UNIVERSIDAD CATOLICA DE SANTA MARIA

FACULTAD DE CIENCIAS E INGENIERIAS FISICAS Y FORMALES

PROGRAMA PROFESIONAL DE INGENIERIA DE SISTEMAS

"Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del Estado"

Tesis presentada por:

Jackeline Tatiana Suca Ancachi

Para optar el Titulo Profesional de:

Ingeniero de Sistemas

AREQUIPA-PERU

2014

Presentación

Sra. Directora del Programa Profesional Ingeniería de Sistemas

Sres. Miembros del Jurado Examinador de Tesis

De conformidad con la disposición del reglamento de Grados y Títulos del Programa Profesional de Ingeniería de Sistemas, remitimos a vuestra consideración el estudio de investigación titulado **"Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del Estado"**, el mismo que al ser aprobado me permitirá optar el Título Profesional de Ingeniero de Sistemas.

Arequipa, Setiembre de 2014

Jackeline Tatiana Suca Ancachi

DEDICATORIA

Esta tesis se la dedico en primer lugar a Dios quién supo guiarme por el buen camino, por darme fuerzas para seguir adelante y no desmayar en los problemas, por mostrarme día a día que con humildad, paciencia y sabiduría todo es posible.

Con todo mi cariño y mi amor a mi madre y padre hicieron que yo pudiera lograr mis sueños, a ustedes por siempre mi corazón y mi agradecimiento.

A mi hermana Maritza por apoyarme en cada momento de mi vida, por motivarme y darme la mano en los momentos más difíciles; y a mi hermana Lourdes por creer en mí, ser paciente conmigo, por sus consejos. Las quiero mucho.

A mi hermano Helmer por ser mi segundo padre, que me ha ayudado a crecer, gracias por estar siempre conmigo en todo momento. Gracias por la paciencia, por el cariño que me das para poder salir adelante y por el apoyo en la realización de la tesis, mi hermano Wilder por ser mi amigo, por aconsejarme y quien siempre me motiva seguir adelante. Los quiero mucho

A mis sobrinos Mijail y Omar por darme la alegría en los momentos más difíciles.

A todas las personas por creer en mí y por apoyarme con sus palabras: a mi cuñado Javier, a mis amigas y a amigos.

Mi agradecimiento a la Universidad Católica Santa María, que me brindó la oportunidad de realizar mis estudios y el cual he recibo apoyo.

A todos mis profesores de la carrera por sus conocimientos, consejos, confianza y formación.

Agradezco a los Ingenieros Manuel Zúñiga, Jorge Martínez y Fernando Paredes por sus observaciones realizadas al trabajo de tesis exigiendo de esta manera hacer un trabajo de calidad, por su paciencia y apoyo incondicional.

INDICE

INDICE DE FIGURAS

INDICE DE FORMATOS

RESUMEN

El SGSI son siglas de un Sistema de Gestión de la Seguridad de la Información, ayuda a establecer procedimientos y controles para la continuidad del negocio de la institución.

El Sistema de Gestión de la Seguridad de Información (SGSI)protege a los activos de información así como, correos electrónicos, informes, actas, página web, documentos, software, hardware, contratos, que ayuda a garantizar los posibles riesgos sean conocidos, asumidos, gestionados y minimizados por la empresa de una forma documentada y estructurada.

El Sistema de Gestión de Seguridad de la Información está definido en la norma ISO 27001, utilizando el ciclo Deming PDCA (Plan, Hacer, Verificar, Actuar) consiste en cuatro fases, especificando requerimientos para mitigar los riesgos que afecten a la institución.

En el presente trabajo se elabora una propuesta metodológica usando la NTP /ISO 27001:2008 en la implementación de un Sistema de Gestión de Seguridad de la Información en una entidad del Estado para mejorar la seguridad de los activos de información y mitigarlos, en caso de haber posibles riesgos que afectan a la continuidad del negocio.

ABSTRACT

The ISMS is anacronym for Management System of Information Security, it helps establish procedures and controls for business continuity of the institution.

The Management System of Information Security (ISMS) protects information assets as well as emails, reports, transactions, web pages, documents, software, hardware, contracts, helping to ensure risks to be known, assumed, managed and minimized by the company in a documented and structured form.

The Management System of Information Security is defined in ISO 27001, using the Deming PDCA cycle (Plan, Do, Check, Act) consists of four phases, specifying requirements to mitigate risks that affect the institution.

In this paper, a methodological proposal was developed, using NTP/ISO 27001: 2008 on the implementation of a Management System of Information Security in a state entity to improve the security of information assets and mitigate if there are potential risks that affect business continuity.

INTRODUCCIÓN

Los activos de información tienen un valor importante para las entidades públicas del Estado, son responsables de su protección y garantizar su confidencialidad, integridad y disponibilidad, ante las amenazas o vulnerabilidades que ponen en riesgo a sus activos de información.

Los riesgos tienen la posibilidad de presentarse y provocar daños a los activos, pueden ser causados por amenazas naturales, humanas, tecnológicas, sociales e instalaciones, por lo cual deben contar con acciones preventivas y correctivas para prevenir los riesgos.

La seguridad de información es un proceso que debe ser controlado, gestionado y monitorizado[1] por la empresa, con el objetivo de garantizar una adecuada implementación de una metodología con el propósito de proteger sus activos tomando como base fundamental el modelo ciclo de Deming conocido como PDCA (Plan, Hacer, Verificar, Actuar) fundamentado en la norma técnica peruana ISO/IEC 27001:2008, con el objetivo de implementar adecuadas políticas de seguridad e involucrar a toda la empresa.

[1]Monitorizado: Realizar seguimiento constante a la información.

CAPÍTULO I

PLANTEAMIENTO OPERACIONAL

1.1 TÍTULO DE LA TESIS

Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en instituciones públicas del Estado

1.2 ANTECEDENTES

Es importante recalcar que el cibercrimen generó pérdidas de US$117.440 millones en los últimos meses del año 2013 en todo el mundo, y aquellos ataques informáticos han provocado 378 millones de víctimas; en los países más afectados por los ataques son Rusia, China y Sudáfrica, incluyendo en la lista a Estados Unidos que lidera en el cibercrimen con 39.146 millones de dólares, segundo China, con 37.796 millones y tercero Europa, con 12.149 millones, según el director de marketing de la compañía de antivirus Norton by Symantec, Roberto Testa, en un informe anual sobre cibercrimen.

En la siguiente figura publicada por Kaspersky Lab (2013), se muestra que nuestra región en términos de ataques informáticos, con un porcentaje de 44 % al 52% de usuarios atacados. Asimismo, también se observa que si un usuario vive en México tiene la probabilidad de ser infectado con un virus en un 50%.Pero en Rusia, India y otros donde la probabilidad es más alta de ataques informáticos con un 76%.

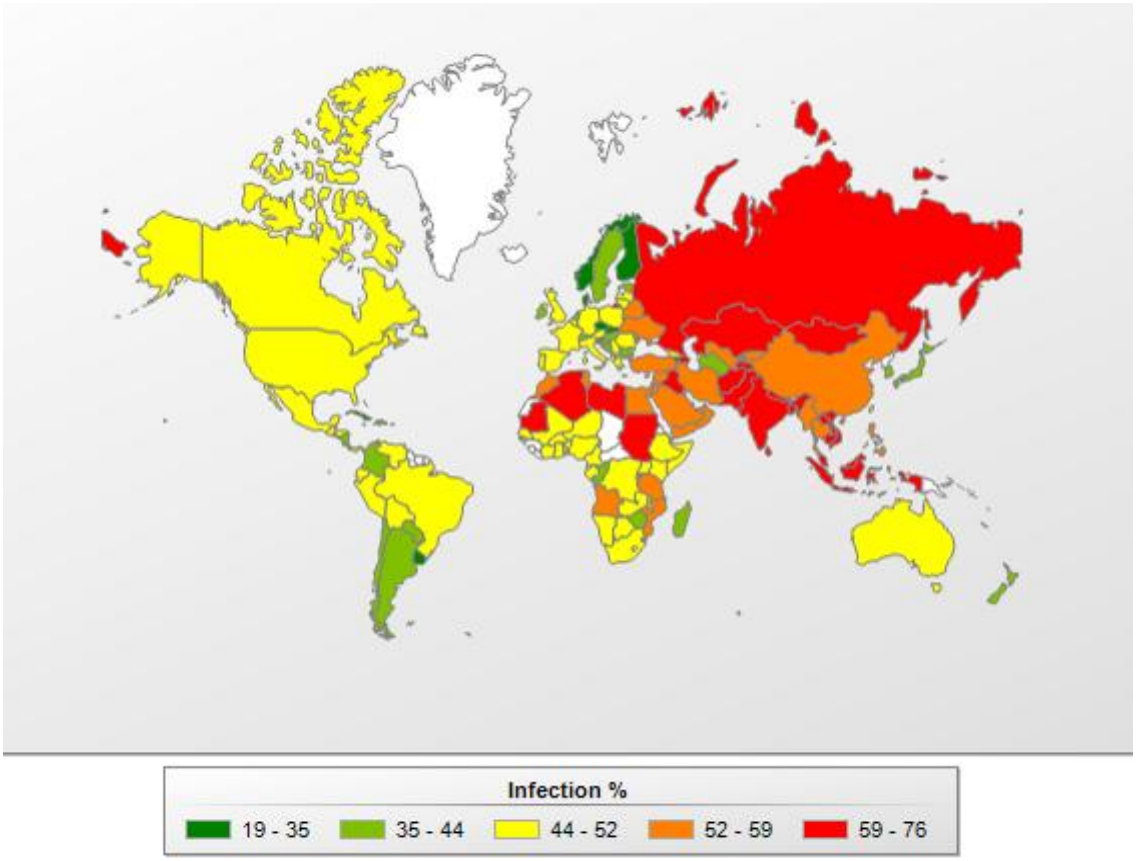


Figura 1.1
Fuente: Informe el panorama de malware en América Latina en el 2013: pronóstico para el 2014, Kaspersky Lab (2013)

El Perú no es ajeno a los cibercriminales, tal como lo informa el diario El Comercio (2013) el Perú es líder en producción de virus informáticos en América Latina, información obtenida del "Informe el panorama de malware en América Latina en el 2013: pronóstico para el 2014", publicado por Kaspersky Lab, que señala que los cibercriminales de Brasil y el Perú generaron la mayor cantidad de código malicioso, es decir que 49.78% de usuarios peruanos sufrieron por los menos un intento de infección en el año 2013, frente al 49.04% de Brasil y el 48.12% de México. Estos ataques según Kaspersky buscan el robo de dinero o de información.

KPMG (2012), elaboró un informe sobre fraude en el Perú, revelando que el 63% de los ejecutivos de las principales firmas nacionales y filiales extranjeras que operan en el país fueron víctimas de fraude. En el 15% de los casos los daños económicos superaron los US$ 500. En general la malversación de activos es el fraude más frecuente (relacionados a los activos financieros) y la corrupción es el segundo fraude más común, seguido por la falsificación de documentación, robo y el fraude de información. Esta información confirma que un ataque mal intencionado por un *hacker* puede afectar la operatividad de la empresa en forma parcial, total, temporal o permanente. Por esta razón, las empresas tienen que enfocar su atención a los posibles riesgos que afectan a los activos de información.

Esta situación ha llevado que el Gobierno Peruano emita políticas respecto a la seguridad de información, a través de Lineamientos de su Política Nacional de Seguridad en el Estado (2002), determina que " una política de seguridad es una estrategia frente a los riesgos que atentan contra la confidencialidad, la integridad y la disponibilidad de los recursos informáticos en las entidades públicas, por lo cual se elabora estrategias para la identificación de los riesgos tanto internos como externos". Con el fin de fortalecer la seguridad de información en las empresas con una gestión de políticas, procedimientos, monitoreo de los posibles riesgos, que garanticen detectar las vulnerabilidades y amenazas contra los activos de información. Para ello se requiere de una metodología que acompañe a la empresa que ayude a mitigarlos y otorgue la confianza a los involucrados a los directivos de la empresa.

Por ello es importante la aplicación de la Norma Técnica Peruana NTP 27001:2008,según el Instituto Nacional de Competencia y de la Protección de Propiedad Intelectual (INDECOPI, 2013), "define que la implementación de un Sistema de Gestión de Seguridad

de Información (SGSI), permite proteger y reducir los riesgos que puedan afectar a los activos de la empresa. El Sistema de Gestión de Seguridad de Información permite proteger la información asegurando su confidencialidad, integridad y disponibilidad para brindar la confianza a las instituciones, empleados, clientes; permitiendo responder oportunamente a los incidentes que puedan afectar a la empresa".

Es necesario que las empresas del estado identifiquen los posibles riesgos, ante posibles vulnerabilidades y amenazas futuras que puedan existir en los activos de información, en algunos casos como accesos no deseados a personas no autorizadas, robo de data, robo hardware, modificación de datos, eliminación de copias de seguridad o cualquier otra acción que ataquen contra la integridad, disponibilidad y confidencialidad en los activos de información.

Las empresas pueden convertir en objetivo de ataques por parte de personas no autorizadas, quienes tratan de acceder esta información para ocasionar daños o perjudicar a la empresa, para beneficio propio o para simple satisfacción personal.

1.3 PREGUNTA GENERAL DE INVESTIGACIÓN

¿Es posible desarrollar un procedimiento para implementar la seguridad de información tomando como base la NTP 27001:2008 de la seguridad de la Información para las empresas del estado peruano?

1.4 OBJETIVOS DE INVESTIGACIÓN

a) Objetivo General

Elaborar una propuesta metodológica para la implementación de la NTP ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas.

b) Objetivos Específicos

- Aplicar el ciclo de Deming (PDCA) que ayude a garantizar la implementación de la gestión de la seguridad de la información en una entidad del estado.
- Identificar y desarrollar las actividades y tareas para la propuesta metodológica.
- Desarrollar procedimientos para identificar y tratar los riesgos que afectan a los activos de información en una entidad pública del estado.

1.5 HIPÓTESIS

Es posible desarrollar una propuesta metodológica usando la Norma Técnica Peruana ISO/IEC 27001:2008 para implementar un sistema de gestión de seguridad de la información en entidades públicas del Estado.

1.6 VARIABLES

a) Dependiente

Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas.

Indicadores

- Estructurado
- Usabilidad
- Amplitud

b) Independientes

- Norma 27001:2008

- Seguridad de la Información
- Gestión de Riesgos

1.7 JUSTIFICACIÓN

En el Perú los ataques informáticos van en aumento, la cifra supera el 50%, por lo cual significa que de cada cien empresas más del 80% son vulnerables a los ataques especialmente en los ministerios del Estado según Andréz Lamouroux Consultor Especialista en Seguridad de la Información y Gerente de Soluciones de Seguridad de Aranda Software. Por esta razón, la investigación aporta elementos, para identificar y gestionar los riesgos en la institución pública, que busca evitar en lo posible ataques a sus activos de información, el cual debe estar respaldada por una gestión de seguridad y procedimientos adecuados, que amerita la participación de los gerentes y empleados.

La reducción de las vulnerabilidades y amenazas a través de una propuesta metodológica ayudara a gestionar la seguridad de la información, identificando las fases y actividades, para la implementación de la metodología.

Finalmente, la propuesta metodológica se basa en el cumplimiento de las buenas prácticas de la Norma Técnica Peruana NTP 27001:2008 para la implementación de un sistema de gestión de seguridad de la información.

1.8 ALCANCES Y LIMITACIONES

a) Alcances

La propuesta está dirigida a las entidades públicas del estado peruano, con el **fin de proteger los activos de la información**, para establecer procedimientos adecuados

e implementarlos, con la finalidad de disminuir los posibles riesgos y vulnerabilidades que existan.

b) Limitaciones

La aplicación de la propuesta metodológica se limitará al área de informática o tecnologías de información que se encargan de la administración de la seguridad de la entidad del Estado, la investigación consistirá en la recopilación de información para lograr mitigar la pérdida de activos, ante posibles riesgos y vulnerabilidades que se presentan en la entidad pública.

CAPÍTULO II

MARCO TEÓRICO

2.1 ESTADO DEL ARTE

Aranda (2009), presentó el trabajo titulado "Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador", da a conocer que "la evolución de la tecnologías de la información y con la continuidad del negocio, así como las posibles amenazas y vulnerabilidades aumentan, por lo tanto es preciso proteger a los activos, garantizando la disponibilidad, la confidencialidad e integridad en la empresa. La forma más adecuada para proteger los activos de información es logrando identificar y centrarse en los posibles riesgos".

Según Gavilanes (2011) en su "Metodología para la implementación de un Sistema de Gestión de la información", "la norma ISO 27001 garantiza la seguridad en la disponibilidad, integridad y confidencialidad, por lo cual determina que una adecuada implementación de la metodología puede lograr mejoras en la seguridad de la información. Con el propósito de identificar los riesgos y amenazas. Mediante esta metodología se garantiza el cumplimiento de las buenas prácticas de seguridad de la Norma ISO 27001 para la empresa".

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

2.2.1 Definición de la Seguridad de Información

Según Wikipedia.org, define como un conjunto de medidas preventivas que permiten resguardar y proteger la información manteniendo la confidencialidad, la disponibilidad e integridad de la empresa.

2.2.2 Factores que amenazan a la Seguridad de Información

Existen diferentes factores que pueden afectar a la seguridad de información dentro de una empresa:

- Factor Humano: son la principal fuente de amenaza que pueden afectar a los activos de información, tales como: personal no autorizado, robo, sabotaje, fraude e ingeniería social.
- Factor Hardware: se presenta cuando hay fallas físicas en los elementos de hardware que conforman las áreas y oficinas de la empresa.
- Factor software: se presenta cuando hay posibles fallas dentro del software de un sistema operativo, software mal desarrollado, software malicioso.
- Factor Natural: este factor se presenta cuando tienen su origen de la naturaleza.

2.2.3 Definición del SGSI.

Según ISO27001.es, sostiene que el Sistema de Gestión de Seguridad de la Información (SGSI) tiene el propósito de garantizar que los posibles riesgos que se presenten sean conocidos, asumidos, y minimizados por la empresa en una forma documentada, estructurada y conocida por el gerente y los empleados.

El Sistema de Gestión de la Seguridad de la Información (SGSI), consiste en la preservación de su confidencialidad, integridad y disponibilidad de los activos, para poder

garantizar la seguridad de la información siendo gestionada correctamente, se define los siguientes tres aspectos importantes que debe tener la seguridad de información:

a) Confidencialidad.

También conocida como privacidad. Se define que la información sea conocida por personas autorizadas dentro de la empresa (Álvarez y García, 2007). Mendillo (2001), asegura que la información no puede estar disponible a persona no autorizadas. En el caso de existir la falta de confidencialidad en la información puede provocar daños a la empresa.

b) Integridad.

Según Álvarez y García (2007), señala que la información debe ser modificada, creada y borrada solo por el personal autorizado, dicha modificación debe ser registrada para posteriores controles. Según Mendillo (2001), asegura que la información recibida y enviada sea exactamente igual, es decir que no haya sido modificada o alterada en su contenido.

c) Disponibilidad.

Para Álvarez y García (2007), señala que la información y sus activos deben estar disponibles a los usuarios autorizados cuando lo requieran. Es decir que la información debe estar en el lugar y momento adecuado.

2.2.4 Para qué sirve un SGSI.

Para Inteco.com, el Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer políticas, procedimientos y controles, con el fin de mantener el riesgo que se asumible para la empresa y así tomar medidas o acciones para mitigarlos.

Según León (2012), las empresas están expuestas a numerosas amenazas, y también a posibles vulnerabilidades, sometiendo a los activos a diferentes de riesgos como fraude, espionaje, sabotaje, robo o vandalismo. Por ejemplo en caso de los virus informáticos, el "hacking" son algunos ejemplos comunes y conocidos, pero se deben considerar que los riesgos son causados espontáneamente e involuntariamente dentro de la empresa.

El Sistema de Gestión de la seguridad de la información ayuda a la empresa a identificar los riesgos que están sometidos los activos de información y tomar decisiones sobre la estrategia a seguir para mitigarlos.

El Sistema de Gestión de la Seguridad de la Información (SGSI), ayuda a proteger a los activos de información de las amenazas producidas por las vulnerabilidades que presentan los activos, permitiendo conocer los riesgos, teniendo los controles adecuadamente implementados para proteger a los activos de la institución, tal como se muestra en Figura 2.1.

Figura 2.1
Fuente: http://www.iso27000.es/sgsi.html

2.2.5 Requisitos de la documentación de un SGSI.

Para Gavilanes (2011), un Sistema de Gestión de la Seguridad de la Información (SGSI) está formado por una serie de documentos que se clasifican en cuatro niveles tal como se

muestra en la Figura 2.2.Cabe señalar que la documentación de un Sistema de Gestión de la Seguridad de la Información tiene los siguientes niveles:

Figura 2.2
Fuente: Implementación de un Sistema de Gestión de la Seguridad de la Información en Desitel de la Espoch, Gavilanes (2011)

a) Documentos de Nivel 1 Manual de seguridad.

En el nivel 1 manual de seguridad contiene el alcance, objetivos, responsabilidades que debe tener la institución.

b) Documentos de Nivel 2 Procedimientos.

En el nivel 2 procedimientos, contiene documentos o informes que ayudan asegurar que se realicen la planificación, implementación y control de los procesos de seguridad de la información en la institución.

c) Documentos de Nivel 3 Instrucciones y formularios.

En el nivel 3 instrucciones y formularios, describen en cómo realizar las tareas y actividades.

d) Documentos de Nivel 4 Registros.

En el nivel 4 registros, proporciona el cumplimiento de los requisitos del SGSI; tal como los documentos generados en los tres niveles superiores.

2.2.6 Beneficios de un SGSI.

Segúnceeisec.com, existen importantes beneficios al implementar un SGSI en una empresa:

a) Realizar la identificación de los riesgos para identificar las amenazas, vulnerabilidades que afectan a la empresa.

b) Minimizar los riesgos en los activos de información

c) Tener una mejora continua en los procesos o actividades.

d) Incrementar la concientización del gerente y los empleados de la empresa en la mejorar de la seguridad de la información.

e) Permite mejorar la imagen de la empresa respecto a la seguridad de sus activos.

f) Cumplir con la política y procedimientos de protección a los activos, como el gerente y los empleados.

En la Figura 2.3 de la Página "Iso 27001.es" se muestra una balanza en donde se compara los costes versus beneficios resaltándose que los beneficios tienen preponderancia sobre los costos en la implementación de Sistema de Gestión de Seguridad de la Información.

Figura 2.3
Fuente: http://www.iso27000.es/sgsi.html

2.2.7 Implementación de SGSI.

Según Gavilanes (2011),se debe establecer y gestionarla implementación del SGSI, para ello se utiliza el ciclo continuo de Deming o PDCA, el cual es tradicional en los sistemas de gestión de la calidad. En la Figura 2.4 se muestra el Ciclo PDCA, a continuación se explicara las cuatros fases:

Figura 2.4
Fuente: http://www.contactopyme.gob.mx/benchmarking/conceptos/ben_pro.asp

a) <u>Plan</u>: Establecer el SGSI.

Según pqsperu.com, define los puntos para el planteamiento del SGSI:

- Establecer alcance del SGSI, debe contener las características del negocio de la empresa y ubicación de los activos, el propósito del SGSI es abarcar toda la empresa; de hecho, es recomendable empezar por un alcance limitado.
- Definir el enfoque de evaluación de riesgos para el SGSI y las necesidades de la empresa, por ende, la ISO 27005 apoya a los requisitos del Sistema de Gestión de Seguridad de la Información fundamentados en la ISO 27001.

- Identificar los activos de información y sus responsables dentro de la empresa.
- Identificar las amenazas y vulnerabilidades de los activos de información.
- Analizar y evaluar los riesgos que afecten a los activos, determinado acciones para la mitigación.
- Identificar e implementar los controles adecuados para lograr la mitigación de los activos de información.
- Definir las responsabilidades de la seguridad, que coordine las tareas, por lo cual será necesario designar un comité de seguridad que trate y busque soluciones respecto a la seguridad de información.
- Especificar una política de la empresa, mostrando el compromiso del gerente y los empleados con la implementación del SGSI fundamentada en la NTP/ISO 27001:2008 y coordinar con los responsabilidades y tareas asignadas.

b) Hacer (*do*)– Implementar.

Según pqsperu.com, define los puntos para la implementación del SGSI:

- Definir un tratamiento de los riesgos y responsables del mismo para resguardar la seguridad de la información.
- Implementar el tratamiento de riesgo con medidas o acciones para mitigar los riesgos.
- Implementar controles adecuados que se presenten en los activos y afecten a la continuidad del negocio de la empresa.
- Desarrollar procedimientos e instrucciones para la implementación del SGSI.

- Implementar y asignar recursos, programas de capacitación y concientización de los empleados.

c) <u>Chequear (*Check*)</u> - Monitorizar y revisar el SGSI.

Según pqsperu.com, define los puntos para el monitoreo y revisión, en caso de haberse producido retrasos en el SGSI.

- Ejecutar procedimientos y revisiones: para detectar los avances de los procedimientos, así como las fases y actividades que se están desarrollando en la empresa.
- Revisar regularmente la evaluación de los riesgos; así como las amenazas y las vulnerabilidades.
- Se debe revisar periódicamente el SGSI por los responsables de la seguridad de la información, para verificar si el alcance sigue siendo conforme, como los objetivos de seguridad de la información.
- Actualizar los planes de seguridad en función de la revisión del SGSI
- Efectuar periódicamente auditorías internas, para determinar si los procesos y procedimientos siguen siendo conformes respecto a los requisitos definidos por la ISO-27001.

d) <u>Actuar (*Act*)</u> - Mantener y mejorar el SGSI.

Según Gavilanes (2011), define los puntos para mantener y mejorar el SGSI:

- Adoptar acciones correctivas, están basadas en la identificación de la causa del problema para evitar un incidente y ocurrencias que volverá a repetirse si no se elimina la causa que lo originó.

- Adoptar acciones preventivas, son aquellas acciones para prevenir que ocurran algo. Estas acciones es prevenir los problemas, determinado cual es la posible fuente de problemas que afecten a la seguridad de información con el objeto de eliminarla.
- Definir acciones de mejora en los objetivos establecidos y los procesos.
- Asegurar el alcance de los objetivos establecidos por la empresa y los responsables de la seguridad de la información.

En la Figura 2.5 se muestra el Ciclo de Deming aplicado al SGSI, identificando las actividades a seguir en un ciclo PDCA, esta figura confirma lo descrito en los párrafos anteriores.

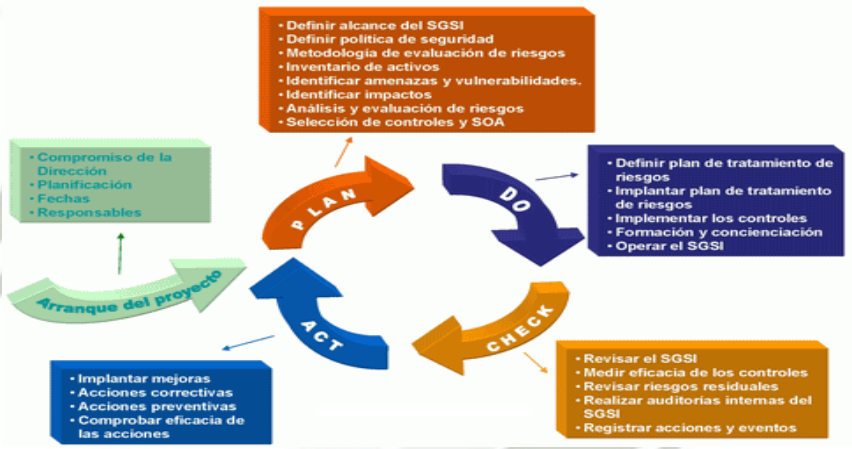


Figura 2.5
Fuente: Ciclo de Deming – Mejora Continua (2005), http://www.iso27000.es/sgsi_implantar.html#seccion1

2.2.8 Tareas de la Gerencia para el SGSI.

Para Gavilanes (2011), es un elemento fundamental la participación de la gerencia de la empresa en la implantación de un Sistema de Gestión de Seguridad de la Información (SGSI) definida por la ISO 27001. La tarea de la gerencia se debe asumir desde un principio de la implementación del SGSI que afecta fundamentalmente a la gestión del

negocio y requiere, por tanto, decisiones y acciones que sólo puede tomar la gerencia de la empresa.

Según León (2012), hay algunas tareas fundamentales del SGSI que asigna a la dirección y se detallan en los siguientes puntos:

a) Compromiso de la Dirección.

Según León (2012), la empresa debe comprometerse con el planteamiento, implementación, revisión, mantenimiento y mejora del SGSI. Se debe tomar las siguientes iniciativas:

- Implantar una política de seguridad de la información.
- La gerencia debe garantizar el alcance de los objetivos establecidos.
- Designar responsabilidades para la seguridad de la información
- Designar todos los recursos disponibles para el SGSI.
- Realizar revisiones del SGSI en un determinado tiempo, establecido por la gerencia de la empresa.

b) Formación y Concientización.

La formación y la concientización[2]es un factor muy importante en la implementación de un SGSI. La gerencia debe designar a los empleados responsabilidades del SGSI, León (2012). Se debe tener en cuenta los siguientes aspectos:

- Establecer el personal adecuado para realizar las tareas de aplicación del SGSI.
- Evaluar las acciones realizadas por el personal que contribuyen a conseguir los objetivos establecidos para implantar el SGSI.

[2]: Concientización: Acción y efecto de crear conciencia entre la gente acerca de un problema o fenómeno que se juzga importante.

Por consiguiente, la gerencia debe asegurar que los empleados deben tener la concientización de la importancia de la implementación y contribución SGSI para la seguridad de información de la empresa.

c) Revisión del SGSI

La dirección de la empresa asigna revisar el SGSI durante un determinado tiempo, lo recomendable es una vez al año, para asegurar que sea adecuado y eficaz para la empresa, León (2012).Por ende, debe recibir información que le ayudaran tomar decisiones adecuadas para la revisión del SGSI:

- Revisión de auditorías del SGSI
- Revisión de observaciones, realizadas por la gerencia y los empleados.
- Proponer y revisar nuevas mejoras en procedimientos que pudieran ser útiles para beneficio y eficacia del SGSI para la empresa.
- Realizar revisiones de medidas o acciones preventivas y correctivas respecto a los riesgos.
- Revisar las vulnerabilidades y amenazas que no fueran identificadas o tratadas adecuadamente en evaluaciones de riesgos de los activos de información.

Según León (2012), cuando se realiza las revisiones de los informes o de la documentación presentada, la gerencia debe tomar decisiones y acciones referentes al SGSI:

- Realizar mejoras del SGSI
- Realizar actualizaciones de la evaluación y mitigación de los riesgos.

- Establecer modificaciones a los procedimientos y controles que no están adecuadamente implementados.
- Verificar la efectividad de los controles implementados.

2.3 NTP ISO/EIC 27001:2008.

2.3.1 Origen de la ISO 27001

La Norma ISO 27001 fue publicada el 15 de Octubre de 2005, esta norma contiene los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) en ingles se conoce como Information Security Management System (ISMS). Tiene su origen en la norma de BSI (British Standards Institution) BS 7799-2esta norma fue publicada en 1998 para certificar la implementación del SGSI dentro de una empresa. La norma ISO 27001:2008 tiene en un Anexo A, donde se encuentra los objetivos de los controles que forma parte del proceso del SGSI, Álvarez y García (2007).

2.3.2 Definición de la ISO 27001.

Según Gavilanes (2011), la norma ISO/IEC 27001 establece una serie sugerencias para elaborar una metodología para un Sistema de Gestión de la Seguridad de la Información (SGSI) para una empresa, la norma se aplica a todo tipo de empresas, incluyendo el tamaño o actividad del negocio.

Para ISO 27001.es, determina los requerimientos para implementar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información conocido con las siglas SGSI, se apoya con el Ciclo de Deming (PDCA) con su acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar).

