. A continuación se realiza un análisis de los totales de tolerancia obtenido en la

investigación antes y después de implementar el plan de seguridad en el proceso de Administración de servidores

	Total de Tolerancia en Riesgos			Total de Tolerancia en Riesgos %		
RIESGOS	NT	RT	TT	NT %	RT %	TT %
TOLERANCIA EFECTIVA	4	11	1	25%	68.75%	6.25%
TOLERANCIA RESIDUAL	0	0	16	0%	0%	100%

TABLA 16 TOTAL DE TOLERANCIA EN RIESGOS %

Elaborado por el autor

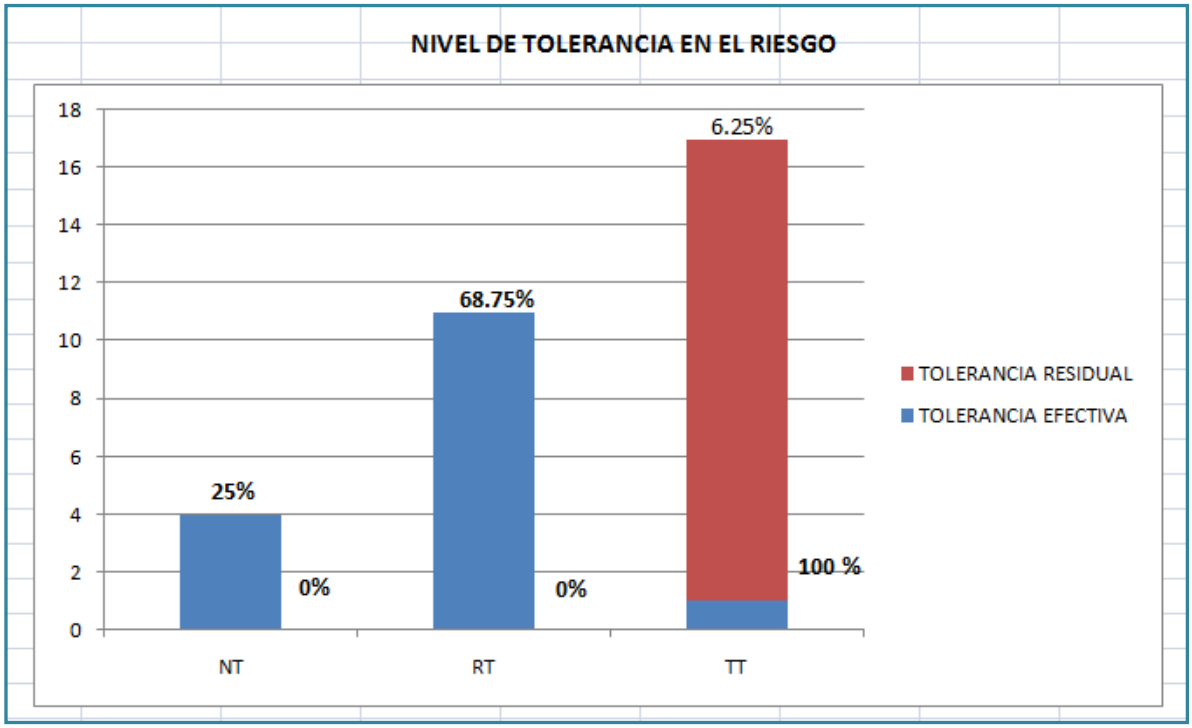


FIGURA 19: NIVEL DE TOLERANCIA EN EL RIESGO %

Elaborado por el autor

Este análisis muestra:

- ✓ NT: el nivel de tolerancia del riesgo efectivo ante la tolerancia del riesgo residual de varia en un 25 % ya que al implementarse el plan de seguridad reduce la tolerancia efectiva en 0%.
- ✓ RT: el nivel de tolerancia del riesgo efectivo ante la tolerancia del riesgo residual de varia en un 68.75 % al implementarse el plan de seguridad reduce la tolerancia efectiva en 0%.
- ✓ TT: el nivel de tolerancia del riesgo efectivo ante la tolerancia del riesgo residual de varia de 6.25% a un 100% tolerable ya que al implementarse el plan de seguridad aumenta la tolerancia residual a si permite cumplir con el objetivo de la investigación que es de darle continuidad al negocio con normalidad por ende.