Según pqsperu.com, define cómo establecer la seguridad de la información en cualquier tipo de empresa, con o sin fines de lucro, privada o pública, pequeña o grande, u objetivo con el propósito de aportar una metodología para la implementación un sistema de gestión de seguridad de la información para la empresa.

2.3.3 Beneficios de la ISO 27001.

Segúnpqsperu.com, la norma ISO 27001 tiene los siguientes beneficios:

a) Contiene una norma clara y estructurada para la seguridad de información.
b) Permite minimizar los posibles riesgos de los activos de información.
c) Implementar y revisar adecuadamente los controles.
d) Integrarse con otros sistemas de gestión como la iso 9001, iso 14001.
e) Permite la continuidad del negocio de la empresa, de acontecimientos que puedan afectar a la empresa.
f) Permite la concientización de los gerentes y empleados respecto a la seguridad de información.

2.3.3 Objetivos de la Norma ISO 27001.

Según Álvarez y García (2007), la norma ISO 27001 tiene los siguientes objetivos:

a) Aportar beneficios con la implementación de SGSI para aumentar la seguridad de en la empresa.
b) La implementación del SGSI ayuda con procedimientos definidos para la seguridad de la información
c) Determina con la implementación del SGSI en un área específica de la empresa, la responsabilidad de mitigar los riesgos y resguardar la seguridad de la información.

2.3.4 Resolución Ministerial de la Norma 27001: 2008

En la Resolución Ministerial 129-2012-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2008 EDI Tecnologías de Información, esta resolución tiene por objetivo incrementar los niveles de Seguridad de la Información en las entidades del Estado establecido por el Consejo de Ministros del Estado Peruano.

2.4 GESTIÓN DE RIESGOS.

2.4.1 Modelos de Gestión de Riesgos

a) Estándar Australiano/neozelandés (ASNZS 4360:2004)

Según Bedon, Urtilla y Ortega (2012), es un proceso de gestión de riesgos planteado por la norma AS/NZS 4360:2004, contiene los siguientes procesos: establecimiento del entorno de la empresa, identificación de riesgos, análisis de riesgos, evaluación de riesgos y tratamiento de riesgos.

b) ISO 31000:2009

Según Bedon, Urtilla y Ortega (2012), define pautas de cómo administrar los posibles riesgos de forma sistemática y transparente que puedan afectar a la institución. El enfoque está constituido por tres elementos claves: los principios para la gestión de riesgos, la estructura de soporte, el proceso de gestión de riesgos.

c) Metodología de Análisis y Gestión de Riesgos de Tecnologías de Información (MAGERIT)

Según Bedon, Urtilla y Ortega (2012), la metodología MAGERIT, desarrollada por el Consejo Superior de Administración Electrónica, y publica por el Ministerio de

Administraciones Publicas de España, está conformado por dos únicos procesos: el análisis de riesgos y gestión de riesgos.

d) Octave

Según SecurityArtWork.com, fue desarrollada por la Universidad Carnegie Mellon y su acrónimo significa "Operationally Critical Threat, Asset and Vulnerability Evaluation", estudia los riesgos en base a tres principios: Confidencialidad, Integridad y Disponibilidad.

e) Cramm

Según SegurityArtWork.com, fue desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico, su acrónimo proviene de CCTA Risk Analysis and Management Method. Contiene tres fases: Definición global de los objetivos de seguridad, Análisis de riesgos e identificación de amenazas y Selección de medidas de seguridad.

En la página "ISO 27000.ES" de gestión de riesgos se muestra la Figura 2.6, cuya fuente es "http://www.iso27000.es/sgsi_implantar.html#seccion1", se define el enfoque de gestión de riesgos apropiada para el SGSI y cualquier requerimiento de negocios.

Figura 2.6
Fuente: http://www.iso27000.es/sgsi_implantar.html#seccion1

2.4.2 Definición de Riesgo

Según Flores (2007), el riesgo es un daño potencial, puede surgir por un proceso presente o un evento futuro. Para González y Tenemaza (2012), un riesgo es como una amenaza, que ocasiona una pérdida de información que afecten al negocio de la empresa.

2.4.3 Gestión de Riesgos

Según Pallas (2009), es un proceso iterativo, por lo cual permite tener un análisis de riesgos. Consiste en la identificación, valoración y su tratamiento del riesgo, para la continuidad del negocio de la empresa y la seguridad de la información de los activos de información.

2.4.4 Proceso de Evaluación de Riesgo

En la Figura 2.7 se muestra el proceso de evaluación del riesgo que permite a una empresa para poder mitigar los riesgos, está conforme con los requerimientos del estándar ISO

27005, apoyando particularmente los requisitos del sistema de gestión de seguridad de la información definidos en ISO 27001.

Figura 2.7
Fuente: Proceso de Evaluación de Riesgo,
Elaboración Propia.

a) Identificación de Riesgos (Activos).

Para Alexander (2012), consiste que cada activo debe estar identificado, clasificado y con su respectivo responsable del mismo acordada por la empresa. Los activos necesitan protección para asegurar la seguridad y la continuidad de la empresa.

Según Peltier (2001), la identificación de los activos es vital para poder mantener una adecuada protección de los activos de la empresa.

Según Poveda (2013), para facilitarla administración y mantenimiento de un inventario de activos se puede clasificar en diferentes categorías los activos de la siguiente manera:

- Activos de información: contiene la base de datos, archivos de datos, documentación del sistema, manuales de usuario, acta, informes.
- Documentos impresos: documentos impresos, contratos, lineamientos, documentos de la compañía, documentos que contiene importantes del negocio.
- Activos de software: contiene software de aplicación, software de sistemas, herramientas de desarrollo.
- Activos físicos: contiene a los equipos de comunicación y computación de la empresa.
- Personal: contiene a los empleados, clientes y proveedores.
- Servicios: consiste en la prestación de servicios técnicos para la empresa

b) Identificación de Amenazas y Vulnerabilidades.

Para Alexander (2012), se debe identificar los riesgos que afecten a la seguridad de la empresa:

- Amenaza: consiste en un incidente no deseado, en él puede causar daño a la empresa, se puede presentar acceso no autorizado, robo, código malicioso,
- Vulnerabilidad: consiste en debilidades de los activos como procedimientos mal definidos y ausencia de política de seguridad. Estas debilidades causan incidentes no deseados, y pueden causar pérdidas, daño o deterioro a los activos de información que tiene la empresa.

c) Mitigación de Riesgos.

Para Poveda (2012), define que los riesgos una vez identificados y evaluados, la siguiente etapa es identificar y evaluar la medida apropiada de cómo tratar los riesgos.

El objetivo primordial es describir la forma de las medidas o acciones que se va realizar para reducir los riesgos. Se presenta las siguientes acciones preventivas y correctivas:

- Acciones Preventivas.

  Son aquellas acciones o medidas que permite eliminar la causa, es decir, antes de que ocurra en los activos. La acción preventiva tiene como objetivo de eliminar y evitar que se produzca dentro de la empresa.

- Acciones Correctivas.

  Son aquellas acciones o medidas que permite la eliminación de la causa origen del problema, y poder evitar que se pueda repetir en el futuro.

d) Listado de Riesgos

Para Alexander (2012), consiste en identificar y seleccionar controles de seguridad apropiados y justificados.

La selección de los controles permite la mitigación de las amenazas y vulnerabilidades que existen en la empresa y en activos. Cuando se seleccionan controles para la implementación se debe tener en cuenta los siguientes puntos:

- El uso correcto de controles
- Permite ayudar a los usuarios en implementar adecuadamente y que cumplan con los requisitos de seguridad de la empresa.

e) Matriz de Riesgos

Para Bedon, Urtilla y Ortega (2012), menciona si el nivel de riesgo es aceptable, el proceso finaliza, en caso contrario, se define un tratamiento para evitar o mitigar; y se

establece los controles que resguarden la seguridad de los activos. Se define los siguientes aspectos que tiene una matriz de riesgos:

- Impacto: consiste en el daño sobre el activo que proviene de una amenaza que afecten a la empresa.
- Probabilidad de Ocurrencia: consiste en que como se presenta una amenaza y provoca que la vulnerabilidad dañe a los activos que puedan afectar a la empresa.
- Nivel de Riesgo: consiste el resultado entre el impacto y probabilidad para determinar el nivel de riesgo en los activos, respecto a las vulnerabilidades y amenazas para determinar si el riesgos es aceptable o inaceptable

2.5 PROPUESTAS METODOLOGICAS PARA IMPLANTAR EL SGSI.

En la Página Web de ISO 27001.es, a continuación se ilustra dos figuras que son importantes para la implementación de la SGSI, en ese sentido en la Figura 2.8 con un enfoque de procesos se muestra la documentación mínima que debe considerarse tales como:

a) Definición de la Política y objetivos de seguridad.
b) Definición del Alcance del SGSI.
c) Identificación de los procedimientos y controles que apoyan el SGSI.
d) Describir el método de evaluación del riesgo.
e) Presentación de un informe sobre la evaluación de riesgo.
f) Determinar un plan de tratamiento de riesgos.
g) Declaración de aplicabilidad (SOA -Statement of Applicability-).
h) Procedimientos para gestionar la documentación del SGSI.

Del mismo modo, en la Figura 2.9 se muestra las actividades que deben seguirse en la implementación de un SGSI, la misma que guarda relación con los conceptos descritos en los párrafos anteriores.

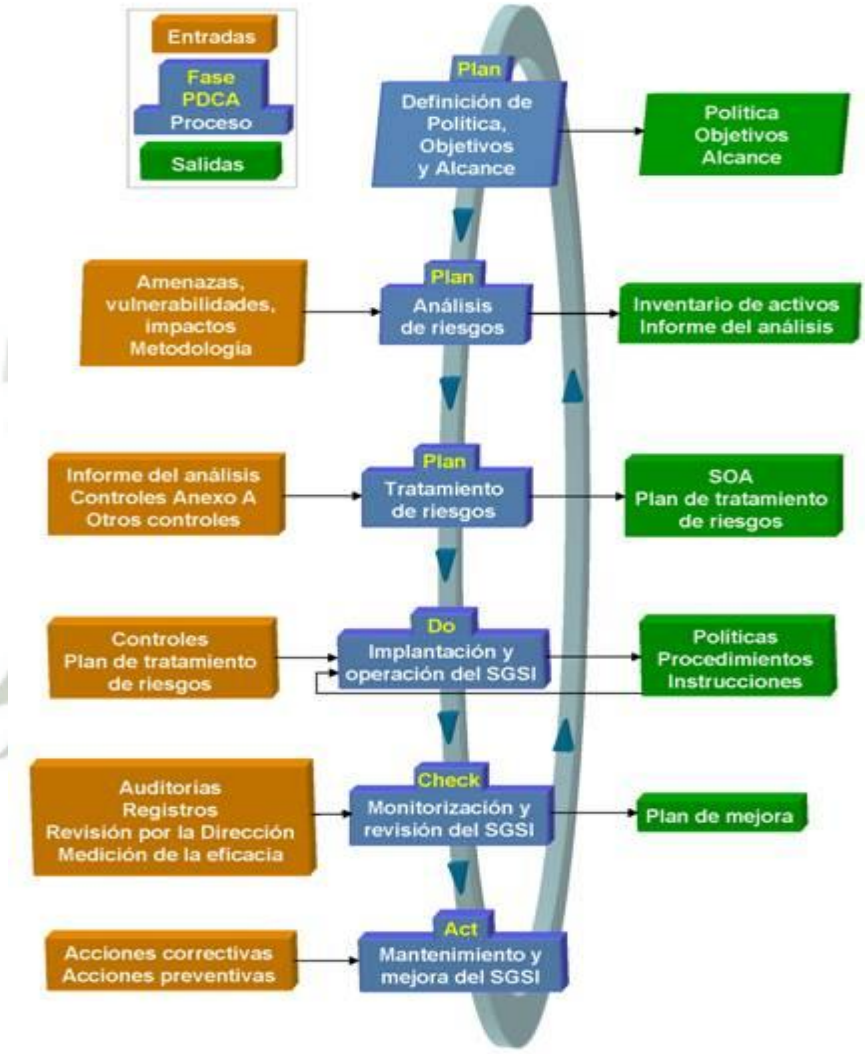


Figura 2.8
Fuente: Propuesta Metodológica Enfoque a Procesos, Página Web ISO 27000.ES, http://www.iso27000.es/sgsi.html

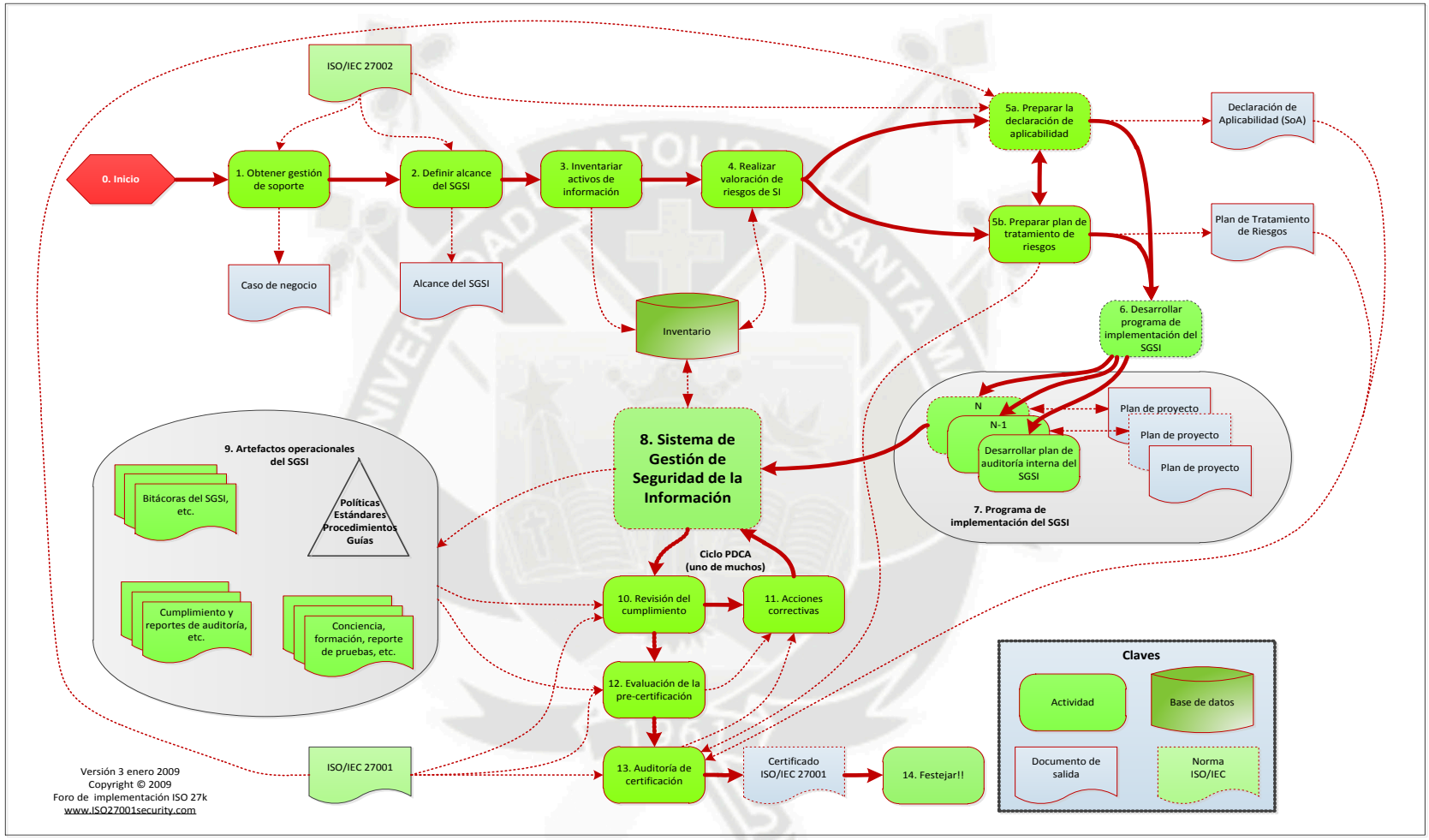


Figura 2.9

Fuente: Implantación del SGSI elaborado Foro de implementación ISO 27k, Página Web ISO 27000.ES, http://www.iso27000.es/sgsi.html

CAPITULO III

PROPUESTA METODOLÓGICA

3.1 RESUMEN DE LA PROPUESTA

A continuación se detalla la estructura de la propuesta metodológica para implementar la norma ISO 27001:2008 con las siguientes fases:

3.1.1 Inicio

a) Acta de Constitución del Comité de Seguridad de la Información

3.1.2 Fase de Planeamiento

a) Definición de la Organización del SGSI.

b) Definición del Alcance.

- Estructura de Desglose de Trabajo (EDT o por sus siglas en inglés WBS) del proyecto.
- Recursos del Proyecto (Estructura de Desglose de Riesgo o por sus siglas en ingles RBS).

c) Plan del SGSI

- Identificación de Activos
- Plan de Gestión de Tiempo
- Plan de Gestión de Costos

- Plan de Gestión de las Comunicaciones
- Plan de Riesgos (Identificación de Riesgos, Acciones de Mitigación de Riesgos, Matriz de Riesgos o Listado de Riesgos y Matriz de Valoración de Riesgos)

3.1.3 Fase de Implementación

- Enunciado del Cronograma y Actualización
- Ficha de Lista de Actividades
- Implementación de Acciones de Mitigación de Riesgos
- Implementación de Listado de Riesgos
- Implementación de Matriz de Valoración de Riesgos

3.1.4 Fase de Monitoreo y Revisión

- Informe de Plan de Proyecto
- Informe de Revisión de los Riesgos
- Informe de Actividades
- Ficha de Sugerencia y Mejora

3.1.5 Fase de Cierre

- Informe de Cierre del Proyecto
- Acta de Transferencia del Proyecto del SGSI

3.2 INICIO

La Dirección del Empresa elabora una Acta de Constitución para la implementación de la NTP ISO/IEC 27001:2008, el acta debe contener el nombre del proyecto y el nombre del gerente general de la empresa.

PROYECTO SGSI Acta de Constitución para la Implementación del Proyecto		
SGS 001	**Versión de la plantilla: 1.0.0**	**Fecha:**
1.- DATOS GENERALES		
Nombre del Proyecto		
Nombre de Gerente General		
Fecha		
Habiéndose cumplido con todos los requerimientos, estándar y criterios de aceptación establecidos, los firmantes aceptamos formalmente el proyecto.		
2.- FIRMAN EN SEÑAL DE APROBACION		
NOMBRE COMPLETO	**FIRMA**	**FECHA**

Formato 3.1 Acta de Constitución del Comité
Fuente: Elaboración Propia

3.3 FASE PLANEAMIENTO

3.3.1 Definición de la Organización del SGSI

La Dirección de la Entidad del Estado debe mostrar su compromiso y aportar los recursos necesarios para la protección de los activos de información de los riesgos, se creara un comité de seguridad con las siguientes jefaturas, que integraran y participaran en la implementación del proyecto, y por lo cual se escogerá por votación por mayoría al jefe del proyecto.

PROYECTO SGSI Miembros del Comité de Seguridad		
SGSI 002	**Versión de la Plantilla:1.0.0**	**Fecha:**
Jefaturas	**Comité de Seguridad**	
Gerente General	Gerente General	
Jefe del Proyecto	Líder del Proyecto	
Jefatura de Área de Tecnologías de Información	Líder de Área de Tecnologías de Información	
Jefatura de Área de Recursos Humanos	Líder de Área de Recursos Humanos	
Jefatura de Área de Logística	Líder de Área de Logística	
Jefatura de Asesoría Legal	Líder de Área de Asesoría Legal	

Formato 3.2 Miembros del Comité
Fuente: Elaboración Propia

3.3.2 Definición del Alcance del Proyecto

El Comité de Seguridad debe establecer el alcance del Sistema de Gestión de Seguridad de la Información (SGSI), identificando a los activos de información, tales como, datos, software, activos fijos, servicios, y personas.

El propósito principal es establecer un Sistema de Gestión de Seguridad de la Información basado en la norma NTP/ISO-IEC 27001:2008, tratando de conseguir su confidencialidad, integridad y disponibilidad de los activos, así asignando a los responsables que estén correctamente determinados para garantizar la seguridad de la información.

a) Elaborar Enunciado del Alcance del Proyecto

- El Jefe del Proyecto define el alcance del proyecto.
- El jefe del proyecto envía un correo electrónico a los miembros del comité de seguridad convocando a una reunión para sustentar los puntos del alcance del proyecto.
- Si algún miembro de comité de seguridad, realiza cambios al alcance del proyecto, según lo indicado por la reunión, envía un correo electrónico y presenta una solicitud, indicando los puntos a modificar o agregar.

b) Revisar el Enunciado del Alcance del Proyecto

- El Jefe del Proyecto revisa la solicitud y en caso de realizar los cambios, envía un correo electrónico a los miembros del comité y solicita que se revise, especialmente, aquellos puntos presentados en la solicitud.

- Los Miembros del Comité de Seguridad revisa los puntos y si hubiera algo adicional que modificar, explicar de qué se trata y deben llegar a un consenso para la aprobación del Alcance del Proyecto.

c) Aprobar el Enunciado del Alcance del Proyecto

- Los Miembros del Comité de Seguridad, envía un correo electrónico al jefe del proyecto, e indicar la aprobación del Alcance del Proyecto.
- El Jefe del Proyecto y los Miembros del Comité de Seguridad firman la aprobación del Alcance del Proyecto, en caso contrario de no aprobar, indicar el motivo de su rechazo al documento. Anexo C

PROYECTO SGSI Alcance del Proyecto		
SGSI 002_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Jefe de Proyecto	<Nombre del Líder del Proyecto>	
Fecha	<Fecha de presentación del Proyecto>	
Objetivos del Proyecto	<Describir las metas hacia las cuales se debe dirigir el trabajo del proyecto en términos como el alcance, tiempo y costo, calidad del proyecto y las metas de la Entidad del Estado>	
Justificación del Proyecto	<Se debe describir la justificación del proyecto>	
Alcance del Proyecto	<Se debe describir el alcance general del proyecto, así como las exclusiones que no se van a considerar en el presente proyecto>	
Entregables del Proyecto	<Se presentara entregables de cada actividad dentro del proyecto>	
Propósito del Producto	<Se debe describir el propósito del producto>	
Descripción del Producto	< Describir el producto, servicio según sea el caso, en sus términos funcionales>	
Objetivos del Producto	<Describir metas hacia las cuales se debe dirigir el trabajo del producto dentro de la empresa/entidad del Estado>	
APROBACION DEL COMITÉ		
En caso de rechazo (indicar el motivo)		
Miembros del Proyecto	**Nombre y Apellidos**	**Firmas**

Formato 3.3 Alcance del Proyecto
Fuente: Elaboración Propia

d) Procedimiento de Actualización del Alcance del Proyecto

- En caso de haber un cambio se debe llenar una solicitud indicando los puntos a modificar o agregar.
- La Solicitud de Cambio contendrá una categoría y prioridad para determinar el riesgo que afecte al alcance del proyecto.
- El proceso que se contempla como recepción de la Solicitud de Cambio es el siguiente:

  El jefe de proyecto recibe la solicitud de cambio.

  El jefe de proyecto revisa la prioridad y categoría, especificados en el formato 3.4.

  El jefe de proyecto evalúa el impacto.
- Cuando se haga la implementación del cambio, el jefe de proyecto debe asegurar que el alcance del proyecto esté de acuerdo al cambio solicitado, envía un correo electrónico a los miembros del comité de seguridad.
- Los Miembros del Comité de Seguridad revisa y deben llegar a un consenso para la aprobación del alcance del proyecto, envía un correo al jefe de proyecto indicando su aprobación al cambio solicitado.
- El Jefe de Proyecto y el Comité de Seguridad firman la aprobación del cambio, en caso de no aprobar, indicar el motivo del rechazo.

PROYECTO SGSI **Descripción de Prioridad y Categoría**		
SGSI 002_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Prioridad	**Descripción**	
Emergencia	<Un cambio que si no se implementa de inmediato puede ocasionar un gran problema a la empresa/entidad>.	
Alta	<Un cambio que es importante para la empresa que debe ser implementado pronto>.	

Media	<Un cambio que es una mejora para el proyecto>.
Baja	<Un cambio que puede ser conveniente o una mejora pero solo en cuestión de forma y que no tendría un gran impacto en el proyecto si se ejecutara>.
Categoría	**Descripción**
Mayor	<Un cambio cuyo impacto sea una gran parte parala área o sector de la Empresa/Entidad del Estado>
Significativa	<Un cambio cuyo impacto en el área, no es mayor, es decir, puede afectar mitad del área de la Empresa/Entidad del Estado>.
Menor	<Un cambio cuyo impacto afecta a un pequeña parte del área de la Empresa/Entidad del Estado>.

Formato 3.4 Categoría y Prioridad
Fuente: Elaboración Propia

PROYECTO SGSI **Solicitud de Cambio del Alcance del Proyecto**		
SGSI 002_4	**Versión de la Plantilla 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud: dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante _____		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio		
PRIORIDAD ☐ Emergencia ☐ Alta ☐ Media ☐ Baja **CATEGORIA** ☐ Mayor ☐ Significativo ☐ Menor **IMPACTO DE NO IMPLEMENTAR EL CAMBIO**		
_____ Firma		
2.- APROBACION DEL COMITÉ		
( ) Aprobado	( ) Desaprobado	
(En caso de rechazo, indicar el motivo)		

ROL	NOMBRE	FECHA	FIRMA

Formato 3.5 Solicitud de Cambio del Alcance del Proyecto
Fuente: Elaboración Propia

3.3.3 Estructura de Desglose de Trabajo (EDT) del proyecto

a) Elaborar Estructura de Desglose de Trabajo

- El Jefe de Proyecto y los Miembros del Comité presenta la Estructura de Desglose de Trabajo conocido como EDT. Ver figura 3.1
- Si algún Miembro del Comité de Seguridad hace un cambio al desglose de trabajo, envía un correo electrónico y solicita una reunión, para explicar y llegar a un consenso para contemplar el cambio solicitado.

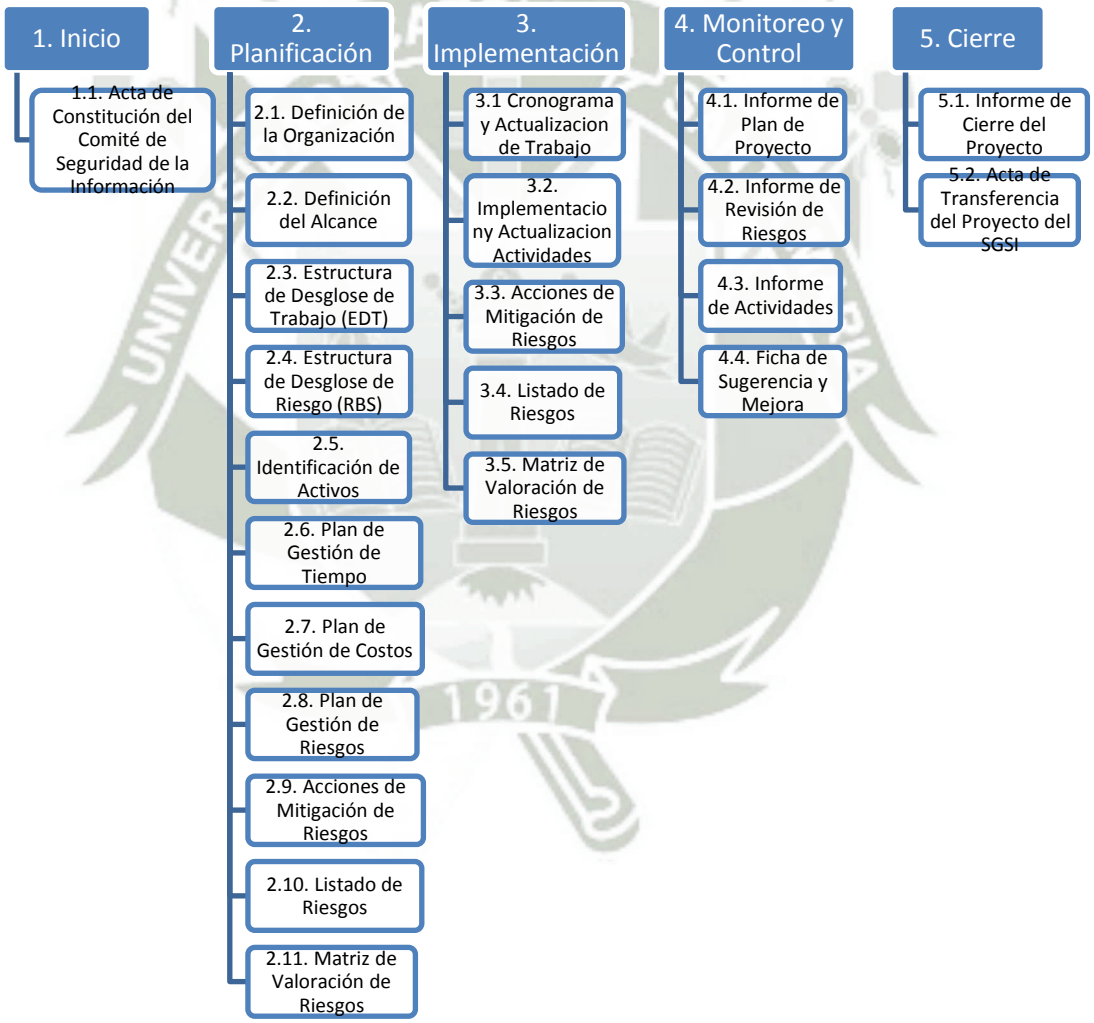


FIGURA 3.1 Estructura de EDT
Fuente: Elaboración Propia

b) Revisar la Estructura de Desglose de Trabajo

- El Jefe del Proyecto revisa la solicitud y en caso de realizar los cambios, envía un correo electrónico a los miembros del comité y solicita que se revise, especialmente, aquellos puntos presentados en la solicitud.
- Los Miembros del Comité de Seguridad revisa el cambio realizado a la Estructura de Desglose de Trabajo, y si hubiera algo adicional que modificar, explicar de qué trata y deben llegar a un consenso para la aprobación de la Estructura de Desglose de Trabajo.

c) Aprobar la Estructura de Desglose de Trabajo

- Los Miembros del Comité de Seguridad envía un correo electrónico y entrega la Estructura de Desglose de Trabajo al jefe del proyecto, indicando su aprobación del contenido.
- El Jefe del Proyecto y los Miembros del Comité de Seguridad firman la aprobación de la Estructura del Desglose de Trabajo, caso contrario de no aprobar, se regresa al punto anterior, indicando el motivo de su rechazo al documento.

PROYECTO SGSI **Solicitud de Cambio de Estructura de Desglose de Trabajo**		
SGSI 003	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud: dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		
IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS		

Firma
2.- APROBACION DEL COMITÉ
( ) Aprobado ( ) Desaprobado
(En caso de rechazo, indicar el motivo)

ROL	NOMBRE	FECHA	FIRMA

Formato 3.6 Solicitud de Cambio de Estructura de Desglose de Trabajo
Fuente: Elaboración Propia

3.3.4 Recursos del Proyecto o Desglose de Riesgos

a) Elaborar Estructura de Desglose de Riesgos

- El Jefe de Proyecto y los Miembros del Comité de Seguridad presenta la Estructura de Desglose de Riesgo conocido como RBS para el proyecto. Ver figura 3.2
- Si algún Miembro del Comité de Seguridad hace un cambio a la estructura, solicita una reunión, para explicar y llegar a un consenso para contemplar el cambio.
- Los Miembros de Comité de Seguridad envía un correo electrónico y presenta la solicitud de cambio, indicando los puntos a modificar o agregar a la estructura.