3.4.3. Análisis de indicadores

Objetivo 1: Al iniciar el proyecto no existía un plan de seguridad de la información que proteja los activos y permita la continuidad del negocio, para darle comienzo se realizó el reconocimiento del proceso y sus activos que lo afectan y que a posterior permiten la continuación de la investigación, esto mediante un Inventario de Activos.

Objetivo 2: Con los resultados del Análisis y Gestión de los riesgos se pudo obtener que después de la Implementación del Plan de seguridad de la información, se logró detectar de manera preventiva las vulnerabilidades, mitigando así los futuros riesgos.

De la misma forma, se logró Implementar procesos de atención inmediata para las vulnerabilidades e incidentes reportados para la Administración de los Servidores como proceso crítico.

- Que los niveles de riesgo disminuyeron significativamente, después de la implementación del Plan de seguridad de la información, lo que permite que los procesos de negocio continúen su operación pese a incidentes.
- Muchos de los riesgos con calificativo no tolerable se redujo a 0% y totalmente tolerable en 100% después de aplicarse el Plan de seguridad de la información.

Objetivo 3: La elaboración del plan del riesgo permitió planificar e implementar soluciones que reducen los riesgos de forma preventiva, soluciones al momento y a futuro, esto permitió darle la continuidad a los procesos de negocio de la empresa Corporación la Sirena.

3.4.4. Análisis de los beneficios

- ✓ Provee a la gerencia dirección y apoyo para gestionar la seguridad de la información.
- ✓ Permite prepararse para una futura certificación en ISO 27001, antes poniendo como base la implementación de la ISO 27002 en toda la empresa.
- ✓ Ayuda a identificar los activos de información y a protegerlos adecuadamente.

- ✓ Asegura una correcta y segura operación de información del proceso crítico, reduciendo riesgos de error humano.
- ✓ Incrementa, sustancialmente, el control de acceso a la información.
- ✓ Minimiza la interrupción en el funcionamiento de las actividades del negocio de la empresa.
- ✓ Demuestra confianza al mercado, proveedor, sociedad y el mismo personal de la empresa.

CONCLUSIONES

1. La aplicación de un plan de seguridad de la información en base a la norma ISO 27002 dominio 17 le permite tener un mejor sistema de gestión en el área de sistemas y toda la organización, de esta manera reducir sus riesgos y estar preparado para actuar de manera inmediata ante cualquier problema, permitiendo su continuidad.

2. Para la implementación de plan de seguridad de la información se requiere de un análisis minucioso y fiable de la situación actual de la empresa, mediante normas y metodologías que no sean rígidas, que se ajusten a su necesidad.

3. Muchas organizaciones tienen un paradigma equivocado, creen que documentar procesos es una pérdida de tiempo. Por lo tanto la documentación de procesos es una herramienta poderosa para el mantenimiento y mejora de cualquier sistema de gestión de la organización.

4. Después de la implementación de un plan de seguridad de la información, se presentaran más activos de información, más amenazas y vulnerabilidades por tanto mayores riesgos. Este escenario no se puede evitar, es por ello que se debe estar preparado para actuar de manera inmediata ante cualquier nueva vulnerabilidad.

5. Los resultados obtenidos de la investigación bajo la Norma ISO 27002 Dominio 17 y metodologías, son útiles y novedosos para la organización ya que le permite actuar de forma adecuada ante las amenazas latentes.

RECOMENDACIONES

1. Se recomienda mantener una constante revisión del plan de seguridad de la información, verificar el cumplimiento por parte de los encargados y empleados de la organización.

2. Establecer los mecanismos que permitan la identificación de nuevos activos de información, también la cultura organizacional para tomar acciones correctivas frente a nuevas vulnerabilidades, amenazas o riesgos y en base a esa información tomar acciones preventivas.

3. Continuar con la utilización de Normas y metodologías para gestionar los riesgos en todos los procesos del área de sistemas y toda la organización en sí; ya que de esta manera se puede lograr una reducción en los riesgos a los cuales son sometidos los activos de información de la organización.

4. Se recomienda realizar una documentación a todos los procesos de la organización para poder gestionarlos de manera óptima y hacer frente a cualquier cambio que se pueda dar.

BIBLIOGRAFÍA

Fuentes Bibliográficas

1. Alexander, Alberto G. (2007) Diseño de un Sistemas de Gestión de Seguridad de la Información (Primera edición), Alfaomega, Colombia.