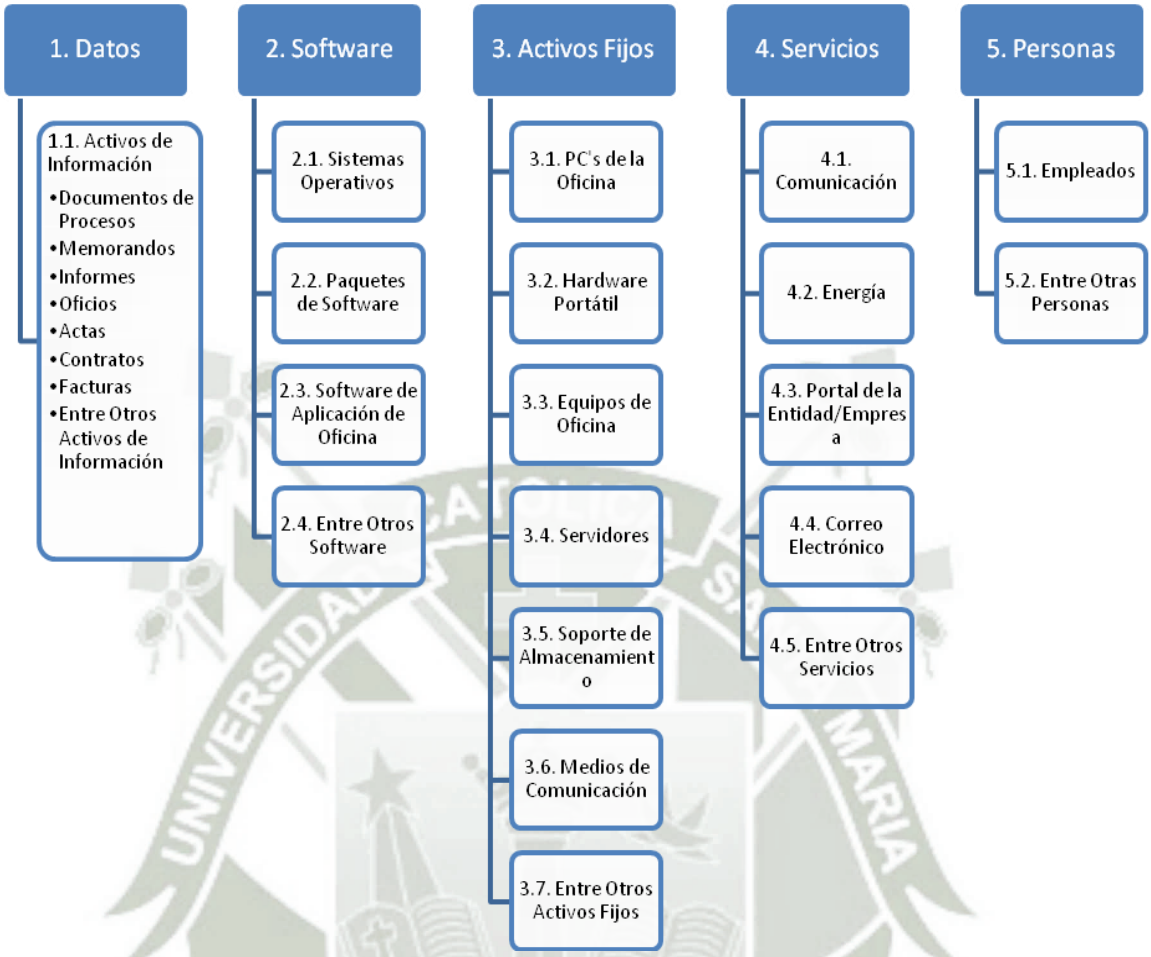


FIGURA 3.2Estructura de Riesgos
Fuente: Elaboración Propia

b) Revisar la Estructura de Desglose de Riesgos

- El Jefe de Proyecto revisa la solicitud presentada por el comité de seguridad, respecto a los puntos a modificar o agregar respecto a la estructura de desglose de trabajo.

- El Jefe del Proyecto en caso de realizar el cambio, presenta los puntos a modificar o agregar, envía un correo electrónico y solicita que revise, especialmente, aquellos puntos presentados en la solicitud.
- Los Miembros del Comité de Seguridad revisa el cambio a la Estructura de Desglose de Trabajo, y si hubiera algo adicional que modificar, explicar de qué trata y deben llegar a un consenso para la aprobación de la Estructura de Desglose de Trabajo.

c) Aprobar la Estructura de Desglose de Riesgos

- Los Miembros del Comité de Seguridad envía un correo electrónico y entrega la Estructura de Desglose de Trabajo al jefe del proyecto, indicando su aprobación del contenido.
- El Jefe del Proyecto y el Comité de Seguridad firman la aprobación de la Estructura del Desglose de Trabajo, caso contrario de no aprobar, indicar el motivo de su rechazo al documento.

PROYECTO SGSI **Solicitud de Cambio de Estructura de Desglose de Riesgo**		
SGSI 004	**Versión de la Plantilla : 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud:dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante _____		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		
IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS		

Firma			
2.- APROBACION DEL COMITÉ			
( ) Aprobado ( ) Desaprobado			
(En caso de rechazo, indicar el motivo)			
ROL	**NOMBRE**	**FECHA**	**FIRMA**

Formato 3.7 Solicitud de Cambio de Estructura de Desglose de Riesgos
Fuente: Elaboración Propia

3.3.5 Identificación de Activos

La Institución del Estado debe tener identificado los activos de información, con el objetivo primordial de identificar los posibles riesgos tal como amenazas y vulnerabilidades que puedan afectar a los activos de información.

a) Elaborar Enunciado para la Identificación de Activos

- El Jefe del Proyecto y los Miembros del Comité, elabora un listado de diagnóstico de los activos para evaluar la seguridad en los activos de información dentro de la empresa. Ver formato 3.8.
- El Jefe del Proyecto y los Miembros del Comité de Seguridad elabora la clasificación de activos por categoría. Ver formato 3.9.

- Los Miembros de Comité de Seguridad deben elaborar formatos para etiquetar a los activos de la información de la entidad y presentar un formato respecto de las características de la seguridad de información, envía un correo electrónico al jefe de proyecto para su revisión. (Ver formato 3.10Categoría de Datos, Ver formato 3.11 Categoría de Software, formato 3.12 Categoría de Activos Físicos, Ver formato 3.13 Categoría de Servicios, Ver formato 3.14 Categoría de Personas, Ver formato 3.15 Informe de Activos de Información, Ver formato 3.17 Características de la seguridad de Información).

b) Revisar el Enunciado para la Identificación de Activos

- El Jefe del Proyecto revisa los formatos presentados por el Comité de Seguridad si hubiera algo adicional que modificar o agregar, envía una solicitud de cambio.
- Los Miembros del Comité de Seguridad revisa y deben llegar a un consenso para decidir si contemplarlo o no el cambio solicitado.
- Los Miembros del Comité de Seguridad envía un correo electrónico al jefe del proyecto para la revisión.

c) Aprobar el Enunciado para la Identificación de Activos

- El Jefe del proyecto revisa y envía un correo electrónico al comité de seguridad, indicando la aprobación de los formatos y solicita que lo firmen en señal de aprobación del contenido de dicho documento.
- El Jefe del Proyecto y los Miembros del Comité de Seguridad firman la aprobación de la Identificación de Activos, caso contrario de no aprobar, indicar el motivo de su rechazo.

d) Procedimiento de Actualización de la Identificación de Activos

- En caso de haber un cambio en la identificación de activos por categorías y etiquetado llenar una solicitud de cambio.
- El Jefe del Proyecto realiza los cambios realizados e informa a los miembros de comité de seguridad los posibles cambios respectivamente.
- Los Miembros del Comité revisan los posibles cambios, y si hubiera algo adicional que modificar, explicar en una reunión, para luego llegar a un consenso para contemplar el cambio.
- Los Miembros del Comité envía un correo electrónico al jefe del proyecto indicando la aprobación del cambio, por consiguiente, el jefe del proyecto y los miembros del comité de seguridad firman el cambio en la identificación de activos de información.

PROYECTO SGSI Listado de Diagnostico				
SGSI 005	**Versión de la Plantilla: 1.0.0**	**Fecha:**		
Ítems		**Si**	**No**	**No aplicable**
Existen procedimientos definidos y aprobados relativos para la seguridad de información.				
Hay procedimientos para la seguridad de información dentro de la empresa.				
Hay roles y responsabilidades definidos para a los empleados implicados en la seguridad de la información.				
Hay inventarios de los activos de información				
Los inventarios cuentan con una adecuada documentación dentro de la institución.				
Se dispone de una clasificación respecto a los activos de la información.				
Existen procedimientos de etiquetado de los activos de información dentro de la empresa				
Se tienen definidas responsabilidades y roles al personal				
Se tiene en cuenta una adecuada política para la selección de personal				
Hay confidencialidad y responsabilidades en los contratos con los empleados de la institución.				

Se imparte la formación y concientización adecuada respecto a la seguridad de información en la empresa			
Hay reportes de incidentes de forma detallada de los activos de información			
Existen controles para protegerse frente al acceso de personal no autorizado a las instalaciones y equipos dentro de la empresa			
En las áreas o oficinas existen controles adicionales al personal propio y ajeno			
La ubicación de los equipos está adecuadamente en instalaciones seguras para minimizar accesos innecesarios			
Existen medidas frente a fallos en la alimentación eléctrica			
Existe medidas de seguridad en el cableado frente a daños e intercepciones que afecten a los activos			
Existe la disponibilidad, confidencialidad e integridad de todos los activos			
Existe algún tipo de seguridad en los equipos ubicados en el exterior de la empresa.			
Existen procedimientos identificados respecto a la seguridad y correctamente documentados			
Hay procedimientos para controlar cambios en los equipos en las áreas u oficinas.			
Existen medidas establecidas para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad			
Existe algún método para reducir el mal uso o deliberado en los activos			
Existen controles contra software maligno o virus			
Realizan copias de seguridad de la información esencial para la empresa			
Existe seguridad en la documentación			
Existen medidas de seguridad en los correos electrónicos de la empresa			
Se han establecido e implantado medidas correctivas y preventivas a los activos de información			
Existe una política de control de accesos los pc’s de las oficinas			
Existe el uso de contraseñas para los empleados y usuarios			
Se protege el acceso a los equipos no utilizados por cierto tiempo			
Existe un control en la conexión de las redes dentro de la institución			
Existe seguridad en las aplicaciones de software			
Existen seguridad en los archivos más importantes para la empresa			
Existe seguridad en los procesos de desarrollo y soporte			
Existen procesos para la gestión de la continuidad del negocio de la empresa del estado.			

Formato 3.8 Listado de diagnostico
Fuente: Elaboración Propia

PROYECTO SGSI Clasificación de Activos		
SGSI 005_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**
1. CATEGORIA DE DATOS		
Documentación de la Empresa		
1.1. Activos de Información	Activos de Información: Documentos de Procesos, Memorandos, Informes, Oficios, Actas, Contratos, Facturas y Otros Activos de Información.	
2. CATEGORIA DE SOFTWARE		
2.1. Sistemas Operativos		
Especificación	Comprende todos los programas de una computadora donde constituyen una base operativa donde se ejecutan todos los programas (servicios o aplicaciones). Activos: Windows 7, Linux Fedora, Windows 8	
2.2. Paquetes de Software		
Especificación	Los paquetes de software es un programa comercializado como soporte, versión y mantenimiento. Presta servicios a los usuarios. Activos: Antivirus Symantec, Microsoft Visio, Microsoft Visual Studio, Oracle, Microsoft Project, Adobe Ilustrator	
2.3. Software de Aplicación de Oficina		
Especificación	Es la información y servicios de TI que son compartidos dentro de la institución pero privados, que utilizan los servicios informáticos (Internet, etc.). Activos: Aplicación Oracle para acceso a la información de usuarios	
3. CATEGORIA DE ACTIVOS FISICOS		
3.1. PCs de la Oficina		
Especificación	Hardware de TI perteneciente ala institución o es utilizado por personal de la misma. Activos: Estaciones de Trabajo	
3.2. Hardware Portátil		
Especificación	Hardware informático diseñado para poder ser transportado manualmente con el fin de utilizarlo en cualquier momento o lugares diferentes en la institución. Activos: Portátil	
3.3. Equipos de Oficina		
Especificación	Hardware para la recepción, la transmisión o la emisión de datos Activos: Impresora, Copiadoras, Teléfonos, Fax.	
3.4. Servidores		

Especificación	Comprende a una computadora o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos. Activos: Disco Duro Extraíble, Memoria Extraíble. USB.
3.5. Soporte de Almacenamiento	
Especificación	Comprende a una computadora o a una red informática para el almacenamiento de datos. Susceptible de almacenar un gran volumen de datos. Activos: Disco Duro Extraíble, Memoria Extraíble. USB
3.6. Medios de Comunicación	
Especificación	Contiene a los medios o soportes de comunicación y telecomunicación para la transportación de datos. Activos: Cableado Estructurado, Tecnología Ethernet, Cables, *Switch, Routers, Modem*
4. CATEGORIA DE SERVICIOS	
4.1. Comunicación	
Especificación	Comprende a los servicios y equipos de telecomunicaciones que dan servicio a la empresa. Activo: Línea telefônica, Central Telefônica
4.2. Energía	
Especificación	Comprendes a los servicios y medios (fuentes de energía y cableado) necesarios para la alimentación eléctrica al hardware y a los periféricos de la empresa
4.3. Portal de la Entidad/Empresa	
Especificación	El portal de la empresa será utilizada por el usuario cuando busque una información de la institución del Estado, para brindan recursos y servicios. Activo: Portal de Información (Pagina Web de la Empresa/Entidad).
4.4. Correo Electrónico	
Especificación	Permite a los usuarios el ingreso, hacer la consulta y la transmisión de documentos o mensajes electrónicos, a partir de computadoras conectadas en red. Activos: Correo Electrónico Interno, Correo Electrónico Vía Web.
5. CATEGORIA DE PERSONAS	
5.1. Empleados	
Especificación	Es el personal que manipula elementos delicados de la empresa/entidad del Estado y tiene la responsabilidad de cuidar los activos de información. Activos: Gerencia de la Empresa/Entidad, Área de Informática, Área de Recursos Humanos.

Formato 3.9 Clasificación de activos
Fuente: Álvarez y García 2007

PROYECTO SGSI 1. Etiquetado de la Categoría de Datos		
SGSI 005_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Código del Activo	Identificador del activo. Número consecutivo para ordenar los activos.	
Nombre del Activo	Es el nombre por el cual se conoce a cada activo.	
Descripción del Activo	Es una breve descripción del activo o bien puede ser el nombre con el cual es conocido dentro de la empresa.	
Tipo de Información	**Tangible:** Todo aquel activo que se encuentre físicamente disponible y sea palpable, como puede ser: guías y reglamentos, contratos, expedientes, notificaciones, papeles de trabajo, manuales de usuario, equipos de cómputo, servidores, discos ópticos, dispositivos magnéticos, etc. **Intangible:** Todo aquel activo que no sea posible accederlo físicamente, como puede ser: bases de datos, software de aplicación, software de sistema, correo electrónico	
Entrada/Salida/Otro	**Entrada:** por cada uno de los procesos identificados, es necesario listar todo aquel requerimiento de entrada necesario a través de la ejecución del proceso para poder llevarlo a cabo (las entradas pueden ser solicitudes, correos electrónicos, etc., en general cualquier información que active la ejecución del proceso). **Salida:** hace referencia a todo aquel resultado obtenido de haber ejecutado el proceso en cuestión. Es posible que se tenga más de una salida por lo que se sugiere se identifiquen dichas salidas en un diagrama de flujo del proceso. **Otro:** Activos de Información que intervienen dentro del flujo del proceso como pueden ser: bases de datos, software de aplicación, equipos de cómputo, manuales, procesos, etc.	
Responsable del activo	En este campo se indica el nombre de la persona o grupo que administra el activo al que se hace referencia.	
Área y Cargo del responsable del activo	En este campo se indica el nombre del área y el cargo que el empleador.	
Lugar de procedencia	En este campo se indica el nombre del área o edificio que provenga la información.	
Medio o formato de almacenamiento	En este campo se indica el tipo de formato.	
Observaciones	Éste es un espacio en donde se puede agregar información adicional sobre el activo y cualquier información que se considera de importancia que por motivos de seguridad se deba conocer.	

Formato 3.10 Etiquetado de la Categoría de Datos
Fuente: Elaboración Propia

PROYECTO SGSI 2. Etiquetado de la Categoría de Software		
SGSI_005_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Código de Activo	Identificador del activo. Número consecutivo para ordenar los activos.	
Nombre del Activo	Es el nombre por el cual se conoce al activo	
Descripción y Subcategoría del Activo	Es una breve descripción del activo o bien puede ser el nombre con el cual es conocido dentro de la empresa.	

Responsable del activo	En este campo se indica el nombre de la persona o grupo que administra el activo al que se hace referencia.
Área y Cargo del responsable del activo	En este campo se indica el nombre el área y el cargo que ocupa el empleador.
Clasificación del Software	En este campo indica la información para la instalación de un software para el procesador (Informe del procesador, información de memoria, unidades de almacenamiento)
Área y Responsable del Mantenimiento	En este campo se indica el nombre del área y del responsable que se encargara del mantenimiento del activo.
Observaciones	Éste es un espacio en donde se puede agregar información adicional sobre el activo y cualquier información que se considera de importancia que por motivos de seguridad se deba conocer.

Formato 3.11 Etiquetado de la Categoría de Software
Fuente: Elaboración Propia

PROYECTO SGSI **3. Etiquetado de la Categoría de Activos Físicos**		
SGSI 005_4	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Código del Activo	Identificador del activo. Número consecutivo para ordenar los activos.	
Nombre del Activo	Es el nombre por el cual se conoce a cada activo listado.	
Descripción del Activo	Es una breve descripción del activo o bien puede ser el nombre con el cual es conocido dentro de la empresa.	
Localización (Edifico, Área, Departamento)	En este campo se indica el lugar donde se encuentra el activo.	
Responsable del activo	En este campo se indica el nombre de la persona o grupo que administra el activo al que se hace referencia.	
Área y Cargo del responsable del activo	En este campo se indica el nombre del área y el cargo que ocupa el empleador.	
Clasificación de hardware	En este campo indica los dispositivos del hardware como CPU, almacenamiento (memoria RAM), periféricos de entrada y salida.	
Dirección IP de la Maquina	En este campo indica la dirección IP (equipos computacionales, Hardware portátil y servidores).	
Horas de Funcionamiento	En este campo indica cuantas horas está en funcionamiento los activos físicos.	
Equipos de Oficina	En este campo indica los equipos de oficina(impresora, scanner; y con sus respectiva información)	
Entrada/Salida de Activos	En este campo indica que activos físicos entran y salen del área.	
Área y Responsable del Mantenimiento del activo	En este campo el nombre del área y el responsable del mantenimiento	
Tipo de conexión (área o equipos)	En este campo el nombre que tipo de conexión se realiza en cada área así como los activos físicos, servidores)	
Tipo de Acceso	En este campo el nombre que tipo de acceso tienen los empleados al uso de los servidores.	
Medios de Comunicación	En este campo el nombre los medios o soportes de comunicación y telecomunicación para la transportación de datos.	

Observaciones	Éste es un espacio en donde se puede agregar información adicional sobre el activo y cualquier información que se considera de importancia que por motivos de seguridad se deba conocer.

Formato 3.12 Etiquetado de la Categoría de Activos Físicos
Fuente: Elaboración Propia

PROYECTO SGSI **4. Etiquetado de la Categoría de Servicios**		
SGSI 005_005	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Código del Activo	Identificador del activo. Número consecutivo para ordenar los servicios	
Nombre de Activo	En este campo se indica el nombre del activo.	
Descripción del Activo	Es una breve descripción del activo (descripción del servicio).	
Responsable del Servicio	En este campo indica el nombre del responsable del servicio que dan a la empresa o que servicio presta la empresa.	
Acceso a los Servicios	En este campo indica usuarios para la transmisión de documentos o mensajes electrónicos, a partir de computadoras conectadas en red a los empleados de la empresa.	
Responsable del activo	En este campo se indica el nombre del activo que está a cargo el empleador en el área de la empresa	
Responsable del Mantenimiento	En este campo indica el nombre del responsable del mantenimiento que dan al servicio.	
Observaciones	Éste es un espacio en donde se puede agregar información adicional sobre el activo y cualquier información que se considera de importancia que por motivos de seguridad se deba conocer.	

Formato 3.13 Etiquetado de la Categoría de Servicios
Fuente: Elaboración Propia

PROYECTO SGSI **5. Etiquetado de la Categoría de Personas**		
SGSI 005__6	**Versión de la Plantilla:1.0.0**	**Fecha:**
Código del Activo	Identificador del activo. Número consecutivo para ordenar los empleados.	
Nombre del Empleador	En este campo se indica el nombre de la persona o grupo que administra el activo al que se hace referencia.	
Área del Empleador	En este campo se indica el nombre del área o edificio que ocupa el empleador.	
Función del Empleador	En este campo se indica el nombre función específica del empleador en el área de la empresa.	
Fecha de ingreso/salida	En este campo se indica la fecha de ingreso y la fecha de salida.	
Nombre del activo al cargo del empleador	En este campo se indica el nombre del activo que está a cargo el empleador en el área de la empresa	
Horas de Trabajo	En este campo indica las horas de trabajo que realiza en el área.	
Acuerdos de confidencialidad	En este campo indica si el empleado tiene un acuerdo de confidencialidad con la empresa o entidad del Estado.	
Accesos Permitidos	En este campo indica que tipo de acceso tiene el empleador a su área de trabajo.	

Observaciones	Éste es un espacio en donde se puede agregar información adicional sobre el activo y cualquier información que se considera de importancia que por motivos de seguridad se deba conocer.

Formato 3.14 Etiquetado de la Categoría de Personas
Fuente: Elaboración Propia

PROYECTO SGSI **Informe de Control de Activos de Información** **Activos de Información**		
SGSI 005_7	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Código del Activos	Identificador del activo. Número consecutivo para ordenar los activos.	
Nombre del Activo	Es el nombre por el cual se conoce a cada activo	
Descripción del Activo	Es una breve descripción del activo o bien puede ser el nombre con el cual es conocido dentro de la empresa.	
Responsable del activo	En este campo se indica el nombre de la persona o grupo que administra el activo al que se hace referencia.	
Tipo	**Información:** contiene archivos, contratos y acuerdos, documentación del sistema, información sobre investigaciones, manuales de usuario, procedimientos de soporte, planes para la continuidad del negocio, acuerdos sobre confidencialidad, pruebas de auditoría. **Software:** indica el software de aplicación, software del sistema, herramientas de desarrollo. **Hardware:** indica los equipos de computación, equipos de comunicaciones, medios removibles y otros equipos. **Servicios:** indica los servicios de computación y comunicaciones.	
Acceso	**Usuarios:** indica el acceso a las personas que utilizan la información para propósitos propios de su labor, adecuados y que tendrán el derecho manifiesto de uso dentro del inventario y la clasificación de activos de información a llevarse a cabo. **Derechos de acceso:** en este campo deben ser ejecutado de manera obligatoria, que empleados o usuarios pueden acceder a los activos de la institución.	
Ubicación	**Físico:** Para este campo se debe escribir el nombre del sitio físico en donde se encuentra el activo, esto puede ser el nombre de una oficina, el nombre de un archivo, caja fuerte, escritorio, A-Z, etc. **Soporte Electrónico:** Para este campo se debe escribir el recurso en donde se encuentra el activo disponible o almacenado, esto puede ser el nombre de un servidor de archivos, base de datos, sistema de gestión de documentos, medio, cinta, etc.	
Atributos	¿Un activo de información para uso de terceros o de clientes que debe protegerse?	
	¿El activo de información que debe ser restringido a un número limitado de empleados?	
	El activo de información que debe ser restringido a personas externas.	
	El activo de información que puede ser alterado o comprometido para fraudes o corrupción.	
	El activo de información se encuentra en un estado crítico para las operaciones internas.	

	El activo de información se encuentra en un estado crítico para el servicio hacia terceros.
Observaciones	Éste es un espacio en donde se puede agregar información adicional sobre el activo y cualquier información que se considera de importancia que por motivos de seguridad se deba conocer.

Formato 3.15 Informe de Control de Activos de Información Activos de Información
Fuente: Elaboración Propia

PROYECTO SGSI Solicitud de Cambio de Activos		
SGSI 005_8	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud: dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante _____		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		
IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS		
_____ Firma		
2.- APROBACION DEL COMITÉ		
( ) Aprobado	( ) Desaprobado	
(En caso de rechazo, indicar el motivo)		

ROL	NOMBRE	FECHA	FIRMA

Formato 3.16Solicitud de Cambio de Activos
Fuente: Elaboración Propia

PROYECTO SGSI Características de la Seguridad de Información			
SGSI 005_9	**Versión de la Plantilla: 1.0.0**		**Fecha:**
	N°	**Clase**	**Descripción**
Confidencialidad	1	Publica	Puede ser revelado y proporcionado a terceras partes

	2	Uso Interno	Puede solo ser revelada y proporcionado dentro de la empresa
	3	Secreto	Puede ser solo revelado y proporcionado a partes específicas y áreas
	4	Alta Confidencialidad	Puede ser solo revelado y proporcionado a partes específicas, dentro de la entidad
Integridad	1	No necesaria	Usado solo para consulta.
	2	Necesaria	En caso de haber un cambio en el contenido, habría problemas, pero no afectan a las operaciones que se realizan dentro de la institución.
	3	Importante	En caso de haber una pérdida, habría una consecuencia fatal en las operaciones en la institución.
Disponibilidad	1	Bajo	En caso, si la información no llega a estar disponible, no existirían efectos en las operaciones en la institución.
	2	Mediano	En caso si la información no llega a estar disponible, existiría algún efecto en las operaciones. Sin embargo las operaciones o los procesos podrían estar retrasados hasta que los activos de información estén disponibles para la institución.
	3	Alto	En caso, si la información no estuviera disponible, cuando sea solicitada en algún momento, hubiera una consecuencia fatal en las operaciones o procesos en la empresa.

Formato 3.17 Características de la Seguridad de Información
Fuente: Murillo (2012)

3.3.6 Plan de Gestión de Tiempo

El Plan de Gestión de Tiempo tiene por objetivo garantizar que los procesos estén definidos para la adecuada implementación del proyecto. El objetivo del plan de gestión de tiempo es permitir saber quién o quiénes son responsables de cada actividad o tarea del proyecto.

a) Elaborar el Enunciado de la Lista de Actividades

- El Jefe de Proyecto y los Miembros del Comité, elabora la lista de actividades en base a la Estructura de Desglose de Trabajo y estiman la duración a cada actividad dentro del proyecto.

- Si algún Miembro del Comité de Seguridad, hace un cambio a la lista de actividades, solicita una reunión con todos los miembros del comité, para explicar y llegar a un consenso para contemplar el cambio, y envía un correo electrónico una solicitud al jefe del proyecto.

b) Revisar el Enunciado de la Lista de Actividades

- El Jefe del Proyecto revisa la solicitud presentada por el comité de seguridad, realiza los cambios en los puntos a modificar o agregar en la lista de actividades, y envía un correo electrónico a los miembros del comité de seguridad.
- El Comité de Seguridad revisa la lista de actividades; y si hubiera algo adicional, que modificar explicar de qué trata y deben llegar a un consenso, para la aprobación de la lista de actividades del proyecto.

c) Aprobar el Enunciado de la Lista de Actividades

- Los Miembros del Comité de Seguridad envía un correo electrónico al jefe del proyecto, indicando la aprobación de la lista de actividades.
- El Jefe del Proyecto y el Comité de Seguridad firman la aprobación de la lista de actividades, caso contrario de no aprobar, indicar el motivo de su rechazo al documento.

d) Elaborar el Enunciado del Diagrama del Tiempo del Proyecto

- El Jefe de Proyecto elabora el diagrama del proyecto en base a la lista de actividades, ingresa al software de gestión de proyectos (MS Project), para la realización del diagrama del cronograma del proyecto y estimaciones de la duración de las actividades, envía un correo electrónico al comité para su revisión.

- Si algún miembro del comité tiene algunas observaciones respecto al cronograma, presenta una solicitud de cambio y envía un correo electrónico al jefe del proyecto para su revisión del diagrama del tiemplo del proyecto.

e) Revisar el Enunciado del Diagrama del Tiempo del Proyecto

- El Jefe del Proyecto revisa la solicitud presentada por el comité de seguridad, y realiza los puntos a modificar o agregar, y envía un correo electrónico al comité de seguridad para su revisión.
- El Comité de Seguridad revisa el cambio al diagrama del tiempo, y si hubiera algo adicional que modificar, explicar de qué trata y deben llegar a un consenso, para la aprobación del diagrama del tiempo.

f) Aprobar el Enunciado del Diagrama del Tiempo del Proyecto

- El Jefe de Proyecto entrega los puntos a modificar o agregar en el diagrama del tiempo al comité de seguridad, para la aprobación del diagrama, envía un correo electrónico al comité de seguridad, indicando la aprobación de la documentación y solicita que lo firmen en señal de aprobación.
- El Jefe del Proyecto y el Comité de Seguridad firman la aprobación del diagrama del tiempo, caso contrario de no aprobar, se regresa al punto anterior, indicando el motivo de su rechazo al documento.

g) Procedimiento de Actualización del Proceso del Tiempo del Proyecto

- En caso de realizar un cambio en el cronograma, debe llenar una solicitud de cambio, indicando los puntos a modificar o agregar.

- El Jefe de Proyecto revisa y envía un correo electrónico al comité de seguridad para la revisión de los puntos a modifica o agregar, y deben llegar a un conceso para la aprobación.
- Los Miembros del Comité de Seguridad envía un correo electrónico al jefe del proyecto, indicando la aprobación y firman en señal de aprobación del contenido de dicho documento.

PROYECTO SGSI **Solicitud de Cambio de Cambio de Plan de Tiempo**		
SGSI 006	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud: dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		
IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS		
Firma		
2.- APROBACION DEL COMITÉ		
( ) Aprobado	( ) Desaprobado	
(En caso de rechazo, indicar el motivo)		

ROL	NOMBRE	FECHA	FIRMA

Formato 3.18 Solicitud de Cambio de Cambio de Plan de Tiempo
Fuente: Elaboración Propia

3.3.7 Plan de Gestión de Costos

El Plan de Gestión de Costos tiene por objetivo garantizar y determinar los costos en que se incurrirán en el proyecto de la Implementación del Sistema de Gestión de Seguridad de Información a Jefe del Proyecto y los Miembros del Comité. Ver formato 3.19 y 3.20

PROYECTO SGSI Estimación de Costos			
SGSI 007	**Versión de las Plantilla: 1.0.0**		**Fecha:**
Participantes del proyecto	**Cargo**	**Costo Hora S/.**	**Costo de Hora Extras**

Formato 3.19Estimación de Costos
Fuente: Elaboración Propia

PROYECTO SGSI Costo de Recursos Humanos por Actividad				
SGSI 007_1		**Versión de la Plantilla: 1.0.0**		**Fecha:**
Cód.	**Nombre**	**Encargado de Fase**	**Costo Hora (S/.)**	**Días Trabajados (*)**

Nota: No cuenta los días feriados.

Formato 3.20 Costo de Recursos Humanos por Actividad
Fuente: Elaboración Propia

a) Elaborar la Estimación de Costos

- El Jefe de Proyecto y los Miembros del Comité elabora la estimación de costos y costo de recursos humanos por actividad; envía un correo electrónico al área de logística y recursos humanos.

b) Revisarla Estimación de Costos

- Las Áreas de Recursos Humanos y Logística revisa la estimación de costos y costo de recursos humanos por actividad, en caso de haber algunas observaciones, envía

un correo electrónico al jefe de proyecto y al comité de seguridad y presentar una solicitud de cambio.