2. Javier Areitio Bertolín. (2008). Seguridad de la información. Redes, informática y sistemas de información. España: Magallanes.

3. Ing. Manuel Collazos Vallager, Colegio de Ingenieros del Perú, (2014). La nueva versión ISO: 27001-2013, Lima, Perú.

4. Luis Gómez Fernández Ana Andrés Álvarez (2012) “Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes” 2° edición, AENOR, Madrid-España

5. Luz Marina Méndez Hinojosa, José Armando Peña Moreno (2007).Manual práctico para el diseño de la escala de likert, México.

Fuentes Electrónicas

1. Julián Gonzales. (2012 - 2014). ¿Seguridad Informática o Seguridad de la Información?, de Seguridad para Todos, Sitio web: http://www.seguridadparatodos.es/2011/10/seguridad-informatica-o-seguridad-de-la.html
2. Elvira Mifsud. (2012-2015). Introducción a la Seguridad Informática/Seguridad de la Información. España, Madrid, de Gobierno de España Sitio web: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1
3. Departamento de Seguridad Informática. (2012). Amenazas a la Seguridad de la Información. Buenos Aires, Argentina, de Universidad Nacional de Luján Sitio web: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12
4. Ing. Carlos Ormella Meyer. (2014). Normas ISO de SI. Madrid, España, de Red Informática de criptografía y seguridad de la información Sitio web: http://www.criptored.upm.es/descarga/normas_segu_info_marzo_2014.pdf
5. Ing. Carlos Ormella Meyer. (2014). Normas ISO de SI. Madrid, España, de Red Informática de criptografía y seguridad de la información Sitio web: http://www.criptored.upm.es/descarga/normas_segu_info_marzo_2014.pdf
6. DRI International. (2013). El portal de ISO 27002 en Español. España, de ISO 27002.ES Sitio web: http://www.iso27000.es/iso27002_17.html
7. Extraída de: Portal de Administración Electrónica. (2012). MAGERIT v. 3.Metodologia de análisis y gestión de riesgos de los SI. España, de Gob. España Sitio web: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.ViR6s9Ivfct
8. Portal de Administración Electrónica. (2012). MAGERIT v. 3.Metodologia de análisis y gestión de riesgos de los SI. España, de Gobierno de España Sitio web: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.ViR6s9Ivfct

9. Gobierno Informático. (2010). Administración de Riesgos. España, de Seguridad Informática Sitio web: http://cata-seguridaddelainformacion.blogspot.pe/2010/03/administracion-de-riesgos.html

ANEXOS

PRESENTACION DEL PROYECTO	
IDENTIFICACION DE LA INSTITUCION	
Nombre de la institución:	Corporación la Sirena
Ubicación:	Jr. Gonzales Prada 420, Surquillo – Lima, Perú
RUC	20100157315
Autoridades Responsable:	Gerente General, Katherine Gavillo
	Gerente Administración, Norma Castañeda
	Jf. de Sistemas, Wolfg Lojas
DESARROLLO DEL PROYECTO	
Responsable del Proyecto:	Asistente de Sistemas, Nataly Laor
Nombre del Proyecto:	"Implementación de un plan de seguridad de la información en base a la Norma ISO 27002 para la continuidad del negocio en el proceso de administración de servidores del área de sistemas de la empresa Corporación La Sirena"
Área:	Área de Sistemas
Proceso de estudio:	Administración de Servidores
Objetivos:	Implementar un plan de seguridad de la información para la continuidad de negocio.
	Realizar un reconocimiento de los activos de Información para su análisis.
	Realizar un análisis y gestión de los riesgos de los activos de información
	Realizar un plan de gestión de los riesgos
Resultado Esperado:	Contar con un plan de seguridad de la información que le permita a la empresa continúan con sus procesos de negocio pese a incidentes.
Duración Total del Proyecto:	Mayo –Noviembre 2015
Justificación del Proyecto:	En vista de los constantes incidentes de perdida, modificación de información, cortes de luz, robos informáticos, etc. de tiene la necesidad de resguardar y permitir su continuidad de los procesos de negocio de la empresa.