- El Jefe de Proyecto y los Miembros del Comité de Seguridad, deben llegar a un conceso para la modificación en la estimación de costos y costo de recursos por actividad, según lo indicado en la solicitud por las áreas de logística y recursos humanos, y envía un correo electrónico a las áreas de logística y recursos humanos.

c) Aprobar la Estimación de Costos

- Las Áreas de Recursos Humanos y Logística revisa; y si hubiera algo adicional que modificar explicar de qué trata y deben llegar a un consenso para la aprobación.
- Las Áreas de Recursos Humanos y Logística envía un correo electrónico al jefe del proyecto y a los miembros del comité, indicando la aprobación y firmar en señal de aprobación del contenido de dicho documento, caso contrario de no aprobar, indicar el motivo de su rechazo al documento.

d) Procedimiento de Actualización de Estimación de Costos

- En caso de haber un cambio en la estimación de costos y costo de recursos por actividad llenar una solicitud de cambio, el jefe del proyecto y los miembros del comité realiza los cambios e informa a las área de recursos humanos y logística
- Las Áreas de Recursos Humanos y Logística revisa los posibles cambios, y si hubiera algo adicional, que modificar explicar de qué trata y deben llegar a un consenso para contemplar el cambio.
- Las Áreas de Recursos Humanos y Logística envía un correo electrónico al jefe del proyecto y a los miembros del proyecto indicando la aprobación del cambio, tanto

como el jefe del proyecto, los miembros del comité, la área de recursos humanos y logística firman el cambio en la estimación de costos.

PROYECTO SGSI **Solicitud de Cambio de Cambio de Plan de Costos**		
SGSI 007_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud: dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante _____		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		
IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS		
_____ Firma		
2.- APROBACION DEL COMITÉ		
( ) Aprobado	( ) Desaprobado	
(En caso de rechazo, indicar el motivo)		

ROL	NOMBRE	FECHA	FIRMA

Formato 3.21 Solicitud de Cambio de Cambio de Plan de Costos
Fuente: Elaboración Propia

3.3.8 Plan de Gestión de las Comunicaciones

El Plan de Gestión de las Comunicaciones tiene por objetivo garantizar que se encuentre definidos los procesos necesarios para asegurar la generación y distribución de la información para llevar a cabo la implementación del Sistema de Gestión de Seguridad de

Información en la empresa. Se debe mostrar los siguientes puntos a seguir en el Plan de Gestión de las Comunicaciones:

a) Flujo de Información del Proyecto

- El Jefe de Proyecto realiza una lista directorio de la empresa o entidades externas, son importantes en el logro de los objetivos del proyecto. Ver formato 3.22

PROYECTO SGSI Medios de Contacto				
SGSI 008	**Versión de la Plantilla:1.0.0**		**Fecha:**	
Código	**Cargo**	**Nombres y Apellidos**	**Correo Electrónico**	**Teléfono**

Formato 3.22 Medios de Contacto
Fuente: Elaboración Propia

Dónde:

Código: En el campo indica el código de cada miembro del proyecto

Cargo: En el campo indica el nombre del cargo de la persona.

Nombres y Apellidos: En el campo indica el nombre y apellidos completos del interesado.

Correo Electrónico: En el campo indica el correo electrónico del interesado.

Teléfono: En el campo indica el teléfono y anexo de la oficina del interesado.

b) Requisitos de la Información del proyecto

El Jefe del Proyecto presenta un formato donde se especifica los requisitos de la información del proyecto. Ver formato 3.23

PROYECTO SGSI Requisitos de Información			
SGSI 008_1	**Versión de la Plantilla: 1.0.0**		**Fecha:**
Nº	**Entregable de Información**	**Código**	**Tiempo Máximo de Respuesta**
1	Informe de rendimiento de costos	IRC	---
2	Informe de rendimiento de tiempo	IRT	---
3	Actas de reuniones	AC	---
4	Requerimientos de información de los activos	RFI	3d

5	Solicitudes de cambios	SC	5d
6	Cambios aprobados	CA	1d
7	Informes del Entregables	IME	---
8	Informe de Cierre de Proyecto	ICP	---
9	Informe de Actividades	IA	2d

Formato 3.23 Requisitos de Información
Fuente: Elaboración Propia

Dónde:

Entregable de Información: Código asignado al entregable

Código: Nombre del entregable mediante el cual se brindará información

Tiempo Máximo de Respuesta: Tiempo máximo de respuesta para la respuesta al documento enviado.

c) Información que será comunicada

El informe de comunicación detalla la información a comunicar dentro de la empresa y se describen en el siguiente formato 3.24

PROYECTO SGSI Informe de Comunicación				
SGSI 008_2		**Versión de la Plantilla: 1.0.0**	**Fecha:**	
N	**Código**	**Entregable de la Información**	**Detalle de Información a comunicar**	**Uso**
1	IRC	Informe de Rendimiento de Costos	Especificara el rendimiento de costos a todos los interesados del proyecto.	Interno
2	IRT	Informe de Rendimiento de tiempo	Especificara el rendimiento de tiempo a todos los interesados del proyecto.	Interno
3	AC	Actas de reuniones	Nombre de la reunión, fecha, hora de inicio/ término, participantes, agenda, acuerdos, pendientes conclusiones y sugerencias	Interno
4	RFI	Requerimientos de información	En los formatos correspondientes, enviados por el interesado que solicita la información específica.	Restringido
5	SC	Solicitudes de cambios	En el formato correspondiente se informará de cualquier cambio solicitado al interesado que Corresponda.	Restringido
6	CA	Cambios aprobados	Se informará en los formatos correspondientes a los interesados correspondientes, sobre los cambios aprobados en el proyecto.	Uso interno
7	IME	Informes de los Entregables	Informar a los interesados respecto a los entregables	Restringido

PROYECTO SGSI Informe de Comunicación				
SGSI 008_2		**Versión de la Plantilla: 1.0.0**		**Fecha:**
N	**Código**	**Entregable de la Información**	**Detalle de Información a comunicar**	**Uso**
8	ICP	Informe de Cierre de Proyecto	Informe final con los datos finales del Proyecto	Restringido
9	IA	Informe de Actividades	Informa a los interesados el avance de las actividades	Restringido

Formato 3.24 Informe de Comunicación
Fuente: Elaboración Propia

Dónde:

Código: Código asignado al entregable.

Entregable de Información: Nombre del entregable mediante el cual se brindará información.

Detalle de Información a comunicar: Especificación resumida de lo que debe contener el entregable de información.

Uso: Tipo de uso que se le debe dar al entregable. Estos pueden ser: uso Interno (dentro de proyecto), uso externo (fuera de proyecto), restringido (solo personas autorizadas), público.

d) Requisitos de Información de los Interesados en el Proyecto

Se mantendrán informado a los interesados principales dentro de la empresa.

PROYECTO SGSI Requisitos de Información										
SGSI 008_3		**Versión de la Plantilla 1.0.0**						**Fecha:**		
	Interesados Principales	**IPC**	**IPT**	**AC**	**RFI**	**SC**	**CA**	**IMAP**	**ICP**	**IA**
1	**Gerente de la Empresa/Entidad del Estado**	√	√	√	√	√	√	√	√	
2	**Área de Tecnologías de Información**	√	√	√	√	√	√	√	√	√
3	**Subgerencia de la Empresa del Estado**		√				√			
4	**Área de Recursos Humanos**				√					√
5	**Área de Logística**				√					√

6	**Jefe Proyecto**	√	√	√	√	√	√	√	√	√
7	**Equipo Proyecto**	√	√	√	√	√	√	√	√	√

Formato 3.25 Requisitos de Información
Fuente: Elaboración Propia

e) Matriz de Comunicaciones

A continuación se muestra la matriz de comunicaciones a los interesados principales del proyecto:

PROYECTO SGSI Matriz de Comunicación					
SGSI 008_4		**Versión de la Plantilla: 1.0.0.**		**Fecha:**	
N	**Interesados Principales**	**Responsables de Distribuir la información**	**Información que será comunicada (entregables)**	**Método de Comunicación a ser utilizado**	**Frecuencia de Comunicación**
1	**Gerente de la Empresa/Entidad del Estado**	Gerente de la Empresa/Entidad del Estado	**IPC, IPT, AC RFI, SC, CA, IMAP, ICP, CT**	Escrito (electrónico y documento impreso) verbal	Semanal
2	**Área de Tecnologías de Información**	Encargado de la Área de la Empresa/Entidad de Estado	**IPC, IPT, AC, , SC, CA, IMAP, ICP, CT**	Escrito (electrónico y documento impreso) y Verbal	Semanal
3	**Subgerencia de la Empresa/Entidad del Estado**	Sub-Gerente de la Empresa/Entidad	**IPT, CA**	Escrito (electrónico y documento impreso) y Verbal	Mensual
4	**Área de Recursos Humanos**	Jefe Área de Recursos Humanos	**RFI, CT**	Escrito (electrónico y documento impreso) y Verbal	Mensual
5	**Área de Logística**	Jefe de Área de Logística	**RFI, CT**	Escrito (electrónico y documento impreso) y Verbal	Mensual
6	**Jefe Proyecto**	Jefe de Proyecto	**IPC, IPT, AC RFI, SC, CA, IMAP, ICP, CT**	Escrito (electrónico y documento impreso) y Verbal	Diaria

PROYECTO SGSI Matriz de Comunicación					
SGSI 008_4		**Versión de la Plantilla: 1.0.0.**		**Fecha:**	
N	**Interesados Principales**	**Responsables de Distribuir la información**	**Información que será comunicada (entregables)**	**Método de Comunicación a ser utilizado**	**Frecuencia de Comunicación**
7	**Equipo Proyecto**	Comité de Seguridad	**IPC, IPT, AC, RFI, SC, CA, IMAP, ICP, CT,**	Escrito (electrónico y documento impreso) y Verbal	Diaria

Formato 3.26 Matriz de Comunicación
Fuente: Elaboración Propia

f) Procedimiento de Actualización de la Gestión de Comunicaciones

- En caso de haber un cambio en la gestión de comunicaciones llenar una solicitud de cambio. Ver formato 3.27
- El Jefe del Proyecto realiza los cambios e informa a los miembros de comité de seguridad los posibles cambios respectivamente.
- Los Miembros del Comité revisa los posibles cambios, y si hubiera algo adicional, que modificar explicar de qué trata y deben llegar a un consenso para contemplar el cambio.
- Los Miembros del Comité envía un correo electrónico al jefe del proyecto indicando la aprobación del cambio, tanto como el jefe del proyecto y los miembros del comité de seguridad firman el cambio en la gestión de comunicaciones.

PROYECTO SGSI Solicitud de Cambio de Gestión de Comunicaciones		
SGSI 008_5	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud: dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante _____		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		

IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS
Firma
2.- APROBACION DEL COMITÉ
( ) Aprobado ( ) Desaprobado
(En caso de rechazo, indicar el motivo)

ROL	NOMBRE	FECHA	FIRMA

Formato 3.27 Solicitud de Cambio de Gestión de Comunicaciones
Fuente: Elaboración Propia

3.3.9 Plan de Riesgos

El Plan de Gestión de Riesgos es garantizar que los riesgos o amenazas para la empresa del estado sean identificados, analizados, documentados y tratados (evitados, transferidos o mitigados)

a) Elaborar Enunciado para la Identificación de Riesgos

- El Jefe del Proyecto y los Miembros del Comité de Seguridad identifican los riesgos que correspondan a los activos de información de la empresa del estado, todos aquellos que presenten amenazas y vulnerabilidades. Ver formatos 3.29,3.30,3.31,.3.32,3.33)

- Si algún miembro del comité tiene algunas observaciones respecto a la identificación de los riesgos, envía un correo electrónico y enviando una solicitud de cambio.

b) Revisar el Enunciado para la Identificación de Riesgos

- El Jefe del Proyecto revisa la solicitud y realiza los puntos a modificar o agregar, y envía un correo electrónico al comité de seguridad para su revisión.
- Los Miembros del Comité de Seguridad revisa el cambio, y si hubiera algo adicional que modificar explicar de qué trata y deben llegar a un consenso para la aprobación de la identificación de riesgos.

c) Aprobar el Enunciado para la Identificación de Riesgos

- Los Miembros del Comité de Seguridad envía un correo electrónico al jefe del proyecto, indicando la aprobación de la documentación y solicita que lo firmen en señal de aprobación del contenido de dicho documento.
- El Jefe del Proyecto y el Comité de Seguridad firman la aprobación de la Identificación de Riesgos, caso contrario de no aprobar, indicar el motivo de su rechazo al documento.

d) Procedimiento de Actualización de Identificación de los Riesgos

- En caso de realizar un cambio en la identificación de riesgos, presentan una solicitud de cambio indicando los puntos a modifica o agregar.
- El Jefe de Proyecto revisa la solicitud, realiza los puntos a modificar o agregar presentados en la solicitud, indicando las vulnerabilidades y amenazas que puedan afectar a los activos de información.

- El Jefe del Proyecto envía un correo electrónico al comité de seguridad, para su revisión y aprobación.
- Los Miembros del Comité de Seguridad envía un correo electrónico al jefe de proyecto indicando su aprobación y firman la identificación de los riesgos.

PROYECTO SGSI **Solicitud de Cambio de Identificación de Riesgos**		
SGSI 009	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Solicitud de Cambio Numero: 000	Fecha de Solicitud:dd/mm/yyyy	Página: 1/1
1.- DATOS GENERALES (ser llenado por el solicitante del cambio)		
Nombre del Solicitante _____		
INFORMACION DEL CAMBIO REQUERIDO Descripción del Cambio (llenar detalladamente y concisamente)		
IMPACTO DE POSIBLE, SI NO SE REALIZA LOS CAMBIOS		
_____ Firma		
2.- APROBACION DEL COMITÉ		
( ) Aprobado	( ) Desaprobado	
(En caso de rechazo, indicar el motivo)		

ROL	**NOMBRE**	**FECHA**	**FIRMA**

Formato3.28 Solicitud de Cambio de Identificación de Riesgos
Fuente: Elaboración Propia

PROYECTO ABC **Lista de Activos (Vulnerabilidades y Amenazas)**		
SGSI 009_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Activos	**Amenazas**	**Vulnerabilidades**
1. Datos		
1.1 Activos de Datos (Documentación)	Divulgación de la información	Información no protegida
	Pérdida de información	Errores por el personal Información no protegida

	Incumplimiento de normas por el personal a cuanto a la información	Falta de conocimiento del personal
	Incorrecta documentación del sistema	Falta de actualización en la documentación

Formato 3.29 Listado de Vulnerabilidades y Amenazas de Datos
Fuente: Elaboración Propia

Activos	Amenazas	Vulnerabilidades
SGSI 009_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
2. Software		
2.1 Sistemas Operativos	Errores de configuración en los sistemas operativos	Falta de capacitación del administrador para la configuración del sistema Falta de documentación del sistema.
	Virus de Computación	Falta de protección a los equipos
	Falta de capacidad de restauración	Falta de copias de seguridad continua de los sistemas operativos
	Perdida de servicio en el mantenimiento en los sistemas operativos.	Instalación de software no autorizado o falta de actualizaciones
	No cumplimiento en la seguridad en los sistema	Falta de políticas de seguridad
	Cambio no autorizado en la configuración	Falta de control de acceso a los sistemas
	Brechas de seguridad no detectadas en el sistema	Falta de monitoreo del sistema operativo
2.2 Paquetes de Software	Virus de computación	Falta de protección
2.3 Software de Aplicaciones de Oficina (Aplicaciones: Base de Datos, Web, SOA, Entre Otros)	Errores de configuración	Falta de capacitación al administrador en los software
	Escapes de información	Falta de control de acceso a los datos
	Errores o falta de actualización	Falta de procedimientos apropiados para la actualización
	Abuso de privilegios en el uso de software de aplicaciones	Falta de políticas de privilegios a los empleados

Formato 3.30 Listado de Vulnerabilidades y Amenazas de Software
Fuente: Elaboración Propia

Activos	Amenazas	Vulnerabilidades
SGSI 009_4	**Versión de la Plantilla: 1.0.0**	**Fecha:**
3. Activos Fijos		
3.1 PCs de la Oficina	Acceso no autorizado de las Pcs de las áreas de la institución	Falta de protección a los equipos de cada área de la institución
	Cambios en la instalación no autorizada	Falta de control y de revisión las PCs de la institución
	Destrucción de las PCs	Falta de protección por parte del personal
	Degradación del Hardware	Falta de mantenimiento adecuado

	Incumplimiento de las políticas de seguridad	Falta de políticas
	Robo	Falta de protección física para los Pc's de oficina.
3.2 Hardware	Instalación no autorizada o cambios en el hardware	Falta de control de acceso al hardware
	Destrucción del hardware	Falta de protección física
	Robo	Falta de protección física adecuada
	Acceso no autorizado de hardware portátil	Falta de políticas de acceso de hardware
	Daños por agua o fuego	Falta de protección
	Degradación del Hardware	Falta de mantenimiento adecuado.
3.3 Equipos de Oficina	Degradación de los equipos	Falta de mantenimiento
	Robo	Fatal de protección física
3.4 Servidores	Acceso no autorizado a los servidores	Ataque de código malicioso
	Degradación o destrucción	Falta de mantenimiento o protección
	Manipulación de la configuración	Falta de control a los servidores
	Corte repentino del fluido eléctrico o aire acondicionado	Mal funcionamiento del aire acondicionado o fluido eléctrico
	Brechas de seguridad no detectadas en los servidores de la institución	Falta de monitoreo de los servidores
3.5 Soporte de Almacenamiento	Acceso no autorizado a través de la red en los soportes de almacenamiento	La existencia de un código malicioso
	Degradación de los soportes de almacenamiento	Falta de mantenimiento
	Indebida manipulación de los soportes de almacenamiento	Falta de control de los soportes de almacenamiento
	Daños por agua o fuego	Falta de protección a los soportes de almacenamiento
	Robo	Falta de protección a los soportes de almacenamiento.
3.6 Medios de Comunicación	Tener daños en los cables	Falta de protección física
	Errores de configuración de routero switch	Falta de conocimiento en la configuración
	Robo	Falta de protección física

Formato 3.31 Listado de Vulnerabilidades y Amenazas de Activos Físicos
Fuente: Elaboración Propia

Activos	Amenazas	Vulnerabilidades
SGSI 009_5	**Versión de la Plantilla: 1.0.0**	**Fecha:**
4. Servicios		
4.1 Comunicación (Servicio de Comunicaciones)	Degradación o deterioro del servicio y equipos	Falta de mantenimiento adecuado a los equipos o servicio.
	Daños por agua o fuego	Falta de políticas de seguridad
	Falla de servicios de Telefonía	Falta de acuerdos bien definidos con terceras partes
4.2 Energía	Degradación o falla en el servicio	Falta de mantenimiento o falla en el servicio

	Errores de configuración	Falta de conocimiento de los empleados
	Robo	Falta de políticas de acceso
	Falla de servicios de prestación de terceros para la institución.	Falta de acuerdos bien definidos con terceras partes
4.3 Portal de la Entidad/Empresa (Portal de la Empresa)	Modificación o alteración no autorizada del sitio web de la institución.	Falta de procedimiento a los cambios en la página web
	Sitio Web no disponible	Fallas en el acceso al sitio web
4.4 Correo Electrónico (Servicio de Correo Electrónico)	Acceso no autorizado por terceras personas	Falta de políticas acceso
	Fallas de servicios de soporte(servicio de Internet)	Falta de acuerdos de soporte en el servicio de internet
	Robo	Falta control de acceso al correo electrónico
	Password simples	No tener password complejos para el correo electrónico.

Formato 3.32 Listado de Vulnerabilidades y Amenazas de Servicios
Fuente: Elaboración Propia

Activos	**Amenazas**	**Vulnerabilidades**
SGSI 009_6	**Versión de la Plantilla: 1.0.0**	**Fecha:**
5. Personas		
5.1 Empleados (Personal)	Errores del personal y acciones equivocadas	Falta de conocimiento y entrenamiento al personal.
	Divulgación o difusión de información Confidencial de la institución	Falta de acuerdos de confidencialidad

Formato 3.33 Listado de Vulnerabilidades y Amenazas de Personas
Fuente: Elaboración Propia

3.3.10 Acciones de Mitigación de Riesgos

a) Enunciado del Proceso de Mitigación de Riesgos

- El Jefe del Proyecto y los Miembros del Comité de seguridad elabora medidas para mitigar los posibles riesgos que puedan afectar a la empresa del Estado (Ver formatos 3.34, 3.35, 3.36, 3.37, 3.38).

b) Proceso de Actualización de Mitigación de Riesgos

- En caso de realizar un cambio en mitigación de riesgos, se debe llenar una solicitud de cambio, indicando los puntos a modificar o agregar.
- El Jefe del Proyecto revisa la solicitud y realiza los puntos a modificar o agregar, envía un correo electrónico al comité de seguridad para su revisión.

- Los Miembros del Comité de Seguridad revisa y si hubiera algo adicional que modificar explicar de qué trata y deben llegar a un consenso para la aprobación y firma en señal de acuerdo.

PROYECTO SGSI Medidas Preventivas y Correctivas		
SGSI 010	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Riesgos	**Medidas Preventivas**	**Medidas Correctivas**
1. Datos		
1.1 Activos de Información (Documentación: Documentos de Procesos, Memorandos, Informes, Oficios, Actas, Contratos, Facturas, Entre Otros)	-Tener copias de seguridad de los archivos -Determinar procedimientos de seguridad que ayuden a establecer acciones en caso de pérdidas de información. -Tener planes de contingencia para salvaguardar a los activos de información evitando daños o pérdidas de la misma.	-Hacer un seguimiento a los procedimientos de seguridad. -Tener una copia de restauración en caso de haber una pérdida de información.

Formato 3.34 Medidas Preventivas y Correctivas de Datos
Fuente: Elaboración Propia

Riesgos	Medidas Preventivas	Medidas Correctivas
SGSI 010_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**
2. Software		
2.1 Sistemas Operativos 2.2 Paquete de Software 2.3 Software de Aplicación de Oficina (Software)	-Realizar periódicamente las actualizaciones o cuando sea requerido por el encargado. -Disponer de Software de calidad y debidamente revisado. -Establecer una política de contraseñas para acceder a los diferentes equipos de la empresa	Tener una copia o actualización del software en caso ser afectado por código malicioso. Tener personal adecuado para el mantenimiento del software. Hacer revisiones periódicamente a los sistemas.

Formato 3.35 Medidas Preventivas y Correctivas de Software
Fuente: Elaboración Propia

Riesgos	Medidas Preventivas	Medidas Correctivas
SGSI 010_2	**Versión de la Plantilla: 1.0.0**	**Fecha:**
3. Activos Fijos		
3.1 PC's de la Oficina 3.2 Hardware Portátil 3.3 Equipo de Oficina 3.4 Servidores (Activos)	- Tener equipos nuevos en caso de pérdida o degradación. -Disponer un completo inventario de todos los activos de la institución. -Tener una alarma conectada cuando no hay personal dentro de las instalaciones de la institución.	-Tener el personal para el mantenimiento y protección de los activos.

3.1 PC's de la Oficina 3.2 Hardware Portátil 3.3 Equipo de Oficina 3.4 Servidores (Hardware)	-La instalación del servidor, donde se almacene toda la información generada dentro de la institución, tener un acceso adecuado, y seguro, a la misma cuando sea necesario. -Prevenir posibles fallos de Hardware. -Tener dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para evitar posibles fallos de los equipos debidos a cortes de energía. -Tener un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	-Tener técnico que asegure una rápida reparación y puesta en marcha de los equipos cuando se produzcan fallas técnicas. **Riesgos asumibles en la institución:** -Fallo en alguna estación PC o portátil durante un periodo inferior a 24 horas.
3.5 Soporte de Almacenamiento (Copias de Seguridad)	-Realizar periódicamente de copias de seguridad de los datos, en especial de los datos críticos, generados en disco duro, USB, etc. -Tener repuestos para los soportes de almacenamiento en caso de degradación o robo garantizar la disponibilidad de los datos ante cualquier contratiempo que puedan afectar a la institución.	-Tener de copias de seguridad en el caso de haberse producido una pérdida de información.
3.6 Medios de Comunicación (Red)	- Tener un diseño de la red interna en la institución que garantice las comunicaciones internas y que sea de carácter confidencial. - Tener correctamente instalados los medios de comunicación. -Tener una política de seguridad para el acceso a la red mediante el empleo de contraseñas. -Tener una adecuada instalación y configuración de un *Router*. -Establecer una correcta configuración de seguridad para la red inalámbrica que evite accesos indeseados a personas no autorizadas.	-Disponer de un correcto servicio de mantenimiento por parte de la empresa área suministradora de internet. -Disponer de una adecuada instalación de los medios de comunicación. **Riesgos asumibles en la institución:** - Si hay un fallo en los sistemas de comunicación de red durante un periodo no superior a 24 horas.

Formato 3.36 Medidas Preventivas y Correctivas de Activos Fijos
Fuente: Elaboración Propia

Riesgos	Medidas Preventivas	Medidas Correctivas
SGSI 010_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
4. Servicios		
4.1 Comunicación 4.2 Energía 4.3 Portal de la Entidad/Empresa 4.4 Correo Electrónico (Desastres Naturales)	Tener una instalación de dispositivos de protección de líneas eléctricas contra sobrecargas. -Tener una instalación de dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para garantizar el suministro eléctrico en caso de caída del sistema eléctrico que pueda afectar a la institución. -Realizar periódicamente de copias de seguridad de la información cuando se envía una información usando el correo electrónico.	-En caso de desastres naturales, establecer medidas preventivas, realizar copias de la información en caso de haber una alteración en la información.

4.1 Comunicación 4.2 Energía 4.3 Portal de la Entidad/Empresa 4.4 Correo Electrónico (Problemas Estructurales)	- Hacer una revisión periódica de la instalación eléctrica. -Tener instalación de dispositivos automáticos de extinción de incendios en los equipos de las oficinas de la institución. - Tener una adecuada distribución de extintores en toda la institución o áreas, en especial cerca de elementos informáticos críticos. -Contratación de dos líneas exteriores con suministradores de Internet para garantizar siempre una conexión mínima a la red.	-Tener medidas preventivas en caso que pueda ocurrir una falla en el portal de la institución.. **Riesgos asumibles en la institución:** -Pérdida de las comunicaciones o servicios durante un periodo inferior a 24 horas.

Formato 3.37 Medidas Preventivas y Correctivas de Servicios
Fuente: Elaboración Propia

Riesgos	**Medidas Preventivas**	**Medidas Correctivas**
SGSI_010_4	**Versión de la Plantilla: 1.0.0**	**Fecha:**
5. Personas		
5.1 Empleados (Personal)	-Hacer una concientización de los empleados de la institución sobre lo importante acerca de mantener la seguridad. -Tener acuerdos de confidencialidad con los empleados de la información más importante para la institución. -Establecer una política de contraseñas para los empleados.	-Realización de cursos de concienciación sobre la importancia de la seguridad de los datos para el personal de la entidad

Formato 3.38 Medidas Preventivas y Correctivas de Personas
Fuente: Elaboración Propia

3.3.11 Listado de Riesgos

- El Jefe de Proyecto y el Comité de Seguridad seleccionan los controles para la mitigación dispuesto por la NTP/ISO 27001:2008 para la empresa de las amenazas y vulnerabilidades, teniendo las medidas correctivas y preventivas para evitar los riesgos de los activos de información.
- El Jefe del Proyecto y Comité de Seguridad presentan con el fin de detallar los criterios de mejora y respaldar los procedimientos presentados para la implementación del proyecto.

PROYECTO SGSI Controles de la Seguridad de Información			
SGSI 010_5	**Versión de la Plantilla:1.0.0**	**Fecha:**	
Dominio		**Objetivos de Control**	**Controles**
1	Política de Seguridad	1	2
2	Organización de la Seguridad de la Información	2	11
3	Gestión de Activos	2	5
4	Seguridad de los Recursos Humanos	3	9
5	Seguridad física y del entorno	2	13
6	Gestión de comunicaciones y operaciones	10	32
7	Control de acceso	7	25
8	Adquisición, Desarrollo y mantenimiento de sistemas	6	16
9	Gestión de incidentes de seguridad	2	5
10	Gestión de continuidad del negocio	1	5
11	Cumplimiento	3	10

Formato 3.39
Fuente: Norma Técnica Peruana 27001:2008

3.3.12 Matriz de Valoración de Riesgos

a) Elaborar Proceso de Matriz de Valoración de Riesgos

- El Jefe del Proyecto y los Miembros del Comité debe presentar la matriz de valoración para los posibles riesgos y la escala de medición de probabilidad y del impacto con su respectiva definición. Ver formato 3.40, 3.41.
- El Jefe del Proyecto y el Comité de Seguridad elabora la matriz de riesgos. Ver formato 3.42.
- Si algún Miembro del Comité de Seguridad tiene algunas observaciones, indicar los puntos a modificar o agregar en la matriz; y envía un correo electrónico al comité de seguridad para que llegue a un consenso para realizar los cambios.
- Los Miembros del Comité de Seguridad envía correo electrónico al jefe del proyecto con los puntos a modificar, indicando su aprobación y firman la documentación.

b) Proceso de Actualización de Matriz de Valoración de Riesgos

- En caso de realizar un cambio en la matriz de valoración de riesgos, se debe llenar una solicitud de cambio, indicando los puntos a modificar o agregar.
- El Jefe del Proyecto revisa la solicitud y realiza los puntos a modificar o agregar, envía un correo electrónico al comité de seguridad para su revisión.
- El Comité de Seguridad revisa y si hubiera algo adicional que modificar explicar de qué trata y deben llegar a un consenso para la aprobación y firma en señal de acuerdo.

Escala de Impacto		
SGSI 012	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Calificación	**Explicación**	
B	**Baja:** los activos de información no serán afectados	
M	**Medio:** algunos activos de información pueden verse afectados	
A	**Alta:** los activos de información están amenazados de riesgo.	

Formato 3.40 Escala de Impacto
Fuente: Elaboración Propia

Escala de Probabilidad		
SGSI 012_1	**Versión de la Plantilla:1.0.0**	**Fecha:**
Calificación	**Explicación**	
B	**Baja:** aunque es improbable que ocurra el evento, podría ocurrir	
M	**Medio:** el evento se podría ocurrir	
A	**Alta:** el evento ocurrirá probablemente	

Formato 3.41 Escala de Probabilidad
Fuente: Elaboración Propia

Matriz de Riesgos			
SGSI 012_2	**Versión de la Plantilla: 1.0.0**		**Fecha:**
Probabilidad de ocurrencia	**B (1)**	**M (2)**	**A(3)**
A (3)	**M 3**	**A 6**	**A 9**
M (2)	**B 2**	**M 4**	**A 6**
B (1)	**B 1**	**B 2**	**M 3**
Impacto de riesgo			

Formato 3.42 Matriz de Riesgos
Fuente: Elaboración Propia

Interpretación de Nivel de Riesgo		
SGSI 012_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Alta	Riesgo alto requiere atención y acción inmediata	
Media	Riesgo moderado, requiere atención del área usuaria	
Baja	Riesgo bajo, se administra con procedimiento rutinarios.	

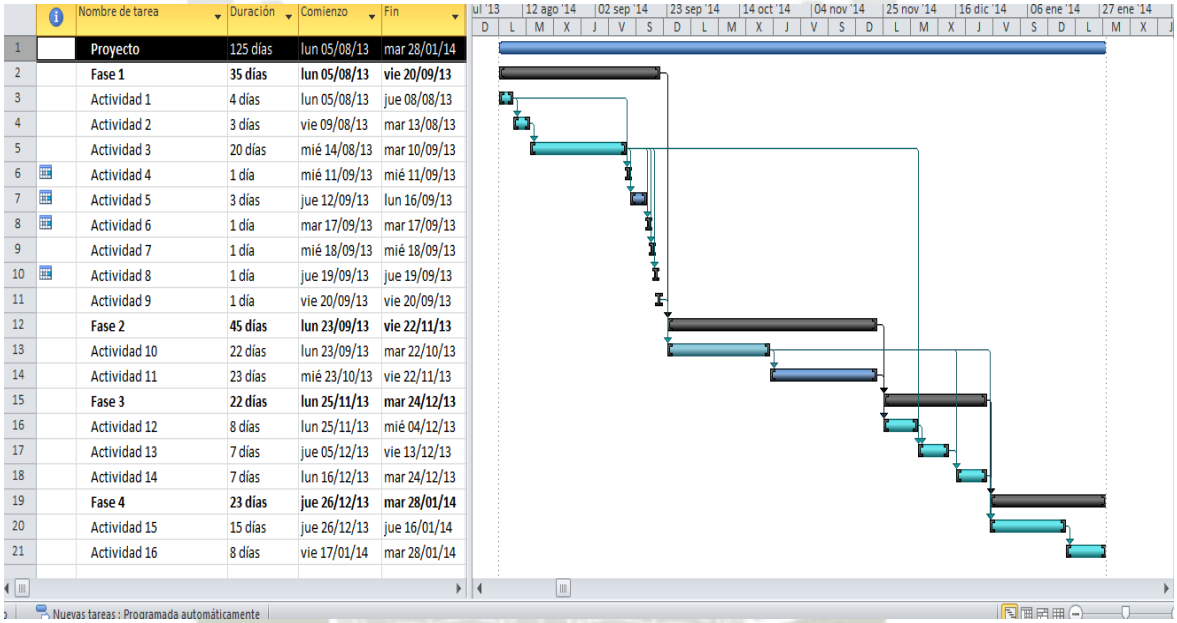
Formato 3.43 Interpretación de Nivel de Riesgo
Fuente: Elaboración Propia

3.4 FASE DE IMPLEMENTACIÓN

3.4.1 Enunciado del Cronograma y Actualización

- El Jefe de Proyecto y los Miembros del Comité de Seguridad debe proseguir y presentar el diagrama del proyecto para su respectiva implementación.
- En caso de haber una sobre asignación, el jefe del proyecto y los miembros del comité nivela los recursos del proyecto generando la extensión en la duración de actividades, en caso se haya sobrepasado la fecha límite de proyecto que se tiene como objetivo, se debe realizar una Compresión del Cronograma.
- El Jefe de Proyecto los miembros del comité corresponde realizarla Compresión del Cronograma., según las características del caso, se deberá utilizar las técnicas de Fast Tracking (recomendado en caso haya poco riesgo puesto que su aplicación lo incrementa).
- El Jefe de Proyecto y los miembros del comité identifica si hay variaciones respecto al cronograma, en caso de encontrar alguna variación respecto al cronograma, recomienda acciones correctivas para que se cumpla con lo definido en el modelo del cronograma.
- El Jefe de Proyecto y los miembros del comité evalúa las acciones correctivas recomendadas y decide si se ejecuta la acción correctiva, envía correo al comité seguridad para su revisión.

- El Jefe del Proyecto y los Miembros del Comité de Seguridad, indican la aprobación solicita que lo firmen en señal de aprobación del contenido de dicho documento.
- El Jefe del Proyecto y el Comité de Seguridad firman la aprobación en la implementación del proyecto, caso contrario de no aprobar, se regresa al punto anterior, indicando el motivo de su rechazo al documento.



	Nombre de tarea	Duración	Comienzo	Fin
1	Proyecto	125 días	lun 05/08/13	mar 28/01/14
2	Fase 1	35 días	lun 05/08/13	vie 20/09/13
3	Actividad 1	4 días	lun 05/08/13	jue 08/08/13
4	Actividad 2	3 días	vie 09/08/13	mar 13/08/13
5	Actividad 3	20 días	mié 14/08/13	mar 10/09/13
6	Actividad 4	1 día	mié 11/09/13	mié 11/09/13
7	Actividad 5	3 días	jue 12/09/13	lun 16/09/13
8	Actividad 6	1 día	mar 17/09/13	mar 17/09/13
9	Actividad 7	1 día	mié 18/09/13	mié 18/09/13
10	Actividad 8	1 día	jue 19/09/13	jue 19/09/13
11	Actividad 9	1 día	vie 20/09/13	vie 20/09/13
12	Fase 2	45 días	lun 23/09/13	vie 22/11/13
13	Actividad 10	22 días	lun 23/09/13	mar 22/10/13
14	Actividad 11	23 días	mié 23/10/13	vie 22/11/13
15	Fase 3	22 días	lun 25/11/13	mar 24/12/13
16	Actividad 12	8 días	lun 25/11/13	mié 04/12/13
17	Actividad 13	7 días	jue 05/12/13	vie 13/12/13
18	Actividad 14	7 días	lun 16/12/13	mar 24/12/13
19	Fase 4	23 días	jue 26/12/13	mar 28/01/14
20	Actividad 15	15 días	jue 26/12/13	jue 16/01/14
21	Actividad 16	8 días	vie 17/01/14	mar 28/01/14

Figura 4.1Cronograma de Actividades
Elaboración Propia

PROYECTO SGSI Cronograma del Proyecto			
SGSI 013	**Versión de la Plantilla:1.0.0**		**Fecha:**
FASES	**FECHA**	**OBJETIVO**	**QUE SE HACE**
Fase de Planteamiento	35 días hábiles	El objetivo es hacer el alcance del proyecto, elaborar la Estructura de Desglose de Trabajo y Estructura de Desglose de Riesgos, elaborar el Plan de SGSI	Dentro del Plan de SGSI, elaborar la identificación de los activos de información, gestión de comunicaciones, costos, tiempo y plan de riesgos para el proyecto, estos puntos abarca dentro de los días establecidos.
Fase de Implementación	45 días hábiles	El objetivo principal es elaborar lista de actividades y el cronograma de red.	En la fase de implementación, se debe tener completo todos los puntos en la fase anterior para hacer la correcta implementación para la empresa.
Fase de	22 días	El objetivo es hacer el	Se debe presentar informes respecto al

Seguimiento y Monitoreo	hábiles	seguimiento al proyecto.	Plan de Proyecto, Plan de Riesgos y Lista de Actividades.
Fase de Cierre	23 días hábiles	El objetivo presentar los entregables del proyecto y fichas de mejora.	Se debe entregar entregable, si cada actividad está implementando correctamente dentro del plazo dado.

APROBACION DEL COMITÉ			
( ) Aprobado		( ) Desaprobado	
(En caso de rechazo , indicar el motivo**)**			
ROL	**NOMBRE**	**FECHA**	**FIRMA**

Formato 3.44 Cronograma del Proyecto
Fuente: Elaboración Propia

- El Jefe del Proyecto y los Miembros del Comité de Seguridad presenta una ficha de actualización para las actividades del proyecto.

PROYECTO SGSI **Ficha de Actualización del Cronograma**			
SGSI 013_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**	
Fases y Sub-Actividades	**Periodo de inicio y final**	**Predecesor y Sucesor de la Actividad**	**Responsable**
Nombre de la fase			
Nombre de la Actividad			
Nombre de la Actividad			
Nombre de la fase			
Nombre de la Actividad			
Nombre de la Actividad			
Nombre de la fase			
Nombre de la Actividad			
Nombre de la Actividad			
Nombre de la fase			
Nombre de la Actividad			

Formato 3.45 Ficha de Actualización del Cronograma
Fuente: Elaboración Propia

Dónde:

Actividad: Indica el nombre de la sub-actividad

Periodo de Inicio y Final: Indica la fecha de inicio y final de la actividad

Predecesor y Sucesor: Indica cual es predecesor y el sucesor de cada actividad.

Responsable: Indica el nombre del responsable de la actividad

3.4.2 Implementación y Actualización de Lista de Actividades

- El Jefe del Proyecto y los Miembros del Comité de Seguridad debe presentar la lista de actividades al comité de seguridad para su implementación.

PROYECTO SGSI Lista de Actividades						
SGSI 013_2	**Versión de la Plantilla: 1.0.0**			**Fecha:**		
Cód.	**Nombre**	**Predecesor**	**Sucesor**	**Duración (horas)**	**Categoría**	**Responsable**
	Inicio					
1	Acta de Constitución de Comité de Seguridad				JP y CS	JP y CS
1.	**Fase de Planteamiento**					
1.1	**Organización del SGSI**					
A1	Elaborar Definición de la		A2	4	JP y CS	JP y CS
A2	Elaborar el Cuadro de Integrantes del Proyecto	A1	A3	4	JP y CS	JP y CS
1.2	**Alcance del Proyecto**					
A3	Elaborar la Definición del Alcance del Proyecto	A3	A4	6	JP y CS	JP y CS
A4	Elaborar EDT del proyecto	A4	A5	4	JP y CS	JP y CS
A5	Elaborar Recursos del RBS	A5	A6	4	JP y CS	JP y CS
1.3	**Elaborar el Plan de SGSI**					
A6	Elaborar Plan de Identificación de Activos	A6	A7	6	JP y CS	JP y CS
A7	Elaborar Plan de Gestión de Tiempo	A7	A8	6	JP y CS	JP y CS
A8	Elaborar Plan de Gestión de Costos	A8	A9	6	JP y CS	JP y CS
A9	Elaborar Plan de Gestión de Comunicaciones	A9	A10	6	JP y CS	JP y CS
1.4	**Elaboración de Plan de Riesgos**					
A10	Elaborar Identificación de Riesgos	A10	A11	6	JP Y CS	JP Y CS
A11	Elaborar Acción de Mitigación de Riesgos	A11	A12	6	JP y CS	JP y CS
A12	Elaborar Matriz de Riesgos	A12	A13	6	JP y CS	JP y CS
A13	Elaborar matriz de Valoración de	A13	A14	6	JP y CS	JP y CS
1.5	**Documentación del Alcance de Proyecto**					
A14	Elaborar Solicitud de Cambio	A1,A14	A15	2	JP y CS	JP y CS
1.6	**Documentación de Activos**					

PROYECTO SGSI Lista de Actividades						
SGSI 013_2	**Versión de la Plantilla: 1.0.0**			**Fecha:**		
Cód.	**Nombre**	**Predecesor**	**Sucesor**	**Duración (horas)**	**Categoría**	**Responsable**
A15	Elaborar Plantilla de Identificación de Activos	A6,A15	A16	3	JP y CS	JP y CS
A16	Elaborar Formatos para la Clasificación de Activos	A15	A17	3	JP y CS	JP y CS
A17	Elaborar Formatos para Inventario de Activos	A17	A18	3	JP y CS	JP y CS
1.7	**Documentación de Gestión de Tiempo**					
A18	Elaborar Lista de Actividades	A7,A18	A19	4	JP	JP y CS
A19	Elaborar Solicitud Cambio de Tiempo	A19	A20	2	JP y CS	JP y CS
1.8	**Documentación de Gestión de Costos**					
A20	Realizar Estimación de Costos de Actividades	A8,A20	A21	4	JP y CS	JP y CS
A21	Elaborar Solicitud de Cambio de Costos	A21	A22	2	JP y CS	JP y CS
1.9	**Documentación de Gestión de Comunicaciones**					
A22	Elaborar Flujo de Información del	A21	A23	4	JP y CS	JP y CS
A23	Elaborar Requisitos de Información	A23	A24	3	JP y CS	JP y CS
A24	Elaborar Información que será comunicada	A24	A25	3	JP y CS	JP y CS
A25	Elaborar Requisitos de Información de los Interesados	A24	A26	3	JP y CS	JP y CS
A26	Elaborar Matriz de Comunicaciones	A26	A27	3	JP y CS	JP y CS
A27	Elaborar Solicitud de Cambio de Comunicaciones	A27	A28	2	JP y CS	JP y CS
1.10	**Documentación Plan de Riesgos**					
A28	Elaborar Lista de Riesgos (vulnerabilidades y amenazas)	A10,A28	A29	4	JP y CS	JP y CS
A29	Elaborar Acciones para Mitigar los Riesgos	A29	A30	4	JP y CS	JP y CS
A30	Elaborar Matriz de Riesgos	A30	A31	4	JP y CS	JP y CS
A31	Elaborar Valoración de Riesgos	A31	A32	4	JP y CS	JP y CS
1.11	**Elaboración de Cronograma del Proyecto**					
A32	Elaborar el Cronograma	A32	A33	6	JP y CS	JP y CS
2.	**Fase de Implementación**					

PROYECTO SGSI Lista de Actividades						
SGSI 013_2	**Versión de la Plantilla: 1.0.0**			**Fecha:**		
Cód.	**Nombre**	**Predecesor**	**Sucesor**	**Duración (horas)**	**Categoría**	**Responsable**
A33	Cronograma y Actualización de Trabajo	A33	A34	5	JP y CS	JP y CS
A34	Implementación y Actualización Actividades	A34	A35	5	JP y CS	JP y CS
A35	Acción de Mitigación de Riesgos	A35	A36	5	JP y CS	JP y CS
A36	Listado de Riesgos	A36	A37	5	JP y CS	JP y CS
A37	Matriz de Riesgos	A37	A38	5	JP y CS	JP y CS
3	**Fase de Monitoreo**					
A38	Elaborar Proceso de Monitoreo y Revisión de los Riesgos	A38	A39	5	JP y CS	JP y CS
A39	Ficha de Sugerencia y Mejora del Proyecto	A39	A40	4	JP y CS	JP y CS
4.	**Fase de Cierre**					
A40	Proceso de Entregables del SGSI	A40	A41	3	JP y CS	JP y CS
A41	Acta de Transferencia del Proyecto de SGSI	A41	A42	3	JP y CS	JP y CS
A42	Fin del Proyecto					

Formato 3.46 Lista de Actividades
Fuente: Elaboración Propia

- Seguidamente el Jefe del Proyecto y los Miembros del Comité de Seguridad presenta una ficha de actualización para las actividades para el proyecto

PROYECTO SGSI Ficha de Actualización de la Lista de Actividades							
SGSI 013_3		**Versión de la Plantilla: 1.0.0**			**Fecha:**		
Código	**Fecha (DD/MM/AAAA)**	**Hora Inicio (HH:MM)**	**Hora Fin (HH:MM)**	**Responsable**	**Actividades del Cronograma**	**Estado de la Actividad**	**Observaciones**

Formato 3.47 Ficha de Actualización de la Lista de Actividades
Fuente: Elaboración Propia

Dónde:

Código: Código asignado a la actividad

Fecha (DD/MM/AA): Indica el día, mes y el año

Hora (HH:MM): Indica la hora del inicio de la actividad

Hora Fin (HH:MM) Indica la hora del final de la actividad

Responsable: Indica el responsable de la actividad

Actividades del Cronograma: Indica la actividad del programa

Estado de la Actividad: Indica cómo se encuentra el proceso (pr), Pendiente (pe), Completo (co)

Observaciones: Indicara las observaciones que contendrá cada actividad

3.4.3 Implementación de Acción de Mitigación de Riesgos

- El Jefe del Proyecto y los Miembros del Comité de Seguridad presenta ficha de acción de mitigación de riesgos para el proyecto.

PROYECTO SGSI Ficha de Acción de Mitigación de Riesgos				
SGSI 013_4	**Versión de la Plantilla:1.0.0**		**Fecha:**	
Nombre del Activo	**Descripción del Riesgo**	**Acción Preventiva**	**Acción Correctiva**	**Responsable**

Formato 3.48 Ficha de Acción de Mitigación de Riesgos
Fuente: Elaboración Propia

Dónde:

Nombre del Activo: Indica el nombre del activo de información de la empresa

Descripción del riesgo: Indicar una breve descripción del riesgo que se presente en el activo

Acciones Preventiva: Indica una breve descripción de medidas preventivas se deben dar para el activo.

Acción Correctiva: Indica una breve descripción que medidas correctivas se deben dar para el activo.

Responsable: Indicar el nombre del responsable.

3.4.6 Implementación de Listado de Riesgos

- El Jefe del Proyecto y los Miembros del Comité de Seguridad presenta ficha de listado de riesgos.

PROYECTO SGSI Ficha Listado de Riesgos		
SGSI 013_5	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Código Activo		

Nombre del Activo	
Descripción de la Amenaza	
Descripción de la Vulnerabilidad	
Nombre del Control	
Objetivo del Control	
Sugerencias del Control	
Observaciones	
Responsable	

Formato 3.49 Ficha Listado de Riesgos
Fuente: Elaboración de la Plantilla

Dónde:

Código del Activo: Indica el código del activo

Nombre del Activo: Nombre del Activo

Descripción de la Amenaza: Indica una descripción de la amenaza

Descripción de la Vulnerabilidad: Indica una descripción de la vulnerabilidad

Nombre del Control: Indica el nombre del control de la NTP/SO 27001:2008

Objetivo: Indica el objetivo del control

Sugerencias del Control: Indica la sugerencias que especifica cada control que se tomara en cuenta en el proyecto

Observaciones Indica las posibles observaciones para control que se tome en cuenta.

Responsable. Indicar el nombre del responsable.

3.4.7 Implementación de Ficha Matriz de Riesgos

- El Jefe del Proyecto y los miembros del Comité de Seguridad presenta ficha matriz de riesgos para el proyecto.

PROYECTO SGSI Ficha de Matriz de Riesgos							
SGSI 013_6		**Versión de la Plantilla:1.0.0**			**Fecha:**		
Nombre del Activo	**Amenazas**	**Vulnera bilidad**	**Nivel de Probabilidad**	**Nivel de Impacto**	**Nivel de Riesgo**	**Mitigación**	**Responsable**

Formato 3.50 Ficha de Matriz de Riesgos
Fuente: Elaboración Propia

Dónde:

Nombre: Indica el nombre del activo.

Amenazas: Indica una descripción de las posibles amenazas que presenten los activos.

Vulnerabilidades: Indicar una descripción de las posibles vulnerabilidades de los activos

Nivel de Probabilidad: Indica si es medio, baja y alta en el activo de información.

Nivel de Impacto: Indica si es medio, baja y alta en el activo de información.

Nivel del Riesgo: Indica el valor del nivel de impacto y nivel de probabilidad si es medio, baja y alta en el activo de información.

Mitigación: Indica que medidas se va tomar sobre el resultado del nivel de riesgo.

Responsable: Indica quien va ser el responsable de ficha de matriz de riesgos

3.5 FASE DE MONITOREO Y REVISIÓN

3.5.1 Elaborar Proceso de Monitoreo y Revisión de los Riesgos

- El Jefe de Proyecto y los Miembros del Comité se reúne con el comité de seguridad para detallar para la presentación de informes de Plan de Proyecto, Revisión de Riesgos y Revisión de Actividades.

PROYECTO SGSI Informe Plan del Proyecto		
SGSI 014	**Versión de la Plantilla:1.0.0**	**Fecha:**
Nombre de la Empresa/Entidad del Estado	**Fecha de Elaboración**	**Fecha de Revisión**
Elaborado por:	**Revisado por:**	
Estado del Plan del Proyecto		
Nombre y Descripción (Fase y Actividad)	**Estado Situacional del Proyecto(**)**	
Indicaciones (posibles cambios)		
Problemas de no realizar cambios		
Observaciones		

Comentarios	
Jefe del Proyecto	**Firma**

Formato 3.51 Informe Plan del Proyecto
Fuente: Elaboración Propia

Dónde:

Pendiente (Pe:; encuentra en proceso de elaboración.

Aceptado (Ac): está conforme con el contenido

Rechazado (Re): no aceptó el contenido

Revisión (Rv): está verificando el contenido

Por Ajustar (Pa; observaciones después de su revisión

Terminado (Te): se terminó pero no requiere aprobación

Aprobado (Ap): aprobado el plan

PROYECTO SGSI **Informe Revisión de Riesgos**			
SGSI 014_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**	
Nombre de la Empresa del Estado		**Fecha de Elaboración**	**Fecha de Revisión**
Elaborado por:		**Revisado por:**	
Especificación del Activo			
Descripción del Riesgos (Amenazas y/o Vulnerabilidades)			
Acciones de Medidas Preventivas			
Acciones de Medidas Correctivas			
Actualización de Activos (posibles nuevos riesgos)			

Recomendaciones	
Comentarios	
Nombre del Gerente de la Empresa	**Firma**

Formato 3.52 Informe Revisión de Riesgos
Fuente: Elaboración Propia

PROYECTO SGSI **Informe de Actividades**			
SGSI 014_2	**Versión de la Plantilla: 1.0.0**	**Fecha:**	
Nombre de la Empresa del Estado		**Fecha de Elaboración**	**Fecha de Revisión**
Elaborado por:		**Revisado por:**	
Estado de la Actividad			
Nombre de la Actividad y Descripción		**Estado del Indicador(**)**	
Medidas Preventivas y Correctivas			
Observaciones			
Comentarios			
Jefe del Proyecto		**Firma**	

Formato 3.53 Informe de Actividades
Fuente: Elaboración Propia

Dónde:

Tipo de Indicador: (A) La actividad avanza si ningún retrasó, (R): La actividad hay retrasó

3.5.2 Ficha de Sugerencia y Mejora del Proyecto

- El Jefe del Proyecto y los Miembros del Comité de Seguridad debe presentar y detallar la presentación de la ficha de sugerencia y mejora del proyecto para la entidad/empresa del estado

Proyecto del SGSI Ficha de Sugerencia y Mejora		
SGSI 014_3	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Nombre del Jefe del Proyecto		
Miembros del Comité de Seguridad		
Descripción de Mejora		
Impacto de la Mejora		
Mejora de Actividades		
Documentación referida		
Responsable		

Formato 3.54 Ficha de Sugerencia y Mejora
Fuente: Elaboración Propia

Dónde:

Descripción de Mejora: Proporcionar una descripción breve de implantación de la mejora, indicado el activo o actividad

Impacto: Proporcionar una descripción breve del impacto que causaría a la empresa/entidad en caso de no haber implantado la mejora.

Mejora de Actividades: Señalar las actividades a realizar para la obtención de mejores resultados.

Documentación referida: Indicar y describir los entregables en base para la realización de las acciones

Responsable: Indica el responsable de la ficha de mejora

3.6 FASE DE CIERRE

3.6.1 Proceso de Entregables del SGSI

- El Jefe del Proyecto y los Miembros del Proyecto ejecuta la aprobación y va certificando que está cumpliendo con los criterios para la entrega de los entregables en cada actividad del proyecto.
- El Jefe del Proyecto y los Miembros del Comité de Seguridad presenta el documento de los entregables de todas aquellos criterios de aceptación que no se están

cumpliendo para que el(los) programador(es) encargado(s) corrijan el entregable (acción correctiva recomendada)

PROYECTO SGSI Entregables del Proyecto					
SGSI 015		Versión de la Plantilla:1.0.0		Fecha:	
Historial de Revisiones	Código	Descripción	Autor	Fecha	Aprobado por

Formato 3.55 Documento de los Entregables
Fuente: Elaboración Propia

PROYECTO SGSI Aprobación del Entregable				
SGSI 015_1		Versión de la Plantilla:1.0.0		Fecha:
Historial de Entregables	Código	Nombre del Entregable	Responsable	Fecha

Formato 3.56 Aprobación de Entregables
Fuente: Elaboración Propia

3.6.2 Acta de Transferencia del Proyecto de SGSI

– El Jefe del Proyecto y los Miembros del Comité de Seguridad presenta el acta de transferencia del proyecto al concluir con la implementación del Sistema de Gestión de Seguridad de Información.

PROYECTO SGSI Acta de Transferencia del Proyecto		
SGSI 015_2	Versión de la Plantilla:1.0.0	Fecha:
1.- DATOS GENERALES		
Nombre del Proyecto		
Nombre del Gerente de la Empresa		
Nombre del Jefe del Proyecto		
Miembros del Comité de Seguridad		
Fecha de Entrega		

Habiéndose cumplido con todos los requerimientos, estándar y criterios de aceptación establecidos, los firmantes aceptamos la transferencia del proyecto.

2.- FIRMAN EN SEÑAL DE APROBACION

NOMBRE COMPLETO	FIRMA	FECHA

3. OBSERVACIONES

Formato 3.57Acta de Transferencia del Proyecto
Fuente: Elaboración Propia

CAPITULO IV

EVALUACION DE LA METODOLOGIA

4.1. Introducción

La evaluación ha sido realizada en una Entidad del Estado Peruano. Se ha aplicado el Cuestionario al personal de informática, las Políticas de la Entidad Pública prohíben detallar los temas tratados y/o conceptos establecidos en esta tesis.

4.2. Perfil de la Empresa y de los Encuestados

a) Perfil de las Entidades Públicas.

Empresa que requieren contratar bienes, obras y/o servicios en el Estado Peruano.

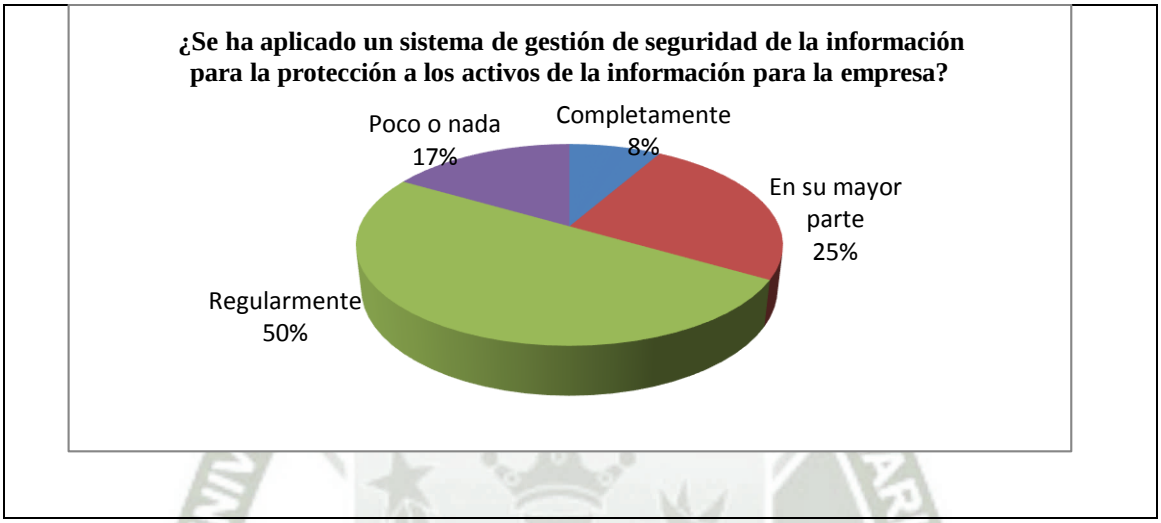
b) Perfil de los Entrevistados

Son todos aquellos que trabajan en la Entidad Pública, que hayan tenido, o tengan relación directa con la Entidad Pública.

4.3. Resultado del Cuestionario

4.3.1. ¿Se ha aplicado un sistema de gestión de seguridad de la información para la protección a los activos de la información para la empresa? (Control)

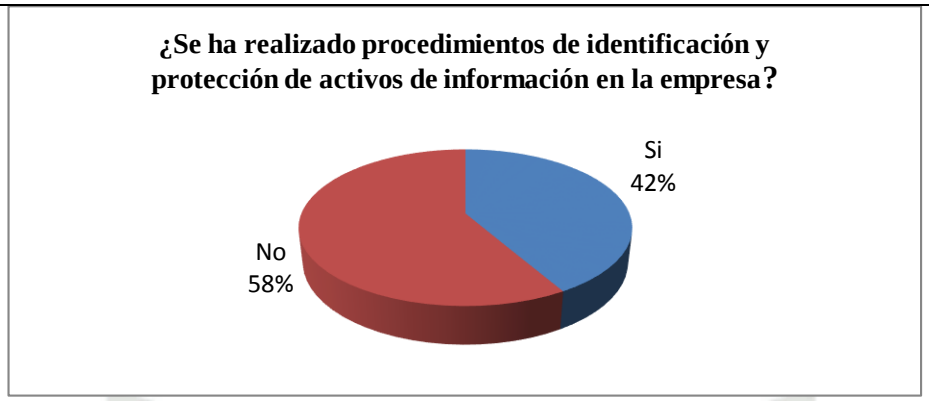
Respuesta	Porcentaje
Completamente	8%
En su mayor parte	25%
Regularmente	50%
Poco o nada	17%



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.2. ¿Se ha realizado procedimientos de identificación y protección de activos de información en la empresa? (Control)

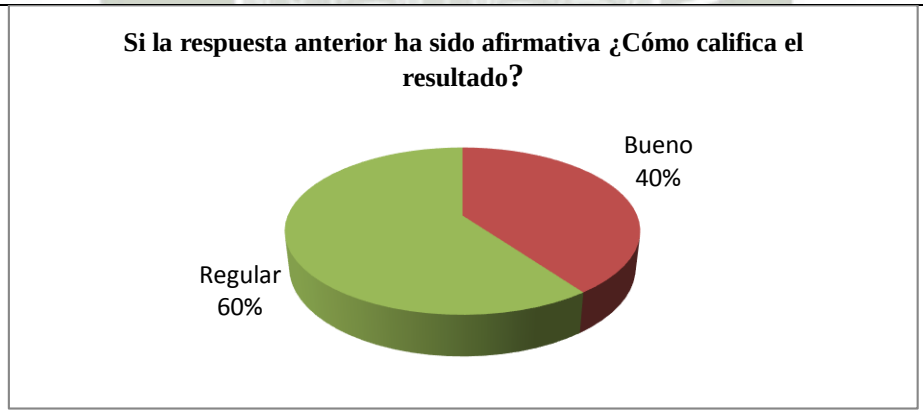
Respuesta	Porcentaje
Si	42%
No	58%



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.3. Si la respuesta anterior ha sido afirmativa ¿Cómo califica el resultado?

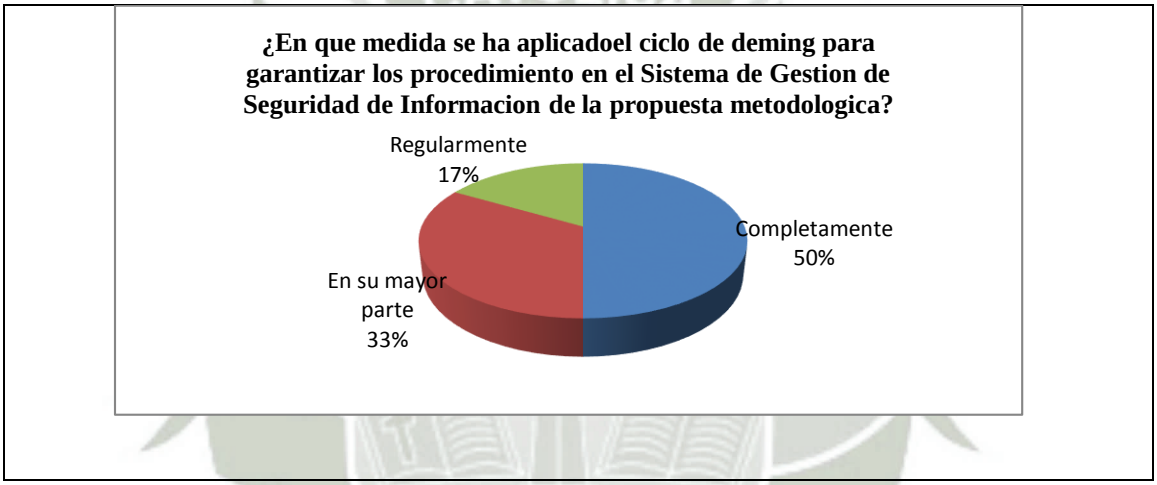
Respuesta	Porcentaje
Muy bueno	-
Bueno	40%
Regular	60%
Malo	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.4 ¿En qué medida se ha aplicado el ciclo de Deming para garantizar los procedimiento en el Sistema de Gestión de Seguridad de Información de la propuesta metodológica?

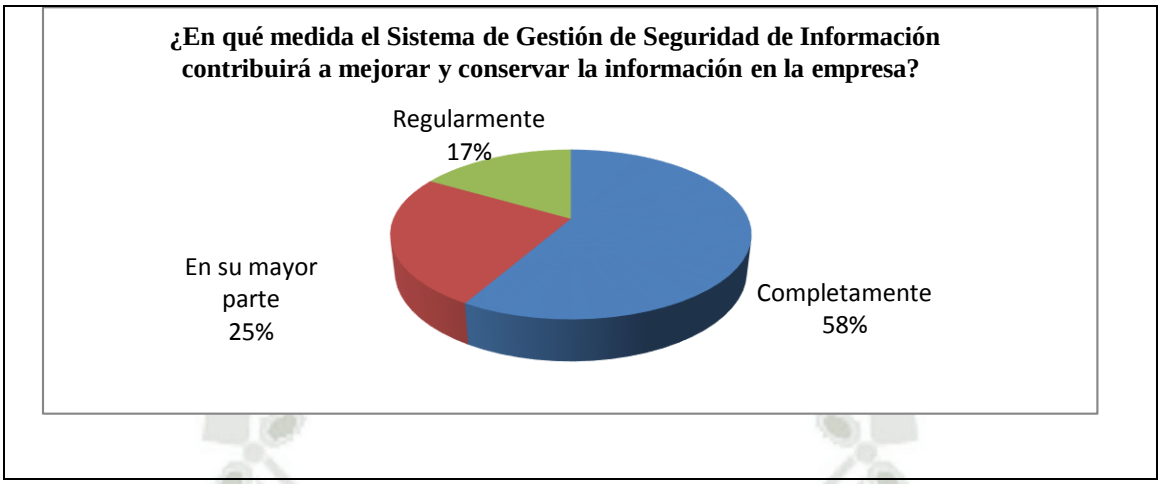
Respuesta	Porcentaje
Completamente	50%
En su mayor parte	33%
Regularmente	17%
Poco o nada	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.5. ¿En qué medida el Sistema de Gestión de Seguridad de Información contribuirá a mejorar y conservar la información en la empresa?