REUNIONES EFECTUADAS PARA LA DETERMINACION DE DATOS EN EL PROYECTO		
OBJETIVO	**FECHA DURACION**	**RESPANSABLES**
Para determinar el proceso crítico:	Mayo 01-03 2015	JEFE DE SISTEMAS ASISTENTE DE SISTEMAS
Activos de información que afectan al proceso de administración de los servidores	Mayo 2015	JEFE DE SISTEMAS ASISTENTE DE SISTEMAS PRACTICANTE DE SISTEMAS
Valoración para el análisis y evaluación del riesgo	Mayo – Noviembre del 2015	JEFE DE SISTEMAS ASISTENTE DE SISTEMAS PRACTICANTE DE SISTEMAS
Implementación de las soluciones al riesgo “Plan de riesgos”	Mayo – Noviembre del 2015	JEFE DE SISTEMAS ASISTENTE DE SISTEMAS PRACTICANTE DE SISTEMAS

<table>
<tr><th colspan="2">ELABORACION DE LA ESCALA DE LIKERT EN ANALISIS DEL RIESGO</th></tr>
<tr><td colspan="2">Para los riesgos ya determinados que afectan al proceso Administración de Servidores</td></tr>
<tr><td>Probabilidad de materialización de las amenazas Valoración</td><td>Pregunta</td></tr>
<tr><td><table>
<tr><td>5: MUY ALTO</td><td>Ocurrencia diaria</td></tr>
<tr><td>4: ALTO</td><td>Ocurrencia Semanal</td></tr>
<tr><td>3: MEDIO</td><td>Ocurrencia Mensual</td></tr>
<tr><td>2: BAJO</td><td>Ocurrencia Anual</td></tr>
<tr><td>1: MUY BAJO</td><td>Ocurrencia en dos añon a mas</td></tr>
</table></td><td>¿Con que frecuencia ocurre la amenaza…….?</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Impacto que ocasiona una amenaza al materializarse</td><td>Pregunta</td></tr>
<tr><td><table>
<tr><td>5: MUY ALTO</td><td>Afecta a mas de un area</td></tr>
<tr><td>4: ALTO</td><td>Afecta a un area</td></tr>
<tr><td>3: MEDIO</td><td>Afecta a un usuario, no hay posibilidad de trabajoalterno</td></tr>
<tr><td>2: BAJO</td><td>Afecta a un usuario, hay posibilidad de trabajoalterno</td></tr>
<tr><td>1: MUY BAJO</td><td>No afecta a la productividad</td></tr>
</table></td><td>¿Cuánto es su alcance de impacto del…….?</td></tr>
<tr><td colspan="2">Se le asigna una valoración a en la escala de Muy alto y Muy bajo para la probabilidad de amenazas se materialicen y su impacto.</td></tr>
</table>

<table>
<tr><th colspan="2">ANALISIS Y EVALUACION DE LOS RIESGOS</th></tr>
<tr><td></td><td></td></tr>
<tr><td>Valoración = C + I + D</td><td>Valoración es la suma de los tres pilares de la seguridad de la información donde:
*C = CONFIDENCIALIDAD
*I = INTEGRIDAD
*D = DIPONIBILIDAD</td></tr>
<tr><td>Riesgo = Probabilidad * Impacto + Valoración</td><td>RIESGO EFECTIVO
Ya que el riesgo no se puede eliminar pero si mitigar esta fórmula permite representar el riesgo en un valor numérico.</td></tr>
<tr><td><table><tr><td>Totalmente Tolerante: TT</td><td>4-15</td></tr><tr><td>Regularmente Tolerante: RT</td><td>16-25</td></tr><tr><td>No Tolerable: NT</td><td>26-40</td></tr></table></td><td>TOLERANCIA EFECTIVA
Se le asigna un valor numérico a la tolerancia dependiendo a la escala en el cuadro.</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td>Riesgo Residual = Probabilidad R * Impacto R + Valoración</td><td>RIESGO RESIDUAL
Ya que el riesgo no se puede eliminar pero si mitigar esta fórmula permite representar el riesgo en un valor numérico.</td></tr>
<tr><td><table><tr><td>Totalmente Tolerante: TT</td><td>4-15</td></tr><tr><td>Regularmente Tolerante: RT</td><td>16-25</td></tr><tr><td>No Tolerable: NT</td><td>26-40</td></tr></table></td><td>TOLERANCIA EFECTIVA
Se le asigna un valor numérico a la tolerancia dependiendo a la escala en el cuadro.</td></tr>
</table>