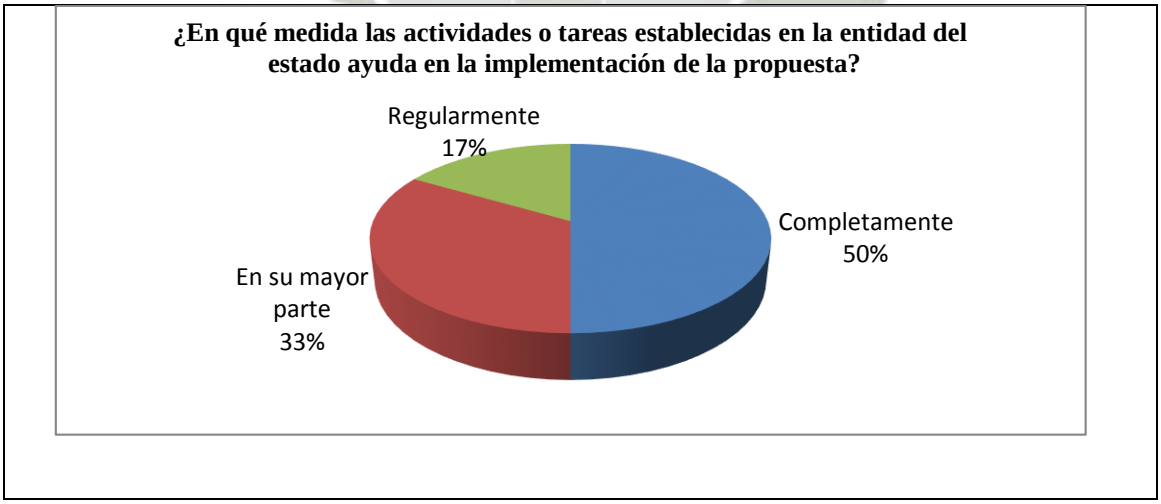
Respuesta	Porcentaje
Completamente	58%
En su mayor parte	25%
Regularmente	17%
Poco o nada	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.6. ¿En qué medida las actividades o tareas establecidas en la entidad del estado ayuda en la implementación de la propuesta?

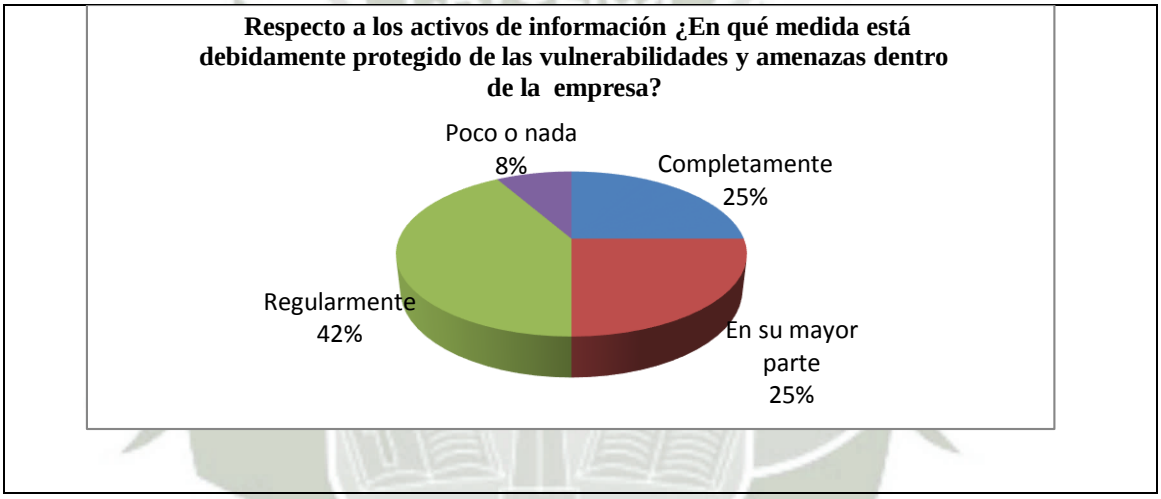
Respuesta	Porcentaje
Completamente	50%
En su mayor parte	33%
Regularmente	17%
Poco o nada	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.7. Respecto a los activos de información ¿En qué medida está debidamente protegido de las vulnerabilidades y amenazas dentro de la empresa?

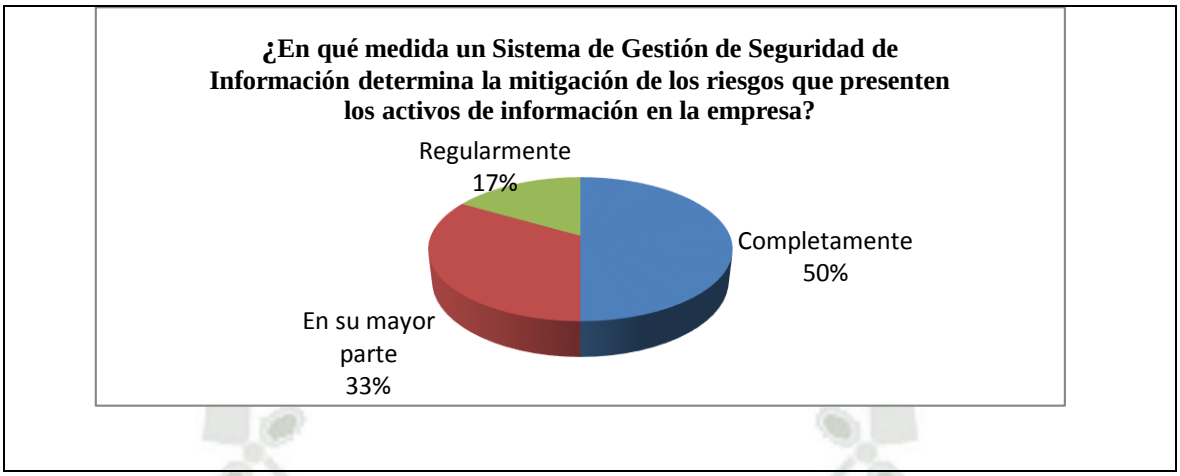
Respuesta	Porcentaje
Completamente	25%
En su mayor parte	25%
Regularmente	42%
Poco o nada	8%



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.8. ¿En qué medida un Sistema de Gestión de Seguridad de Información determina la mitigación de los riesgos que presenten los activos de información en la empresa?

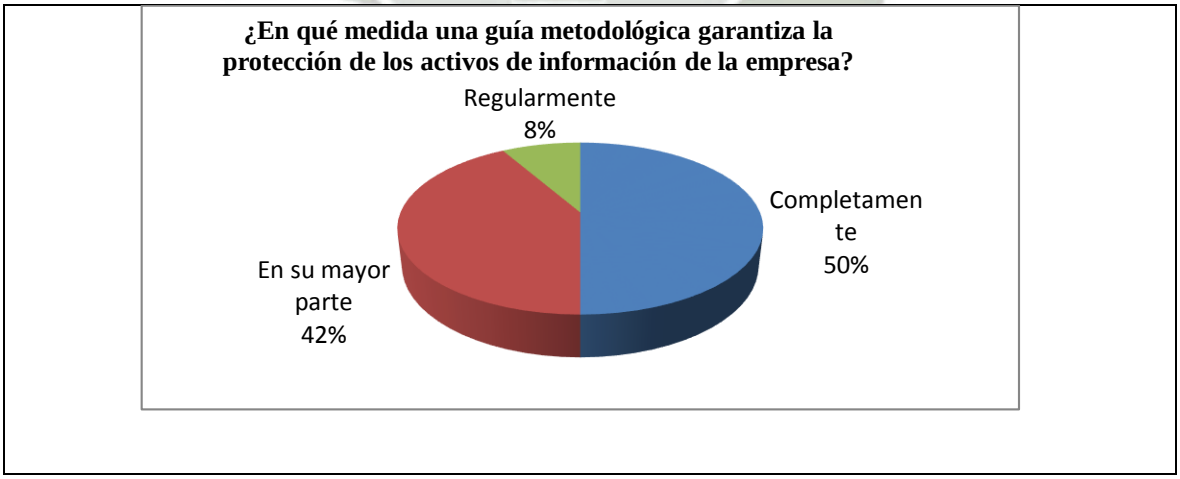
Respuesta	Porcentaje
Completamente	50%
En su mayor parte	33%
Regularmente	17%
Poco o nada	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.9. ¿En qué medida una guía metodológica garantiza la protección de los activos de información de la empresa?

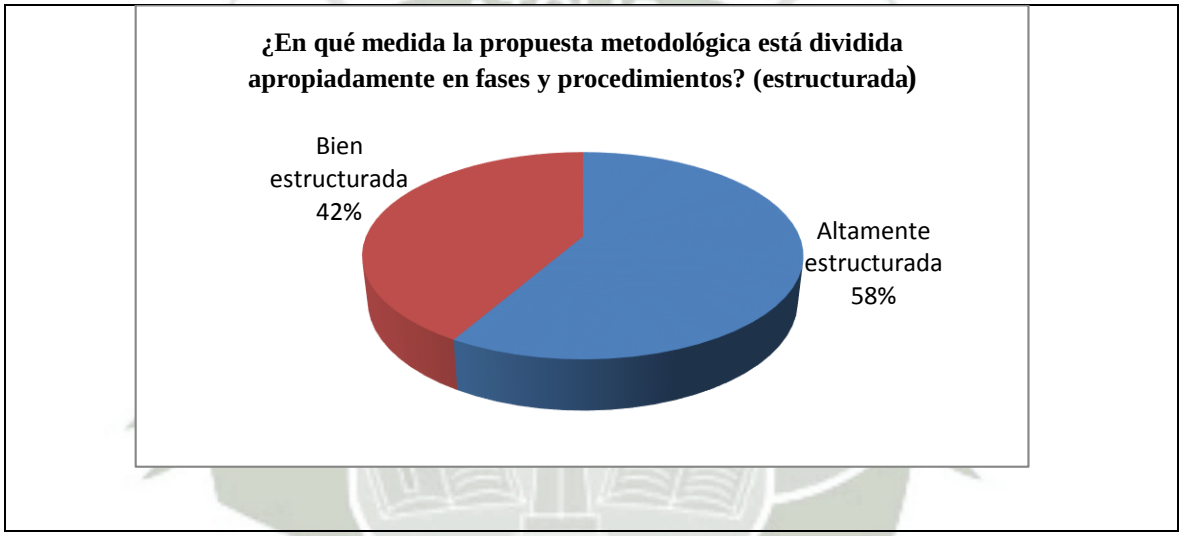
Respuesta	Porcentaje
Completamente	50%
En su mayor parte	42%
Regularmente	8%
Poco o nada	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.10. ¿En qué medida la propuesta metodológica está dividida apropiadamente en actividades y tareas? (estructurada)

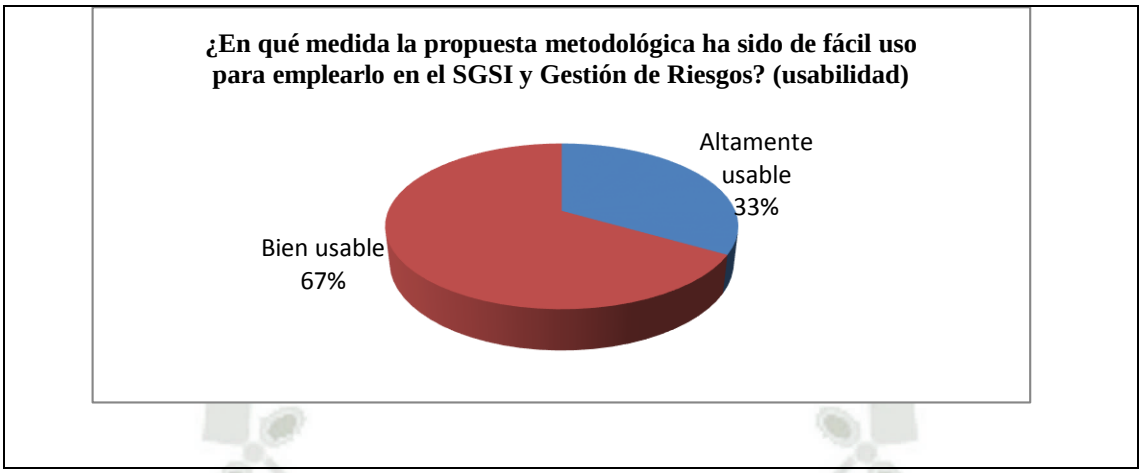
Respuesta	Porcentaje
Altamente estructurada	58%
Bien estructurada	42%
Poco estructurada	-
Nada estructurada	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.11. ¿En qué medida la propuesta metodológica ha sido de fácil uso para emplearlo en el SGSI y Gestión de Riesgos? (usabilidad)

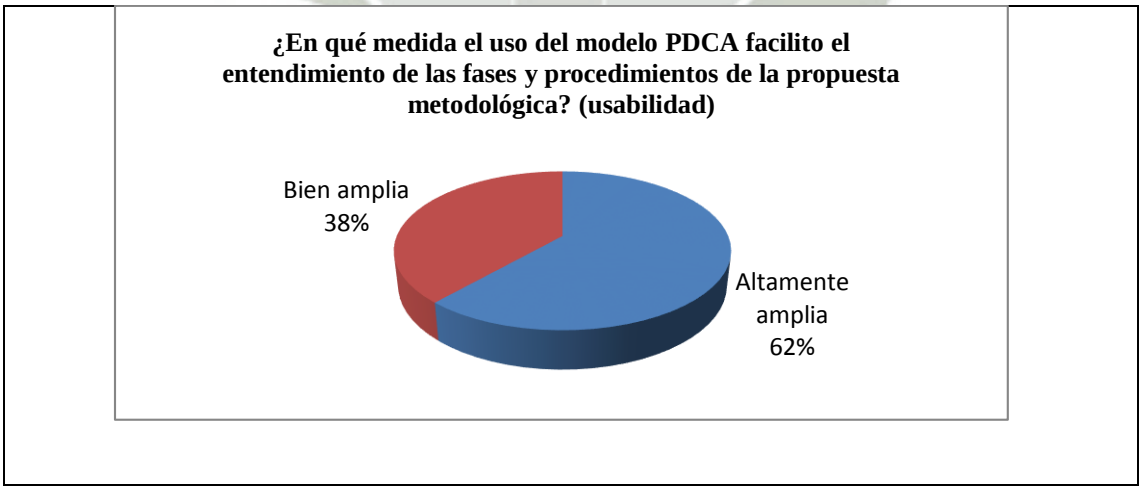
Respuesta	Porcentaje
Altamente usable	67%
Bien usable	33%
Poco usable	-
Nada usable	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.12 ¿En qué medida el uso del modelo PDCA facilito el entendimiento de las fases y procedimientos de la propuesta metodológica? (usabilidad)

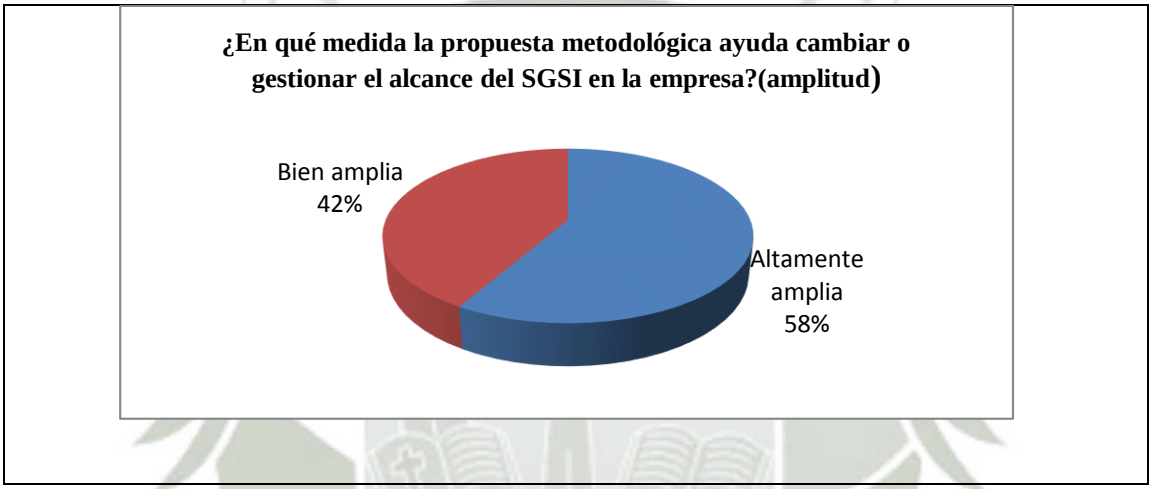
Respuesta	Porcentaje
Altamente amplia	58%
Bien amplia	42%
Poco amplia	-
Nada amplia	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

4.3.13. ¿En qué medida la propuesta metodológica ayuda cambiar o gestionar el alcance del SGSI en la empresa? (amplitud)

Respuesta	Porcentaje
Altamente amplia	58%
Bien amplia	42%
Poco amplia	-
Nada amplia	-



Fuente: Encuesta dirigida a empleados
Elaboración Propia

CONCLUSIONES

1. Se determinó que la propuesta metodología presentada para la implementación de la NTP ISO/IEC 27001:2008 en una entidad pública, permite gestionar y proteger los activos que son parte fundamental de la seguridad de la información.
2. Al aplicar adecuadamente el ciclo de Deming (PDCA) ayuda a garantizar la implementación de un SGSI, determinando que los procedimientos en cada fase tienen el propósito de lograr la seguridad de información en los activos de la entidad del Estado.
3. Con la identificación y el desarrollo de las actividades y tareas dadas en la propuesta metodológica, se ha logrado determinar que los requerimientos dados ayudan con la implementación de la NTP/ISO 27001:2008.
4. Asignando los controles adecuados para mitigar y designando a los responsables de dichas tareas ayudan a tener un mejor control en los activos de información en la gestión de riesgos en la propuesta metodológica.
5. Se determinó que la identificación las amenazas y vulnerabilidades que se presentan a los activos de información pueden ser mitigados en la institución del estado.
6. Es fundamental tener medidas preventivas y correctivas que ayudan a mitigar los riesgos en los activos de información para contrarrestar las amenazas y vulnerabilidades que afecten la continuidad del negocio de la institución.
7. A través de elaboración de una matriz de riesgos permite determinar el nivel de riesgo que se presenten en los activos de información y por lo cual permitirá mitigar el riesgo que se presenten en la institución del estado.

8. El éxito de la implementación de la propuesta y/o mejora permanente es el apoyo y el compromiso de la gerencia de la entidad del Estado.
9. La implementación de la NTP 27001:2008 permite que la institución tome conciencia respecto a la seguridad de la información acerca de los activos que puedan ser afectados por los riesgos que se presentan en la institución del estado.

RECOMENDACIONES

1. Desarrollar un aplicativo de seguimiento y control para dar soporte a la propuesta metodológica para una entidad del Estado.
2. Ampliar la propuesta metodológica para todas las áreas en las entidades del Estado peruano para garantizar su confidencialidad, integridad y disponibilidad de los activos de información.
3. Desarrollar una mejora continua a la estructura metodológica dentro del contexto de los procedimientos y fases de la propuesta
4. Debe lograr el compromiso de la gerencia y los empleados para garantizar la adecuada implementación de la propuesta metodológica dentro de la entidad del Estado.
5. Se recomienda registrar y mantener actualizada todos los procedimientos, especialmente a los activos de información que pueden sufrir posibles riesgos que afecten a la entidad.
6. La entidad debe formar un Comité de Seguridad para la implementación de la metodología y realizar seguimiento a los procedimientos del proyecto.

BIBLIOGRAFIA

- Alberto G. Alexander, *Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El enfoque ISO 27001:2005*.
- Álvarez Zurita, Flor María y García Guzmán, Pamela Anabel (2007), *Implementación de Sistema de Gestión de Seguridad de Información basado en la Norma ISO 27001, para la Intranet de la Corporación Metropolitana de Salud,* Escuela Politécnica Nacional, Ecuador.
- Ampuero Chang, Carlos Enrique (2011), *Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de seguros*. Facultad de Ciencias y Ingeniería, Pontificia Universidad Católica del Perú.
- Aranda Segovia, José Alfonso (2009), *Implementación del Primer Sistema de Gestión de Seguridad de la Información, en el Ecuador, Certificado bajo la Norma ISO27001:2005,* Facultad de Ingeniería en Electricidad y Computación, Ecuador.
- Castañeda Cadena, Luis Armando y Quezada Sarasti, Washington Ricardo (2007), *Aplicación de la Norma Técnica 27001:2005, para la Gestión de la Seguridad de la Información en la Dirección de Desarrollo Institucional (DDI) del Instituto Ecuatoriano de Seguridad Social,* Escuela Politécnica Nacional, Ecuador.
- Edsel Enrique Urueña (2012), *Sistema de Gestión de la Seguridad de la Información – Sgsi.*
- Gavilanes Pilco, Verónica Isabel (2011), *Elaborar una metodología aplicando la norma ISO 27001en la Implementación de un Sistema de Gestión de Seguridad de*

Información (SGSI) en el Desitel en la Espoch, Facultad de Informática y Electrónica, Escuela Superior de Politécnica de Chimborazo.

- Instituto Nacional de Estadística e Informática (2002), *Lineamientos de* Política *Nacional de Seguridad de la Información en el Estado Peruano*
- Norma Técnica Peruana NTP-ISO/IEC 27001:2008 (2008), *EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información*
- *Pallas Mega, Gustavo(2009), Metodología de Implantación de un SGSI en un grupo empresarial jerárquico, Instituto de Computación – Facultad de Ingeniería Universidad de la República*
- Poveda, José M. (2013), *Auditoria Informática.*
- Información de Sistema de Gestión de Seguridad de la Información - Disponible en: <http://www.ceeisec.com/nuevaweb/doc/informacionSGSI.pdf>
- El Portal de ISO 27001 en español. <http://www.iso27000.es/sgsi.html>
- Gestión de Riesgos en la Seguridad Informática <http://www.protejete.wordpress.com>
- Blog de Kaspersky sobre El panorama de malware en América Latina en el 2013: pronóstico para el 2014 <http://latam.kaspersky.com/Malware2013LatAm>
- Introducción a análisis de riesgos- Metodologías (I y II). <http://www.securityartwork.es/2012/04/02/introduccion-al-analisis-de-riesgos-%E2%80%93-metodologias-ii/>
- Consultoría Iso 27001 - Sistemas de gestión de seguridad de la información <http://www pqsperu.com>

- Instituciones deben implementar la Norma ISO 27000, Aranda Software. - <arandasoft.com/instituciones-peruanas-deben-implementar-la-n/>

ANEXOS

ANEXOA

ENCUESTA

El objetivo de esta encuesta es identificar el alcance de la propuesta metodológica de Seguridad de la Información.

- Esta encuesta tiene 13 preguntas

- Lea atentamente cada una de ellas y responda marcando con una X la alternativa que mejor identifiqué su parecer.

- Si se equivoca o desea corregir su respuesta solicite al encuestador una nueva encuesta, la anterior se destruirá.

- No ponga su nombre, ni ninguna identificación suya en esta encuesta.

- Si no le corresponde llenar la encuesta por favor devuélvala al encuestador.

1. ¿Se ha aplicado un sistema de gestión de seguridad de la información para la protección a los activos de la información para la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

2. Se ha realizado procedimientos de identificación y protección de activos de información en la empresa?

Si	( )
No	( )

3. Si la respuesta anterior ha sido afirmativa ¿Cómo califica el resultado?

Muy bueno	( )
Bueno	( )
Regular	( )
Malo	( )

4. ¿En qué medida se ha aplicado el ciclo de Deming para garantizar los procedimientos en el Sistema de Gestión de Seguridad de Información de la propuesta metodológica?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

5. ¿En qué medida el Sistema de Gestión de Seguridad de Información contribuirá a mejorar y conservar la información en la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

6. ¿En qué medida la estructura metodológica establecida en la empresa del estado mejora la protección de los activos de información?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

7. Respecto a los activos de información ¿En qué medida está debidamente protegido de las vulnerabilidades y amenazas dentro de la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )

Poco o nada	( )

8 ¿En qué medida un Sistema de Gestión de Seguridad de Información determina la mitigación de los riesgos que presenten los activos de información en la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

9. ¿En qué medida una guía metodológica garantiza la protección de los activos de información de la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

10. ¿En qué medida la propuesta metodológica está dividida apropiadamente en fases y procedimientos? (estructurada)

Altamente estructurada	( )

Bien estructurada	( )
Poco estructurada	( )
Nada estructurada	( )

11. ¿En qué medida la propuesta metodológica ha sido de fácil uso para emplearlo en el SGSI y Gestión de Riesgos? (usabilidad)

Altamente usable	( )
Bien usable	( )
Poco usable	( )
Nada usable	( )

12. ¿En qué medida el uso del modelo PDCA facilito el entendimiento de las fases y procedimientos de la propuesta metodológica? (usabilidad)

Altamente usable	( )
Bien usable	( )
Poco usable	( )
Nada usable	( )

13. ¿En qué medida la propuesta metodológica ayuda cambiar o gestionar el alcance del SGSI en la empresa? (amplitud)

Altamente amplia	( )
Bien amplia	( )
Poco amplia	( )
Nada amplia	( )

ANEXO B

CONTROLES PARA LA SEGURIDAD DE INFORMACION

A.1.Política de Seguridad

A.1.1 Política de la Seguridad de Información

Objetivo Principal: dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requisitos del negocio, las leyes y las regulaciones. Pasos:

1	Documentos de política de seguridad de la información	Control: La gerencia deberá aprobar, publicar y comunicar a todos los empleados y terceras partes que lo requieren.
2	Revisión de la Política de Seguridad de información	Control: La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurad que siga siendo apropiada, conveniente y efectiva.

A.2 Seguridad Organizacional

A.2.1 Organización Interna

Objetivo: Gestionar la seguridad de la Información dentro de la organización. Pasos:

1	Comité de Gestión de Seguridad de la Información	Control: La gerencia debe respaldar activamente la seguridad dentro de la organización a través de una dirección clara, un compromiso apropiado, recursos adecuados y conocimiento de responsabilidades de la seguridad de información.
2	Coordinación de la seguridad de la información	Control: Las actividades en la seguridad de información deben ser coordinados por representantes de diferentes partes de la organización que tengan roles relevantes y funciones de trabajo.
3	Asignación de responsabilidades sobre seguridad de la información	Control: Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.
4	Proceso de autorización para las nuevas instalaciones de procesamiento de información	Control: Debe establecerse y definirse un proceso de gestión de autorización para facilitar los nuevos procesamientos información.
5	Acuerdos de confidencialidad	Control: Se debe identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información.
6	Contacto con autoridades	Control: Se debe mantener contactos apropiados con las autorizaciones relevantes
7	Contacto con grupos de interés especial	Control: Se debe mantener contactos con grupos de interés especial u otros foros de especialistas en seguridad así como de asociaciones profesionales.
8	Revisión independiente de seguridad de la información	Control: El alcance de la organización para mejorar la seguridad de información, así como su implementación (como por ejemplo: los

		objetivos de control, los controles, las políticas procesos y procedimientos) deben ser revisados independientemente durante intervalos planificados o cuando ocurran cambios significativos en la implementación.

A.2.2 Seguridad del acceso a terceras partes

Objetivo: Mantener la seguridad de las instalaciones de procesamiento de la información organizacional que acceden, procesan, comunican o gestionan terceros. Pasos:

1	Identificación de riesgos por el acceso de terceros	Control: Se evaluara los riesgos al acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementaran controles de seguridad adecuados ante de permitir su acceso.
2	Requisitos de seguridad cuando se trata con clientes	Control: Se deben identificar todo los requisitos de seguridad antes de dar acceso a clientes a los activos o a la información de la empresa.
3	Requisitos de seguridad en contratos con terceros	Control: Los acuerdos que involucran el acceso, procesamiento, comunicación o manejo de terceros de las instalaciones de procesamiento de información organizacional o la adición de productos o servicios a dichas instalaciones deben cubrir todos los requisitos de seguridad necesarios.

A.3Gestión de Riesgos

A.3.1 Responsabilidad por Activos

Objetivo: Mantener la protección apropiada de los activos de la organización. Pasos:

1	Inventario de activos	Control: Se elaborara y mantendrá un inventario de todos los activos importantes que sean claramente identificados.
2	Propiedad de los activos	Control: Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad d un aparte designada de la organización.
3	Uso aceptable de los activos	Control: Se deben de identificar, documentar e implementar las reglas para el uso aceptable de los activos de información asociados con las instalaciones de procesamiento de información.

A.3.2 Clasificación de la Información

Objetivo: Asegurar que los activos de información reciban un nivel de protección adecuado. Pasos:

1	Guías de clasificación	Control: La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad parala organización.
2	Etiquetado y tratamiento de la información	Control: Se definirá e implementara un conjunto de procesamientos apropiados para etiquetar y manejar información de conformidad con el esquema de clasificación adoptado por la organización.

A.4.Seguridad en Recursos Humanos

A.4.1 Previo al Empleo

Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa. Pasos:

1	Roles y responsabilidades	Control: Se definirán y documentarán los roles y las responsabilidades de los empleados, contratista y usuarios externos en concordancia con la política de seguridad de la información de la organización
2	Investigación	Control: Se debe hacer un chequeo y verificación de informaciones anteriores de todos los candidatos para empleos, contratistas y personal externo, en concordancia con las leyes, regulaciones y ética; y proporcional a los requisitos del negocio, la clasificación de la información a ser accedida y a los riesgos percibidos.
3	Términos y condiciones de la relación laboral	Control: Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad comoparte de los términos y condiciones iníciales de su empleo en donde se señalara la responsabilidad del empleado en cuando a la seguridad de la información.

A.4.2 Durante el empleo

Objetivo: Asegurar que todos los empleados, contratistas y usuarios externos sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que

estén preparados para aplicar la política de seguridad de la organización en el curso de trabajo normal y reducir el riesgo de error humano. Pasos:

1	Gestión de responsabilidades	Control: La gerencia debe requerir a los empleados, contratistas y a los usuarios externos aplicar la seguridad en concordancia con las políticas y procedimientos de la organización.
2	Concientización, educación y entrenamiento en la seguridad de información	Control: Todos los empleados de la organización y, donde sea relevante, contratistas y usuarios externos deben recibir una adecuada concientización, entrenamiento y actualizaciones regulares en los procesos y políticas organizacionales, como acciones relevantes de su función laboral.
3	Proceso disciplinario	Control: Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad.

A.4.3 Finalización o cambio de empleo

Control: Asegurar que los empleados, contratistas y usuarios externos dejen o cambien de organización de una forma ordenada. Pasos:

1	Responsabilidades de finalización	Control: Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados tan pronto como sea posible.
2	Devolución de activos	Control: Todos los empleados, contratistas y usuarios externos deben realizar la devolución de los activos de la organización que están en su posesión cuando termine su empleo, contrato o acuerdo.
3	Retiro de los derechos de acceso.	Control: El derecho de acceso a la información y a las instalaciones del procesamiento de información, que se le otorga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios.

A.5. Seguridad Física y del Entorno

A.5.1 Áreas Seguras

Objetivo: Prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización. Pasos:

1	Seguridad física perimetral	Control: Las organizaciones usarán perímetros de seguridad (barreras como paredes, puertas con control de entrada por tarjeta o recepciones) para proteger áreas que contienen información e instalaciones de procesamiento de información.

2	Controles físicos de entradas	Control: Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que únicamente personal autorizado pueda ingresar.
3	Seguridad de oficinas, despachos y recursos	Control: Se deben designary mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.
4	Protección contra amenazas externas y ambientales	Control: Se deben designar y mantener protección física contra daños por fuego, inundación, terremoto, explosión, manifestación civil y otras formas de desastre natural o realizado por el hombre.
5	El trabajo en las áreas seguras	Control: Se debe designar y mantener protección física y pautas para trabajar en áreas seguras.
6	Áreas de carga, descarga y acceso público	Control: Las áreas de carga, descarga y acceso público y otras áreas donde las personas tengan acceso deben controlarse y, cuando sea posible, aislarse de las instalaciones de procesamiento de información para evitar un acceso no autorizado.

A.5.2 Seguridad de los Equipos

Objetivo: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización. Pasos:

1	Ubicación y protección de equipos	Control: El equipamiento será ubicado o protegido para reducir los riesgos de amenazas, peligros ambientales y oportunidades de acceso no autorizado.
2	Suministro eléctrico	Control: El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el fallo en el suministro eléctrico.
3	Seguridad del cableado	Control: Se protegerá el cableado de energía y telecomunicaciones que transportan datos o respaldanservicios de información frente a interpretaciones o daños.
4	Mantenimiento de equipos	Control: El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad
5	Seguridad de equipos fuera de los locales de la organización	Control: Se debe aplicar seguridad al utilizar equipamiento para procesar información tomando en cuenta los diferentes riesgos en los que se incurre.
6	Seguridad en el Re-uso o eliminación de equipos	Control: Todos los equipos que contienen almacenamiento de datos deben ser revisados con el finde asegurar que los datos sensibles y los software con licencia han sido removidos o sobrescritos ante de desecharlos o reutilizarlos.
7	Retiro de propiedad	Control: Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.

A.6 Gestión de Comunicaciones y Operaciones

A.6.1 Procedimientos y Responsabilidades de Operación

Objetivo: Asegurar la operación correcta y asegura de los recursos de procesamiento de información. Pasos:

1	Documentación de procedimientos operativos	Control: Los procedimientos operativos deberán estar documentados, mantenidos y estar disponibles a todos los usuarios que lo requieran.
2	Gestión de cambios	Control: Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información
3	Segregación de tareas	Control: Se segregarán las obligaciones y las áreas de responsabilidad con el fin de reducir las oportunidades de modificaciones no autorizadas o mal uso de los activos de la organización.
4	Separación de las instalaciones de desarrollo, prueba y operación	Control: Se separarán las instalaciones de desarrollo, prueba y operación con el fin de reducir el riesgo de acceso no autorizado o cambios en el sistema operacional.

A.6.2 Gestión de Entrega de Servicios Externos

Objetivo: Implementar y mantener un nivel apropiado de información y servicios de entrega en concordancia con los acuerdos de servicios de entrega por parte de terceros que participan con la empresa. Pasos:

1	Entrega de servicios	Control: Debemos asegurarnos que los controles de seguridad, las definiciones de servicio y los niveles de entrega incluidos en el acuerdo de servicios externos sean implementados, estén operativos y sean mantenidos por el personal externo.
2	Monitoreo y revisión de los servicios externos	Control: Los servicios, reportes y registros provistos por terceras partes deben ser monitoreados y revisados regularmente. Igualmente, se deben de llevar a cabo auditorias con regularidad.
3	Gestión de cambios de los servicios externos	Control: Se debe manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de la política de seguridad de información, procedimientos y controles,tomando en cuenta la criticidad de los sistemas de negocio y procesos envueltos en la reevaluación.

A.6.3 Planificación y Aceptación del Sistema

Objetivo: Minimizar el riesgo de fallas de los sistemas. Pasos:

1	Gestión de la capacidad	Control: Se monitorearán las demandas de capacidad u se harán las proyecciones de futuros requisitos de capacidad para asegurar el

		desarrollo requerido por el sistema.
2	Aceptación del sistema	Control: Se establecerán los criterios de aceptación para nuevos sistemas de información, actualizaciones y nuevas versiones y se llevarán a cabo pruebas adecuadas del sistema antes de la aceptación.

A.6.4 Protección contra Software Malicioso

Objetivo: Proteger la integridad del software y de la información. Pasos:

1	Controles contra software malicioso	Control: Para ofrecer protección frente a software malicioso, se implementarán controles de detección, prevención y procedimientos adecuados de toma de conciencia con los usuarios.
2	Controles contra software móvil	Control: Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este operar de acuerdo a una política de seguridad clara y definida, Igualmente, se debe prevenir la ejecución de código móvil no autorizado.

A.6.5 Gestión Interna de Respaldo y Recuperación

Objetivo: Mantener la integridad y disponibilidad del procesamiento de información y servicios de comunicación. Pasos:

1	Recuperación de la información	Control: Se obtendrán y probarán las copias de recuperación y respaldo de información y software regularmente en concordancia con la política acordada.

A.6.6 Gestión de Seguridad de Redes

Objetivo: Asegurar la salvaguarda de información en las redes y la protección de la infraestructura de soporte. Pasos:

1	Controles de red	Control: Se implementará un conjunto de controles para lograr y mantener la seguridad en las redes, y mantener la seguridad de los sistemas y aplicaciones usuarios de la red, incluyendo la información en tránsito.
2	Seguridad de los servicios de red	Control: Se deben identificar e incluir en cualquier acuerdo de servicio de red los aspectos de seguridad, niveles de servicio y requisitos de gestión, así estos servicios sean provistos interna o externamente.

A.6.7 Utilización y Seguridad de los Medios de Información

Objetivo: Prevenir daños, modificaciones o destrucciones a los activos e interrupciones de las actividades del negocio. Pasos:

1	Gestión de medios removibles	Control: Deben de existir procedimientos para la gestión de medios removibles.
2	Eliminación de medios	Control: Se eliminarán los medios de forma segura cuando ya no se necesiten, utilizando procedimientos formales.
3	Procedimientos de manipulación de la información	Control: Se establecerán procedimientos para el manejo y almacenamiento de la información con el fin de proteger dicha información de divulgaciones no autorizadas o su mal uso que puedan afectar a la empresa.
4	Seguridad de la documentación de sistemas	Control: La documentación de los sistemas se protegerá de accesos no autorizados en la empresa.

A.6.8 Intercambio de Información

Objetivo: Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas. Pasos:

1	Políticas y procedimientos para el intercambio de información	Control: Se deben establecer políticas y controles para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación.
2	Acuerdos de intercambio	Control: Se deben de establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
3	Seguridad de medios físicos en tránsito	Control: Los medios a ser transportados deberán ser protegidos de acceso no autorizado, mal uso o corrupción durante su transporte fuera de los límites físicos de la empresa.
4	Seguridad del correo electrónico	Control: La información contenida en correos electrónicos debe ser protegida apropiadamente para no ser divulgada y afectar el contenido..
5	Seguridad en los sistemas de información de negocio	Control: Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información del negocio.

A.6.9 Servicios de comercio electrónico

Objetivo: Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso. Pasos:

1	Seguridad en comercio electrónico	Control: El comercio electrónico será protegido frente a actividades fraudulentas, controversias contractuales y divulgación o

		modificación de información
2	Seguridad en las transacciones en línea	Control: La información contenida en las transacciones en línea debe ser protegida para prevenir transmisiones incompletas, rutas incorrectas, alteración no autorizada de mensajes, o duplicación no autorizada de mensajes.
3	Información disponible públicamente	Control: Se protegerá la integridad de la información públicamente disponible para prevenir modificaciones no autorizadas.

A.6.10 Monitoreo

Objetivo: Detectar actividades de procesamiento de información no autorizadas. Pasos:

1	Registro de auditoria	Control: Se deben producir y guardar, por un periodo acordado, los registros de auditoria que registran las actividades de los usuarios, excepciones y eventos de seguridad, con el fin de asistir a investigaciones futuras y al monitoreo del control de acceso.
2	Uso del sistema demonitoreo	Control: Se deben establecer procedimientos para monitoreas las instalaciones de procesamiento de información y los resultados del monitoreo de actividades debe ser revisados regularmente.
3	Protección de la información de registro	Control: Las instalaciones e información de registro deben ser protegidas contra acceso forzado y no autorizado.
4	Registros de administrador y operador	Control: Las actividades del administrador y operaciones deben ser registradas.
5	Registros con faltas	Control: Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas.
	Sincronización de reloj	Control: Los relojes de todos los sistemas relevantes de procesamiento de información dentro de la organización deben estar sincronizados con una fuente de tiempoactual acordado por la empresa.

A.7. Control de Accesos

A.7.1 Requisitos de Negocio para el Control de Accesos

Objetivo: Controlar los accesos a la información. Pasos:

1	Política de control de accesos	Control: Se debe establecer, documentar y revisad una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.

A.7.2 Gestión de Acceso de Usuarios

Objetivo: Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información. Pasos:

1	Registros de usuarios	Control: Habrá un procedimiento de registro y anulación formal de

		usuarios para otorgar y eliminar el acceso a todos los servicios y sistemas información
2	Gestión de privilegios	Control: Se restringirá y controlará la asignación y uso de privilegios.
3	Gestión de contraseñas de usuario	Control: Se controlará la asignación de contraseñas a través de un proceso de gestión formal.
4	Revisión de los derechos de acceso de los usuarios	Control: La gerencia conducirá un proceso formal y de manera periódica para revidar los derechos de acceso del usuario.

A.7.3 Responsabilidades de los Usuarios

Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento. Pasos:

1	Uso de contraseñas	Control: Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
2	Equipo informático de usuario desatendido	Control: Se exige al usuario que asegure protección adecuada a un equipo desatendido.
3	Política de pantalla y escritorio limpio	Control: Se debe adoptar una política de escritorio limpio para papeles y dispositivos de almacenamiento removibles. Igualmente, se debe adoptar una política para las instalaciones de procesamiento de información.

A.7.4 Control de Acceso a la Red

Objetivo: Prevenir el acceso no autorizado a los servicios de red. Pasos:

1	Política de uso de los servicios de la red	Control: Los usuarios deben tener acceso directo únicamente a los servicios uso está específicamente autorizado.
2	Autenticación de usuarios para conexiones externas	Control: Deben usarse apropiados métodos de autenticación para controlar el acceso de usuarios remotos.
3	Autenticación de equipos en la red	Control: Se debería equipos con identificación automática para autentificar conexiones desde ubicaciones y equipos específicos
4	Protección para la configuración de puertos y diagnóstico remoto	Control: Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes.
5	Segregación en las redes	Control: Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes.
6	Control de conexión a las redes	Control: La capacidad de conexión de los usuarios de redes compartidas, especialmente aquellas que se extienden fuera de las fronteras de la organización, debe restringirse de conformidad con la políticade control de acceso y los requisitos de las aplicaciones de negocio.
7	Control de enrutamiento en la red	Control: Se deben implementar controles de *ruteo* para asegurar que las conexiones de computadora y los flujos de información no violen la política de control de acceso de las aplicaciones de negocios

A.7.5 Control de Acceso al Sistema Operativo

Objetivo: Prevenir accesos no autorizados a los sistemas operativos. Pasos:

1	Procedimientos seguros de conexión	Control: Se usará un proceso de registro de conexión (login) seguro para acceder a los servicios de información.
2	Identificación y autenticación del usuario	Control: Todos los usuarios tienen un identificador único para su uso propio y exclusivo para sus actividades y debe elegirse una técnica de autenticación adecuada para sustentar la identidad del usuario.
3	Sistema de gestión de contraseñas	Control: Sistemas de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraseñas de calidad.
4	Uso de los programas utilitarios del sistema.	Control: Se debe registrar y controlar firmemente el uso de programas utilitarios que puedan ser capaces de forzar el sistema y los controles de aplicación.
5	Desconexión automática de terminales	Control: Las sesiones inactivas deben cerrarse luego de un periodo definido de inactividad.
6	Limitación del tiempo de conexión	Control: Se usará restricciones de tiempos de conexión para ofrecer seguridad adicional para las aplicaciones de alto riesgo.

A.7.6 Control de Acceso a las Aplicaciones e Información

Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas. Pasos:

1	Restricción de acceso a la información	Control: El acceso a las funciones de información y de aplicación por usuarios y personal de soporte serán restringidos conla política de control de acceso.
2	Aislamiento de sistemas sensibles	Control: Los sistemas sensibles tendrán un ambiente de cómputo dedicado.

A.7.7 Informática Móvil y Teletrabajo

Objetivo: Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de teletrabajo. Pasos:

1	Informática y comunicaciones móviles	Control: Se pondrá en práctica una política formal y se adoptarán los controles adecuados para protegerse frente a los riesgos de trabajar con puntos de computadores móviles y medios de comunicación.
2	Teletrabajo	Control: Se desarrollarán e implementaran políticas, procedimientos y estándares para las actividades de teletrabajo.

A.8. Adquisición de sistemas de información, desarrollo y mantenimiento

A.8.1 Requisitos de Seguridad de los Sistemas de Información

Objetivo: Garantizar que la seguridad esté incluida dentro de los sistemas de información.

Pasos:

1	Análisis y especificación de los requisitos de seguridad	Control: Los requisitos de negocios para nuevos sistemas, o ampliaciones de los sistemas existentes, especificarán los requisitos de control

A.8.2 Proceso Correcto en Aplicaciones

Objetivo: Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones. Pasos:

1	Validación de los datos de entrada	Control: Se validará el ingreso de datos a los sistemas de aplicación para asegurar que sean correctos y adecuados.
2	Control del proceso interno	Control: Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados.
3	Integridad de mensajes	Control: Se deben identificar requisitos para la autenticación y protección de la integridad de mensajes. Igualmente, se deben implementar e identificar controles apropiados.
4	Validación de los datos de salida	Control: Los datos de salida de una aplicación se validarán para garantizar que el procesamiento de la información almacenada sea correcto y adecuado a las circunstancias.

A.8.3 Controles Criptográficos

Objetivo: Proteger la confidencialidad, autenticidad o integridad a través de medios Criptográficos. Pasos:

1	Política de uso de los controles criptográficos	Control: Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.
2	Gestión de claves	Control: Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnica criptográfica dentro de la organización.

A.8.4 Seguridad de los Activos del Sistema

Objetivo: Asegurar la seguridad de los archivos del sistema. Pasos:

1	Control del software en producción	Control: Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales.
2	Protección de los datos de prueba	Control: Se protegerán y controlarán los datos de prueba los cuales

	del sistema	debe ser seleccionado cuidadosamente.
3	Control de acceso a la librería de programas fuente	Control: El acceso a las librerías de programas fuente debe ser restringido.

A.8.5 Seguridad en los Procesos de Desarrollo y Soporte

Objetivo: Mantener la seguridad del software de aplicación y la información. Pasos:

1	Procedimientos de control de cambios	Control: La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios.
2	Revisión técnica de los cambios en el sistema operativo	Control: Cuando los sistemas operativos son cambiados, se deben de revidar y probar las aplicaciones críticas de negocio con el fin de asegurar que no existan impactos adversos en las operaciones o seguridad de la organización.
3	Restricciones en los cambios a los paquetes de software	Control: No se debe fomentar las modificaciones en los paquetes. Se debe limitar a cambios necesarios estos cambios deben ser estrictamente controlados.
4	Fuga de información	Control: Se deben de prevenir las oportunidades de fuga de información.
5	Desarrollo externo del software	Control: La organización debe supervisar y monitorear el desarrollo externo de software.

A.8.6 Gestión de Vulnerabilidades Técnicas

Objetivo: Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas. Pasos:

1	Control de vulnerabilidades técnicas	Control: Se debe obtener información a tiempo sobre las vulnerabilidades técnicas de los sistemas de información que se utilizan. La exposición de la organización a tales vulnerabilidades debe ser evaluada y se debe tomar medidas apropiadas asociadas al riesgo.

A.9.Gestión de Incidentes en la Seguridad de Información

A.9.1 Reportando Eventos y Debilidades en la Seguridad de Información

Objetivo: Asegurar que los eventos y debilidades en la seguridad de información asociados con los sistemas de información sean comunicados de manera tal que permitan tomar una acción correctiva a tiempo. Pasos:

1	Reportando eventos de la	Control: Los eventos en la seguridad de información deben ser

	seguridad de información	reportados los más rápido posibles a través de canales apropiados.
2	Reportando debilidades de seguridad	Control: Todos los empleados, contratistas o personal externo usuario de los sistemas y servicios de información, deben estar obligados de notar y reportar cualquier debilidad en la seguridad de los sistemas y servicios.

A.9.2 Gestión de los Incidentes y Mejoras en la Seguridad de Información

Objetivo: Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información. Pasos:

1	Responsabilidades y procedimientos	Control: Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de información.
2	Aprendiendo de los incidentes en la seguridad de información	Control: Deben existir mecanismos que habiliten que los tipos, volúmenes y costos de los incidentes en la seguridad de información sean cuantificados y monitoreados.
3	Recolección de evidencia	Control: Cuando exista una acción de seguimiento contra una persona u organización, luego de que un incidente en el sistema de información involucre una acción legal (civil o criminal), se debe de recolectar, retener y presentar evidencia conforme con las reglas dentro de la jurisdicción.

A.10 Gestión de la Continuidad del Negocio

A.10.1 Aspectos de la Gestión de Continuidad del Negocio en la Seguridad de Información

Objetivo: Neutralizar las interrupciones a las actividades del negocio y proteger los procesos críticos del negocio de los efectos de fallas mayores o desastres en los sistemas de información y asegurar su reanudación oportuna. Pasos:

1	Incluyendo la seguridad de la información en la gestión de la continuidad del negocio.	Control: Se deben de establecer procedimientos y responsabilidades de gestión con el fin de asegurar una respuesta rápida, efectiva y ordenada ante incidentes en la seguridad de la información.
2	Continuidad del negocio y evaluación de riesgos	Control: Los eventos que pueden causar interrupciones en los procesos del negocio deben ser identificados en los procesos del negocio así comolas probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
3	Desarrollando e implementado planes de continuidad que incluyen	Control: Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al

	la seguridad de la información.	nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.
4	Marco de planificación de la continuidad del negocio	Control: Un simple marco de los planes de continuidad del negocio debe ser mantenido para asegurar que todos los planes sean consistentes, que anexen consistentemente los requisitos de seguridad de la información, para identificar prioridades reprueba y mantenimiento.
5	Probando, manteniendo y reevaluando los planes de continuidad del negocio	Control: Los planes de continuidad del negocio deben ser probados y actualizados regularmente con el fin de asegurar que se encuentren actuales y que sean efectivos.

A11 Cumplimiento

A.11.1 Cumplimiento de los Requisitos Legales

Objetivo: Evitar los incumplimientos de cualquier ley civil o penal, requisito, reglamento, regulación u obligación contractual, y de cualquier requisito de seguridad. Pasos:

1	Identificación de la legislación aplicable	Control: Se definirán y documentarán explícitamente todos los requisitos legales, regulatorios y contractuales relevantes y se deben mantener actualizados cada sistema de información y la organización.
2	Derechos de propiedad intelectual	Control: Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales en el uso de material con respecto a derechos de propiedad intelectual y uso de productos de software propietario.
3	Salvaguarda de los registros de la organización	Control: Se protegerán los registros importantes de la organización frente a pérdidas, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.
4	Protección de los datos u privacidad de la información	Control: Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales.
5	Prevención en el mal uso de la instalaciones de procesamiento de la información	Control: Los usuarios deben ser disuadidos de utilizar las instalaciones del procedimiento de información para propósitos no autorizados.
6	Regulación de los controles criptográficos	Control: Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos.

A.11.2 Cumplimiento con las Políticas y Estándares de Seguridad y del Cumplimiento Técnico

Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales. Pasos:

1	cumplimiento con los estándares y la política de seguridad	Control: Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro e sus áreas de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de las políticas y estándares de seguridad.
2	Comprobación del cumplimiento técnico	Control: Debe verificarse regularmente de la implementación de normas de seguridad en los sistemas de información.

A.11.3 Consideraciones sobre la Auditoria de Sistemas

Objetivo: Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema. Pasos:

1	Controles de auditoría de sistemas	Control: Se planificarán cuidadosamente las auditorias de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos de negocio.
2	Protección de las herramientas de auditoría de sistemas	Control: Se protegerá el acceso a las herramientas de auditoría del sistema para prevenir cualquier posible mal uso o daño.

ANEXO C

PROYECTO SGSI Alcance del Proyecto		
SGSI 002_1	**Versión de la Plantilla: 1.0.0**	**Fecha:**
Jefe de Proyecto		
Fecha	13/02/2014	
Objetivos del Proyecto	El objetivo es asegurar la confiabilidad de la información y evitar su uso indebido que podría ocasionar serios problemas en los bienes y/o servicios que ofrece la entidad a la ciudadanía. Para ello se ha identificado los activos, tecnología, procesos, productos, aplicaciones y entorno físico controlando el alcance, tiempo y costo, manteniendo la calidad y límites que tiene la Entidad Pública para su implementación.	
Justificación del Proyecto	Es necesario proteger toda información considerada de valor que pudiera tener el riesgo de ser atacado o sustraído.	
Alcance del Proyecto	La entidad desarrollará, implementará, operará, monitoreará, revisará, mantendrá y continuará la mejora del Sistema de Gestión de Seguridad de la Información, para lograrlo documentará las actividades y riesgos. Las Políticas de Seguridad de la Información son de aplicación para todos los trabajadores, proveedores y terceros que tengan acceso a la información. Esta sección se complementa con el Documento de Alcance y Límites del Sistema de Gestión de Seguridad de la Información. La política de un Sistema de Gestión de la Seguridad de la Información, en términos de las características del negocio, la organización, su localización, activos y tecnología deberá tener la siguiente información: • Incluir un marco para establecer sus objetivos y establecer un sentido total de dirección y principios para acción con miras a la seguridad de la información. • Considerar los requisitos del negocio, legales o regulatorios y obligaciones de seguridad contractual. • Establecer el contexto estratégico organizacional y la gestión del riesgo en el cual tiene lugar el establecimiento y mantenimiento el Sistema de Gestión de Seguridad de la Información. • Establece criterios frente a los cuales se evaluará el riesgo y se definirá la estructura de evaluación del riesgo.	
Entregables del Proyecto	Los entregables del proyecto son los siguientes: • Documento de Políticas del Sistema de Gestión de Seguridad de la Información. • Definición de la Organización. • Definición del Alcance. • Estructura de Desglose de Trabajo (EDT). • Estructura de Desglose de Riesgo (RBS). • Identificación de Activos. • Plan de Gestión de Tiempo. • Plan de Gestión de Costos. • Plan de Gestión de las Comunicaciones. • Plan de Gestión de Riesgos. • Acciones de Mitigación de Riesgos. • Listado de Riesgos. • Matriz de Valoración de Riesgos. • Enunciado del Cronograma y Actualización. • Implementación Lista de Actividades • Implementación de Acciones de Mitigación de Riesgos • Implementación de Listado de Riesgos • Implementación de la Matriz de riesgos • Informe de Plan de Proyecto. • Informe de Revisión de Riesgos. • Informe de Actividades. • Ficha de Sugerencia y Mejora.	

	• Informe de Cierre del Proyecto. • Acta de Transferencia de las Actividades del Proyecto del SGSI.
Propósito del Producto	La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada es el propósito de la implementación del SGSI. Es importante en el creciente ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo electrónico o por medios electrónicos, mostrada en video o hablada en conversación. La seguridad de la información protege este amplio rango de amenazas y minimiza los daños de la organización y maximiza el retorno de la inversión.
Descripción del Producto	La implementación del SGSI implica la aplicación de un conjunto de lineamientos que establecen el marco de referencia sobre el cual se sustenta las normas y/o procedimientos sobre la actuación del personal en relación a los recursos de la organización que estén relacionados a la información, enunciando lo que deseamos proteger y el por qué hacerlo, sin llegar a ser una descripción técnica. Las políticas descritas son una invitación a los miembros de la organización a reconocer que la información es un activo así como un motor de intercambio y desarrollo en el ámbito de las funciones que desempeña en la organización. Todos los miembros tienen que tener conciencia y vigilar el uso y limitaciones de la información que son críticos que requieren atención y la aplicación de políticas de la seguridad de la información.
Objetivos del Producto	La entidad elaborará policitas y/o lineamientos con la finalidad de asegurar la confiabilidad de la información, y evitar su uso indebido, lo cual podría ocasionar serios problemas en los bienes y servicios que ofrece a la ciudadanía. La entidad considera que estas políticas por sí solas no constituyen una garantía para la seguridad de la información, sino depende del esfuerzo de todo el personal que labora en la organización para velar por su cumplimiento, por esta razón se debe utilizar una metodología que ayude a orientar la aplicación de las políticas la información considerada de valor para la organización. El ámbito de aplicación de la SGSI debe estar organizado en base a las siguientes políticas: • Políticas Generales de la Organización • Políticas sobre Activos • Políticas sobre Recursos Humanos • Políticas sobre Seguridad Física y del Entorno • Políticas sobre Comunicaciones y Operaciones • Políticas sobre Control de Accesos • Políticas sobre Adquisición de Sistemas de Información, Desarrollo y Mantenimiento • Políticas sobre Incidentes en la Seguridad de Información • Políticas sobre Continuidad del Negocio • Políticas sobre Cumplimiento

APROBACION DEL COMITÉ

No hay ninguna razón para rechazar el proyecto

Miembros del Proyecto	Nombre y Apellidos	Firmas
Secretaria General		
Jefatura de Recursos Logística		
Jefatura de Recursos Humanos		
Jefatura de Tecnologías de la		
Jefatura de Asesoría Jurídica		

ANEXO D

PROYECTO SGSI Listado de Diagnostico				
SGSI 005	**Versión de la Plantilla: 1.0.0**	**Fecha:**		
Ítems		**Si**	**No**	**No aplicable**
Existen procedimientos definidos y aprobados relativos para la seguridad de información.		Si		
Hay procedimientos para la seguridad de información dentro de la empresa.		Si		
Hay roles y responsabilidades definidos para a los empleados implicados en la seguridad de la información.			No	
Hay inventarios de los activos de información			No	
Los inventarios cuentan con una adecuada documentación dentro de la institución.			No	
Se dispone de una clasificación respecto a los activos de la información.			No	
Existen procedimientos de etiquetado de los activos de información dentro de la empresa			No	
Se tienen definidas responsabilidades y roles al personal			No	
Se tiene en cuenta una adecuada política para la selección de personal			No	
Hay confidencialidad y responsabilidades en los contratos con los empleados de la institución.		Si		
Se imparte la formación y concientización adecuada respecto a la seguridad de información en la empresa			No	
Hay reportes de incidentes de forma detallada de los activos de información			No	
Existen controles para protegerse frente al acceso de personal no autorizado a las instalaciones y equipos dentro de la empresa			No	
En las áreas u oficinas existen controles adicionales al personal propio y ajeno			No	
La ubicación de los equipos está adecuadamente en instalaciones seguras para minimizar accesos innecesarios		Si		
Existen medidas frente a fallos en la alimentación eléctrica		Si		
Existe medidas de seguridad en el cableado frente a daños e intercepciones que afecten a los activos			No	
Existe la disponibilidad, confidencialidad e integridad de todos los activos			No	
Existe algún tipo de seguridad en los equipos ubicados en el exterior de la empresa.		Si		
Existen procedimientos identificados respecto a la seguridad y correctamente documentados			No	
Hay procedimientos para controlar cambios en los equipos en las áreas u oficinas.			No	
Existen medidas establecidas para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad			No	
Existe algún método para reducir el mal uso o deliberado en los activos			No	
Existen controles contra software maligno o virus		Si		
Realizan copias de seguridad de la información esencial para la empresa			No	
Existe seguridad en la documentación			No	
Existen medidas de seguridad en los correos electrónicos de la empresa			No	
Se han establecido e implantado medidas correctivas y preventivas a los activos de información			No	
Existe una política de control de accesos los pc's de las oficinas			No	
Existe el uso de contraseñas para los empleados y usuarios		Si		

Se protege el acceso a los equipos no utilizados por cierto tiempo	Si		
Existe un control en la conexión de las redes dentro de la institución		No	
Existe seguridad en las aplicaciones de software	Si		
Existen seguridad en los archivos más importantes para la empresa	Si		
Existe seguridad en los procesos de desarrollo y soporte		No	
Existen procesos para la gestión de la continuidad del negocio de la empresa del estado.		No	

ANEXO E

Formato de Listado de Categoría de Datos

Codigo del Activo	Nombre del Activo	Descripción del Activo	Tipo de Información	Entrada/Salida/ Otro	Responsable del activo	Área del responsable del activo	Cargo del responsable del activo	Lugar de procedencia	Medio o formato de almacenamiento	Observaciones
001DA	Documentos de Procesos	Documentos de Procesos	Tangible	Salida	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Impreso	
002DA	Memorandos	Memorandos	Tangible	Salida	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Impreso	
003DA	Informes	Informes	Tangible	Salida	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Impreso	
004DA	Oficios	Oficios	Tangible	Salida	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Impreso	
005DA	Actas	Actas	Tangible	Salida	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Impreso	
006DA	Contratos	Contratos	Tangible	Salida	Jefe de Oficina de Administración	Unidad Órganica de la Institucion	Jefe de Oficina de Administración	Unidad Órganica de la Institucion	Impreso	
007DA	Facturas	Facturas	Tangible	Salida	Jefe de Oficina de Administración	Unidad Órganica de la Institucion	Jefe de Oficina de Administración	Unidad Órganica de la Institucion	Impreso	
008DA	Guías y reglamentos	Guías y reglamentos	Tangible	Entrada	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Digital	
009DA	Expedientes	Expedientes	Tangible	Entrada	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Impreso	
010DA	Notificaciones	Notificaciones	Tangible	Salida	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Digital	
011DA	Papeles de Trabajo	Papeles de Trabajo	Tangible	Entrada	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Digital	
012DA	Manuales de usuario	Manuales de usuario	Tangible	Entrada	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Director o Jefe de Oficina	Unidad Órganica de la Institucion	Digital	

Formato de Listado de Categoría de Software

Codigo de Activo	Nombre del Activo	Descripción del Activo	Sub Categoría	Responsable del activo	Área del responsable del activo	Cargo del responsable del activo	Clasificacion del software	Área y Responsable del Mantenimiento	Observaciones
001SW	Windows	Windows	2.2. Paquetes de Software	Encargado de Tecnologias de Informacion	Encargado de Tecnologias de Informacion	Presidente de la Unidad de Tecnologias de Informacion	1.1 procesador Intel Core 2 Quad Q9650 de 3.0 Ghz, disco duro de 500 GB de 7200 RPM SATA o superior, unidad de c y d	Unidad de Tecnologías de la Información	
002SW	Linux	Linux	2.1. Sistemas Operativos	Encargado de Tecnologias de Informacion	Encargado de Tecnologias de Informacion	Presidente de la Unidad de Tecnologias de Informacion	1.2 procesador: Intel Core2 Duo™ 1.83GHz, AMD Athlon™ 64 X2 3800+, AMD Turion™ x2 ó superiores. Memoria: 1024MB de RAM, unidad de almacenamiento c y d	Unidad de Tecnologías de la Información	
003SW	Aplicativo 1	Aplicativo 1	2.2. Paquetes de Software	Director de la Institucion	Dirección de la Institucion	Director de la Institucion	1.2 procesador: Intel Core2 Duo™ 1.83GHz, AMD Athlon™ 64 X2 3800+, AMD Turion™ x2 ó superiores. Memoria: 1024MB de RAM, unidad de almacenamiento c y d	Área Usuaria y Sub Dirección de Desarrollo de Proyectos	
004SW	Aplicativo 2	Aplicativo 2	2.2. Paquetes de Software	Director de la Institucion	Dirección de la Institucion	Director de la Institucion	1.1 procesador Intel Core 2 Quad Q9650 de 3.0 Ghz, disco duro de 500 GB de 7200 RPM SATA o superior, unidad de c y d	Área Usuaria y Sub Dirección de Desarrollo de Proyectos	
005SW	Aplicativo 3	Aplicativo 3	2.2. Paquetes de Software	Director de la Institucion	Dirección de la Institucion	Director de la Institucion	1.1 procesador Intel Core 2 Quad Q9650 de 3.0 Ghz, disco duro de 500 GB de 7200 RPM SATA o superior, unidad de c y d	Área Usuaria y Sub Dirección de Desarrollo de Proyectos	
006SW	Aplicativo 4	Aplicativo 4	2.2. Paquetes de Software	Directora de una area	Dirección de la area	Directora de la area	1.1 procesador Intel Core 2 Quad Q9650 de 3.0 Ghz, disco duro de 500 GB de 7200 RPM SATA o superior, unidad de c y d	Área Usuaria y Sub Dirección de Desarrollo de Proyectos	
007SW	Tribunal de Contrataciones del Estado	Tribunal de Contrataciones del Estado	2.3. Software de Aplicación de Oficina	Presidenta del Tribunal de Contrataciones del	Tribunal de Contrataciones del Estado	Presidenta del Tribunal de Contrataciones del Estado	1.1 procesador Intel Core 2 Quad Q9650 de 3.0 Ghz, disco duro de 500 GB de 7200 RPM SATA o superior, unidad de c y d	Área Usuaria y Sub Dirección de Desarrollo de Proyectos	
008SW	Antivirus	Antivirus	2.2. Paquetes de Software	Encargado de Tecnologias de Informacion	Encargado de Tecnologias de Informacion	Presidente de la Unidad de Tecnologias de Informacion	1.2 procesador: Intel Core2 Duo™ 1.83GHz, AMD Athlon™ 64 X2 3800+, AMD Turion™ x2 ó superiores. Memoria: 1024MB de RAM, unidad de almacenamiento c y d	Unidad de Tecnologías de la Información	
009SW	Microsoft Visio	Microsoft Visio	2.2. Paquetes de Software	Encargado de Tecnologias de Informacion	Encargado de Tecnologias de Informacion	Presidente de la Unidad de Tecnologias de Informacion	1.2 procesador: Intel Core2 Duo™ 1.83GHz, AMD Athlon™ 64 X2 3800+, AMD Turion™ x2 ó superiores. Memoria: 1024MB de RAM, unidad de almacenamiento c y d	Unidad de Tecnologías de la Información	
010SW	Oracle	Oracle	2.2. Paquetes de Software	Encargado de Tecnologias de Informacion	Encargado de Tecnologias de Informacion	Presidente de la Unidad de Tecnologias de Informacion	1.1 procesador Intel Core 2 Quad Q9650 de 3.0 Ghz, disco duro de 500 GB de 7200 RPM SATA o superior, unidad de c y d	Unidad de Tecnologías de la Información	

Formato de Listado de Categoría de Activos Físicos

Codigo del Activo	Nombre del Activo	Descripción del Activo	Sub Categoría	Localización (Edifico, Área, Departamento)	Responsable del activo	Área del responsable del activo	Cargo del responsable del activo	Dirección IP	Clasificación de hardware	Horas de Funcionamiento	Equipos de Oficina	Entrada/Salida de Activos Físicos	Área del Mantenimiento del activo	Responsable del Mantenimiento del activo	Tipo de conexión (área o	Tipo de Acceso	Medios de Comunicación	Observaciones
001ACT	PC	PC	3.2. Hardware Portátil	1.2 Secretaria General	Director de la Institucion	Dirección de la Institucion	Director de la Institucion	1.1 Ip privadas		8 horas	Si		Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información	LAN	Usuario	Cable	
002ACT	Hardware Portátil	Hardware Portátil	3.2. Hardware Portátil	1.2 Secretaria General	Director de la Institucion	Dirección de la Institucion	Director de la Institucion	1.1 Ip privadas		8 horas	Si	Si	Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información	LAN	Usuario	Cable	
003ACT	Impresora	Impresora	3.3. Equipos de Oficina	1.3 Tecnologias de Informacion			Jefaturas de la Empresa				Si		Soporte Tecnico	Soporte Tecnico		Usuario	Cable	
004ACT	Copiadoras	Copiadoras	3.3. Equipos de Oficina	1.2 Secretaria General			Jefaturas de la Empresa				Si		Soporte Tecnico	Soporte Tecnico		Usuario	Cable	
005ACT	Teléfonos	Teléfonos	3.3. Equipos de Oficina	1.1 Recursos Humanos			Jefaturas de la Empresa				Si		Telefonica	Telefonica		Usuario	Cable	
006ACT	Fax	Fax	3.3. Equipos de Oficina	1.1 Recursos Humanos			Jefaturas de la Empresa				Si		Telefonica	Telefonica		Usuario	Impreso	
007ACT	Servidores	Servidores	3.4. Servidores	Centro de Cómputo	Jefe de la Unidad de Tecnologías de	Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información			12 horas	No		Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información	LAN	Usuario	Cable	
008ACT	Disco Duro Extraíble	Disco Duro Extraíble	3.5. Soporte de Almacenamiento	Centro de Cómputo	Jefe de la Unidad de Tecnologías de	Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información				No		Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información		Administrador		
009ACT	Memoria Extríble USB	Memoria Extríble USB	3.5. Soporte de Almacenamiento	Centro de Cómputo	Jefe de la Unidad de Tecnologías de	Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información				Si		Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información		Administrador	Cable	
010ACT	Cableado Estructurado	Cableado Estructurado	3.6. Medios de Comunicación	Centro de Cómputo	Jefe de la Unidad de Tecnologías de	Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información				No		Unidad de Tecnologías de la Información	Jefe de la Unidad de Tecnologías de la Información		Administrador	Fibra Óptica	

Formato de Listado de Categoría de Servicios

Codigo del Activo	Nombre de Activo	Descripción del Activo	Sub Categoría	Responsable del Servicio	Acceso a los Servicios	Responsable del activo	Responsable del Mantenimiento	Observaciones
001SERV	Línea telefónica	Línea telefónica	4.1. Comunicación	Jefe de la Unidad de Tecnologías de la Información	Ingreso al Servicio	Jefe de la Oficina de Administración	Jefe de la Unidad de Tecnologías de la Información	
002SERV	Central telefónica	Central telefónica	4.1. Comunicación	Jefe de la Unidad de Tecnologías de la Información	Ingreso al Servicio	Jefe de la Oficina de Administración	Jefe de la Unidad de Tecnologías de la Información	
003SERV	Fuentes de energía	Fuentes de energía	4.2. Energía	Jefe de la Unidad de Logistica	Ingreso al Servicio	Jefe de la Oficina de Administración	Jefe de la Unidad de Logistica	
004SERV	Cableado electrico	Cableado electrico	4.2. Energía	Jefe de la Unidad de Logistica	Transmisión de Datos	Jefe de la Oficina de Administración	Jefe de la Unidad de Logistica	
005SERV	Portal Web	Portal Web	4.3. Portal de la Entidad/Empresa	Jefe de la Unidad de Tecnologías de la Información	Transmisión de Datos	Jefe de la Oficina de Administración	Jefe de la Unidad de Tecnologías de la Información	
006SERV	Correo Electrónico Interno	Correo Electrónico Interno	4.4. Correo Electrónico	Jefe de la Unidad de Tecnologías de la Información	Transmisión de Datos	Jefe de la Oficina de Administración	Jefe de la Unidad de Tecnologías de la Información	
007SERV	Correo Electrónico Externo	Correo Electrónico Externo	4.4. Correo Electrónico	Jefe de la Unidad de Tecnologías de la Información	Transmisión de Datos	Jefe de la Oficina de Administración	Jefe de la Unidad de Tecnologías de la Información	

Formato de Listado de Categoría de Personas

Codigo del Activo	Nombre del Empleador	Sub Categoría	Área del Empleador	Función del Empleador	Fecha de ingreso/salida	Nombre del activo a cargo del empleador	Horas de Trabajo	Accesos Permitidos	Acuerdos de confidencialidad	Observaciones
001EMPL	Jefe de la Oficina de Administración	5.1. Empleados	Oficina de Administración	Administrador	Por Definir	Todos	Tiempo Completo	Administrador	si	
002EMPL	Jefe de la Unidad de Tecnologías de la Información	5.1. Empleados	Unidad de Tecnologías de la Información	Administrar los Centros de Computo	Por Definir	Todos	Tiempo Completo	Usuario	no	
003EMPL	Jefe de la Unidad de Recursos Humanos	5.1. Empleados	Unidad de Recursos Humanos	Administrar los recursos humanos de la organización	Por Definir	Todos	Tiempo Parcial	Administrador	si	

Formato de Características de los Activos de Información

Codigo del Activo	Nombre del Activo	Caracteristicas	Clase	Descripcion
001DA	Documentos de Procesos	1.1 Confidencialidad	C.2 Uso Interno	C.2 Puede solo ser revelada y proporcionado dentro de la empresa
002DA	Memorandos	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
003DA	Informes	1.3 Disponibilidad	D.3 Alto	D.2 Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones. Sin embargo las operaciones o los procesos podrían ser demorados hasta que los activos de información estén disponibles para la empresa.
004DA	Oficios	1.3 Disponibilidad	C.2 Uso Interno	C.2 Puede solo ser revelada y proporcionado dentro de la empresa
005DA	Actas	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
006DA	Contratos	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.4Puede ser solo revelado y proporcionado a partes específicas, dentro de la empresa.
007DA	Facturas	1.2 Integridad	I.3 Importante	I.3 Si la integridad se perdiera, hubiera un efecto fatal en las operaciones en la empresa.
008DA	Guías y reglamentos	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
009DA	Expedientes	1.1 Confidencialidad	C.3 Secreto	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
010DA	Notificaciones	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
011DA	Papeles de Trabajo	1.1 Confidencialidad	C.2 Uso Interno	C.2 Puede solo ser revelada y proporcionado dentro de la empresa
012DA	Manuales de usuario	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
013DA	Equipo de cómputo	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un efecto fatal en las operaciones o procesos en la empresa.
014DA	Servidores	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un efecto fatal en las operaciones o procesos en la empresa.
015DA	Discos ópticos	1.1 Confidencialidad	C.3 Secreto	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
016DA	Dispositivos magnéticos	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un efecto fatal en las operaciones o procesos en la empresa.
017DA	Base de Datos	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
018DA	Software de aplicación	1.3 Disponibilidad	D.2 Mediano	D.2 Si la información no llegara a estar disponible, hubiera algún efecto en las operaciones. Sin embargo las operaciones o los procesos podrían ser demorados hasta que los activos de información estén disponibles para la empresa.
019DA	Software de sistema	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un efecto fatal en las operaciones o procesos en la empresa.
020DA	Correo electrónico	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
001SW	Windows	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un efecto fatal en las operaciones o procesos en la empresa.
002SW	Linux	1.3 Disponibilidad	D.3 Alto	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un efecto fatal en las operaciones o procesos en la empresa.
003SW	SEACE 1	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
004SW	SEACE 2	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
005SW	SEACE 3	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
006SW	RNP 4	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
007SW	Tribunal de Contrataciones	1.1 Confidencialidad	C.4 Alta Confidencialidad	C.3 Puede ser solo revelado y proporcionado a partes específicas y departamentos.
008SW	Antivirus	1.2 Integridad	I.3 Importante	I.3 Si la integridad se perdiera, hubiera un efecto fatal en las operaciones en la empresa.
009SW	Microsoft Visio	1.3 Disponibilidad	D.2 Mediano	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
010SW	Oracle	1.3 Disponibilidad	D.2 Mediano	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
011SW	Microsoft Project	1.3 Disponibilidad	D.2 Mediano	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
012SW	WebLogic	1.3 Disponibilidad	D.2 Mediano	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.
013SW	Alfresco	1.3 Disponibilidad	D.2 Mediano	D.3 Si la información no tuviera disponibilidad, cuando sea necesitada en algún momento, hubiera un fatal efecto en las operaciones o procesos en la empresa.

Informe de Control de Activos de Información

Nº	Nombre del Activo	Descripción del Activo	Responsable del activo	Tipo	Acceso	Ubicación	Atributos						Observaciones
							¿El activo de información se encuentra en un estado crítico para el servicio hacia terceros?	¿El activo de información que debe ser restringido a un número limitado de empleados?	¿El activo de información que debe ser restringido a personas externas?	¿El activo de información que puede ser alterado o comprometido para fraudes o corrupción?	¿El activo de información se encuentra en un estado crítico para las operaciones internas?	¿El activo de información se encuentra en un estado crítico para el servicio hacia terceros?	
1	1.1 Datos	1.1 Actas	1.3 Area de Secretaria General	Información	Usuarios	Físico	Clientes	Si	Si	Si			
2	1.4 Servicios	1.8 Linea Telefonica	1.1 Area de Tecnologias de Informacion	Servicios	Usuarios		Terceros	No					
3	1.3 Activos Fisicos	1.3 Hardware	1.1 Area de Tecnologias de Informacion	Hardware	Usuarios		Terceros		Si	No			
4	1.1 Datos	1.2 Informes	1.3 Area de Secretaria General	Información	Usuarios	Físico	Clientes		Si	Si	Si		
5	1.2 Software	1.4 PC's	1.1 Area de Tecnologias de Informacion	Software	Usuarios			Si	Si				
6	1.1 Datos	1.2 Informes	1.4 Area de Finanzas	Información	Usuarios	Físico		Si	Si		Si	Si	
7	1.3 Activos Fisicos	1.5 Servidores	1.3 Area de Secretaria General	Hardware	Usuarios	Soporte Electrónico	Terceros		Si		Si		
8	1.1 Datos	1.2 Informes	1.3 Area de Secretaria General	Información		Físico			Si	Si			
9	1.1 Datos	1.1 Actas	1.3 Area de Secretaria General	Información		Físico		Si	Si	Si	Si		
10	1.5 Personas	1.6 Empleados	1.2 Area de Recursos Humanos	Servicios	Usuarios			Si					
11	1.1 Datos	1.1 Actas	1.4 Area de Finanzas		Usuarios	Físico			Si				
12	1.4 Servicios	1.7 Portal Web	1.1 Area de Tecnologias de Informacion		Derechos de Acceso	Soporte Electrónico			Si	Si		Si	
13	1.4 Servicios	1.8 Linea Telefonica	1.2 Area de Recursos Humanos		Derechos de Acceso	Soporte Electrónico	Terceros	No	No		No		

ANEXO E

Listado de Activos con sus Respectivas Vulnerabilidades y Amenazas - Categoría Datos

Nº	Activos	Amenazas	Vulnerabilidades
001DA	1.1.1. Documentos de Procesos	2.1.1. Errores de configuración del servicio	1.1.1. Información no protegida
002DA	1.1.1. Documentos de Procesos	1.1.2. Pérdida de información	1.1.2. Errores por el personal
003DA	1.1.1. Documentos de Procesos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
004DA	1.1.1. Documentos de Procesos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
005DA	1.1.2. Memorandos	1.1.1. Divulgación de información	1.1.1. Información no protegida
006DA	1.1.2. Memorandos	1.1.2. Pérdida de información	1.1.2. Errores por el personal
007DA	1.1.2. Memorandos	1.1.3. Incumplimiento de normas por el personal a	1.1.3. Falta de conocimiento del personal
008DA	1.1.2. Memorandos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
009DA	1.1.3. Informes	1.1.1. Divulgación de información	1.1.1. Información no protegida
010DA	1.1.3. Informes	1.1.2. Pérdida de información	1.1.2. Errores por el personal
011DA	1.1.3. Informes	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
012DA	1.1.3. Informes	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
013DA	1.1.4. Oficios	1.1.1. Divulgación de información	1.1.1. Información no protegida
014DA	1.1.4. Oficios	1.1.2. Pérdida de información	1.1.2. Errores por el personal
015DA	1.1.4. Oficios	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
016DA	1.1.4. Oficios	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
017DA	1.1.5. Actas	1.1.1. Divulgación de información	1.1.1. Información no protegida
018DA	1.1.5. Actas	1.1.2. Pérdida de información	1.1.2. Errores por el personal
019DA	1.1.5. Actas	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
020DA	1.1.5. Actas	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
021DA	1.1.6. Contratos	1.1.1. Divulgación de información	1.1.1. Información no protegida
022DA	1.1.6. Contratos	1.1.2. Pérdida de información	1.1.2. Errores por el personal
023DA	1.1.6. Contratos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
024DA	1.1.6. Contratos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
025DA	1.1.7. Facturas	1.1.1. Divulgación de información	1.1.1. Información no protegida
026DA	1.1.7. Facturas	1.1.2. Pérdida de información	1.1.2. Errores por el personal
027DA	1.1.7. Facturas	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
028DA	1.1.7. Facturas	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
029DA	1.1.8. Guías y reglamentos	1.1.1. Divulgación de información	1.1.1. Información no protegida
030DA	1.1.8. Guías y reglamentos	1.1.2. Pérdida de información	1.1.2. Errores por el personal
031DA	1.1.8. Guías y reglamentos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
032DA	1.1.8. Guías y reglamentos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
033DA	1.1.9. Expedientes	1.1.1. Divulgación de información	1.1.1. Información no protegida
034DA	1.1.9. Expedientes	1.1.2. Pérdida de información	1.1.2. Errores por el personal
035DA	1.1.9. Expedientes	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
036DA	1.1.9. Expedientes	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.
037DA	1.1.10. Notificaciones	1.1.1. Divulgación de información	1.1.1. Información no protegida
038DA	1.1.10. Notificaciones	1.1.2. Pérdida de información	1.1.2. Errores por el personal
039DA	1.1.10. Notificaciones	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal
040DA	1.1.10. Notificaciones	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.

Listado de Activos con sus Respectivas Vulnerabilidades y Amenazas - Categoría Software

Nº	Activos	Amenazas	Vulnerabilidades
001SW	2.1.1. Windows	2.1.1. Errores de configuración del servicio	2.1.1. Falta de capacitación del administrador.
002SW	2.1.1. Windows	2.1.1. Errores de configuración del servicio	2.1.2. Incompleto o incorrecto documentación del sistema.
003SW	2.1.1. Windows	2.1.2. Virus de Computación	2.1.3. Falta de Protección a los equipos
004SW	2.1.1. Windows	2.1.4. Perdida de Servicio	2.1.5. Actualizaciones incorrectas.
005SW	2.1.1. Windows	2.1.4. Perdida de Servicio	2.1.6. Instalación de software no autorizado
006SW	2.1.1. Windows	2.1.5. Controles de Seguridad no cumplidos	2.1.7. Falta de políticas de Seguridad
007SW	2.1.1. Windows	2.1.6. Alteración no autorizado de la configuración	2.1.8. Falta de control de acceso
008SW	2.1.1. Windows	2.1.7. Análisis de trafico	2.1.9. Falta de establecimiento de una conexión segura
009SW	2.1.1. Windows	2.1.8. Brechas de seguridad no detectadas	2.1.10. Falta de monitoreo de la red.
010SW	2.1.2. Linux	2.1.1. Errores de configuración del servicio	2.1.1. Falta de capacitación del administrador.
011SW	2.1.2. Linux	2.1.1. Errores de configuración del servicio	2.1.2. Incompleto o incorrecto documentación del sistema.
012SW	2.1.2. Linux	2.1.2. Virus de Computación	2.1.3. Falta de Protección a los equipos
013SW	2.1.2. Linux	2.1.4. Perdida de Servicio	2.1.5. Actualizaciones incorrectas.
014SW	2.1.2. Linux	2.1.4. Perdida de Servicio	2.1.6. Instalación de software no autorizado
015SW	2.1.2. Linux	2.1.5. Controles de Seguridad no cumplidos	2.1.7. Falta de políticas de Seguridad
016SW	2.1.2. Linux	2.1.6. Alteración no autorizado de la configuración	2.1.8. Falta de control de acceso
017SW	2.1.2. Linux	2.1.7. Análisis de trafico	2.1.9. Falta de establecimiento de una conexión segura
018SW	2.1.2. Linux	2.1.8. Brechas de seguridad no detectadas	2.1.10. Falta de monitoreo de la red.
019SW	2.2.3. SEACE 1	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
020SW	2.2.4. SEACE 2	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
021SW	2.2.5. SEACE 3	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
022SW	2.2.6. RNP 4	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
023SW	2.2.7. Tribunal de Contrataciones del Estado	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
024SW	2.2.8. Antivirus	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
025SW	2.2.9. Microsoft Visio	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
026SW	2.2.10. Oracle	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
027SW	2.2.11. Microsoft Project	2.2.1. Virus de computación	2.2.1. Falta de protección actualizada
028SW	2.3.12. WebLogic	2.3.1. Errores de configuración	2.3.1. Falta de capacitación del administrador del sistema
029SW	2.3.12. WebLogic	2.3.2. Escapes de información	2.3.2. Falta de control de acceso a los datos
030SW	2.3.12. WebLogic	2.3.3. Errores de actualización	2.3.3. Falta de procedimientos apropiados
031SW	2.3.12. WebLogic	2.3.4. Abuso de privilegios	2.3.4. Falta de políticas de seguridad
032SW	2.3.13. Alfresco	2.3.1. Errores de configuración	2.3.1. Falta de capacitación del administrador del sistema
033SW	2.3.13. Alfresco	2.3.2. Escapes de información	2.3.2. Falta de control de acceso a los datos
034SW	2.3.13. Alfresco	2.3.3. Errores de actualización	2.3.3. Falta de procedimientos apropiados
035SW	2.3.13. Alfresco	2.3.4. Abuso de privilegios	2.3.4. Falta de políticas de seguridad

Listado de Activos con sus Respectivas Vulnerabilidades y Amenazas - Categoría Activos Fijos

Nº	Activos	Amenazas	Vulnerabilidades
001ACT	3.1.1. PC	3.1.1. Acceso no autorizado de las Pcys oficina	3.1.1. Falta de protección a los equipos de cada área de la empresa/entidad
002ACT	3.1.1. PC	3.1.2. Instalación no autorizada o cambios de software	3.1.2. Falta de control y de revisión de los software de la empresa/entidad.
003ACT	3.1.1. PC	3.4.2. Degradación o Falla	3.1.3. Falta de conocimientos de seguridad por parte del personal de la empresa
004ACT	3.1.1. PC	3.1.4. Degradación del Hardware	3.1.4. Falta de mantenimiento adecuado
005ACT	3.1.1. PC	3.1.5. Copia de Software o Información no autorizada	3.1.6. Falta de protección física para los Pc's de oficina.
006ACT	3.1.1. PC	3.1.6. Robo	3.1.6. Falta de protección física para los Pc's de oficina.
007ACT	3.2.2. Hardware Portátil	3.2.1. Instalación de no autorizada o cambios de Software	3.2.1. Falta de control de acceso
008ACT	3.2.2. Hardware Portátil	3.2.2. Ataque destructivo	3.2.2. Falta de protección física
009ACT	3.2.2. Hardware Portátil	3.2.3. Robo	3.2.3. Falta de protección física adecuada
010ACT	3.2.2. Hardware Portátil	3.1.4. Degradación del Hardware	3.2.4. Falta de conocimiento de protección de derechos de SW por parte del empleado.
011ACT	3.2.2. Hardware Portátil	3.4.2. Degradación o Falla	3.2.5. Falta de protección por desatención de equipos
012ACT	3.2.2. Hardware Portátil	3.2.6. Incumplimiento con controles de seguridad	3.2.6. Falta de conocimiento de seguridad por parte del personal
013ACT	3.2.2. Hardware Portátil	3.2.7. Degradación del Hardware	3.2.7. Falta de mantenimiento adecuado.
014ACT	3.3.3. Impresora	3.3.1. Degradación o Falla Hardware	3.3.1. Falta de mantenimiento
015ACT	3.3.3. Impresora	3.1.6. Robo	3.3.2. Fatal de protección física
016ACT	3.3.4. Copiadoras	3.3.1. Degradación o Falla Hardware	3.3.1. Falta de mantenimiento
017ACT	3.3.4. Copiadoras	4.2.4. Falla de servicios de Energía	3.3.2. Fatal de protección física
018ACT	3.3.5. Teléfonos	3.3.1. Degradación o Falla Hardware	3.3.1. Falta de mantenimiento
019ACT	3.3.5. Teléfonos	4.2.4. Falla de servicios de Energía	3.3.2. Fatal de protección física
020ACT	3.3.6. Fax	3.3.1. Degradación o Falla Hardware	3.3.1. Falta de mantenimiento
021ACT	3.3.6. Fax	4.2.4. Falla de servicios de Energía	3.3.2. Fatal de protección física
022ACT	3.4.7. Servidores	3.4.1. Acceso no autorizado a través de la red	3.4.1. La existencia de un código malicioso
023ACT	3.4.7. Servidores	3.4.2. Degradación o Falla	3.4.2. Falta de mantenimiento
024ACT	3.4.7. Servidores	3.4.3. Manipulación de la configuración	3.4.3. Falta de control a los servidores
025ACT	3.4.7. Servidores	4.2.4. Falla de servicios de Energía	3.4.4. Falta de establecimiento de una conexión segura.
026ACT	3.4.7. Servidores	3.5.3. Manipulación de la configuración	3.4.5. Falta de monitoreo de los servidores
027ACT	3.5.8. Disco Duro Extraíble	3.5.1. Acceso no autorizado a través de la red	3.5.1. La existencia de un código malicioso
028ACT	3.5.8. Disco Duro Extraíble	3.5.2. Degradación o Falla	3.5.2. Falta de mantenimiento
029ACT	3.5.8. Disco Duro Extraíble	3.5.3. Manipulación de la configuración	3.5.3. Falta de control a los servidores
030ACT	3.5.8. Disco Duro Extraíble	3.5.4. Análisis de trafico	3.5.4. Falta de establecimiento de una conexión segura.
031ACT	3.5.8. Disco Duro Extraíble	3.1.6. Robo	3.5.5. Falta de monitoreo de los servidores
032ACT	3.5.9. Memoría Extríble USB	3.1.6. Robo	3.5.1. La existencia de un código malicioso
033ACT	3.5.9. Memoría Extríble USB	3.5.2. Degradación o Falla	3.5.2. Falta de mantenimiento
034ACT	3.5.9. Memoría Extríble USB	3.5.3. Manipulación de la configuración	3.5.3. Falta de control a los servidores
035ACT	3.5.9. Memoría Extríble USB	5.1.2. Divulgación de información confidencial	3.5.4. Falta de establecimiento de una conexión segura.
036ACT	3.5.9. Memoría Extríble USB	3.5.5. Brechas de seguridad no detectadas	3.5.5. Falta de monitoreo de los servidores
037ACT	3.6.10. Cableado Estructurado	3.6.1. Daños de cables	3.6.1. Falta de protección física
038ACT	3.6.10. Cableado Estructurado	3.5.2. Degradación o Falla	3.6.2. Falta de establecimiento de una conexión segura
039ACT	3.6.10. Cableado Estructurado	3.6.3. Brechas de seguridad no detectadas	3.6.3. Falta de monitoreo de la red.
040ACT	3.6.11. Tecnología Ethernet	3.6.1. Daños de cables	3.6.1. Falta de protección física
041ACT	3.6.11. Tecnología Ethernet	4.1.2. Errores de configuración	3.6.2. Falta de establecimiento de una conexión segura
042ACT	3.6.11. Tecnología Ethernet	3.6.3. Brechas de seguridad no detectadas	3.6.3. Falta de monitoreo de la red.
043ACT	3.6.12. Switch	3.6.1. Daños de cables	3.6.1. Falta de protección física
044ACT	3.6.12. Switch	3.1.6. Robo	3.6.2. Falta de establecimiento de una conexión segura
045ACT	3.6.12. Switch	3.6.3. Brechas de seguridad no detectadas	3.6.3. Falta de monitoreo de la red.
046ACT	3.6.13. Routers	3.6.1. Daños de cables	3.6.1. Falta de protección física
047ACT	3.6.13. Routers	3.1.6. Robo	3.6.2. Falta de establecimiento de una conexión segura
048ACT	3.6.13. Routers	3.6.3. Brechas de seguridad no detectadas	3.6.3. Falta de monitoreo de la red.
049ACT	3.6.14. Modem	3.6.1. Daños de cables	3.6.1. Falta de protección física
050ACT	3.6.14. Modem	3.1.6. Robo	3.6.2. Falta de establecimiento de una conexión segura
051ACT	3.6.14. Modem	3.6.3. Brechas de seguridad no detectadas	3.6.3. Falta de monitoreo de la red.

Listado de Activos con sus Respectivas Vulnerabilidades y Amenazas - Categoría Servicios

Nº	Activos	Amenazas	Vulnerabilidades
001SERV	4.1.1. Línea telefónica	4.1.1. Degradación del servicio y equipos	4.1.1. Falta de mantenimiento adecuado
002SERV	4.1.1. Línea telefónica	4.1.2. Errores de configuración	4.1.2. Falta de conocimiento del administrador
003SERV	4.1.1. Línea telefónica	3.6.1. Daños de cables	4.1.3. Falta de políticas
004SERV	4.1.1. Línea telefónica	4.1.4. Falla de servicios de Telefonía	4.1.4. Falta de acuerdos bien definidos con terceras partes
005SERV	4.1.2. Central telefónica	4.1.1. Degradación del servicio y equipos	4.1.1. Falta de mantenimiento adecuado
006SERV	4.1.2. Central telefónica	4.1.2. Errores de configuración	4.1.2. Falta de conocimiento del administrador
007SERV	4.1.2. Central telefónica	3.6.1. Daños de cables	4.1.3. Falta de políticas
008SERV	4.1.2. Central telefónica	4.1.4. Falla de servicios de Telefonía	4.1.4. Falta de acuerdos bien definidos con terceras partes
009SERV	4.2.3. Fuentes de energía	4.2.1. Degradación del servicio y equipos	4.2.1. Falta de mantenimiento adecuado
010SERV	4.2.3. Fuentes de energía	4.2.2. Errores de configuración	4.2.2. Falta de conocimiento del Personal de Mantenimiento o Administrador
011SERV	4.2.3. Fuentes de energía	3.6.1. Daños de cables	4.2.3. Falta de políticas
012SERV	4.2.3. Fuentes de energía	4.2.4. Falla de servicios de Energía	4.2.4. Falta de acuerdos bien definidos con terceras partes
013SERV	4.2.4. Cableado electrico	4.2.1. Degradación del servicio y equipos	4.2.1. Falta de mantenimiento adecuado
014SERV	4.2.4. Cableado electrico	4.2.2. Errores de configuración	4.2.2. Falta de conocimiento del Personal de Mantenimiento o Administrador
015SERV	4.2.4. Cableado electrico	3.6.1. Daños de cables	4.2.3. Falta de políticas
016SERV	4.2.4. Cableado electrico	4.2.4. Falla de servicios de Energía	4.2.4. Falta de acuerdos bien definidos con terceras partes
017SERV	4.3.5. Portal Web	4.3.1. Modificación no autorizada del sitio	4.3.1. Falta de procedimiento para los cambios
018SERV	4.3.5. Portal Web	4.3.2. Sitio Web no disponible	4.3.2. Fallas en los acuerdos de niveles de servicio
019SERV	4.4.6. Correo Electrónico	5.1.2. Divulgación de información	4.4.1. Falta de políticas
020SERV	4.4.6. Correo Electrónico Interno	4.4.2. Fallas de servicios de soporte(telefonía, servicios de Internet)	4.4.2. Falta de acuerdos bin definidos con terceras partes
021SERV	4.4.6. Correo Electrónico Interno	4.4.3. Suplantación de la identidad del usuario dentro de la empresa	4.4.3. Falta control de acceso
022SERV	4.4.6. Correo Electrónico	5.1.1. Errores del personal y acciones	4.4.4. Falta de establecimiento de una conexión segura.
023SERV	4.4.7. Correo Electrónico	4.3.2. Sitio Web no disponible	4.4.1. Falta de políticas
024SERV	4.4.7. Correo Electrónico Externo	4.1.4. Falla de servicios de Telefonía	4.4.2. Falta de acuerdos bin definidos con terceras partes
025SERV	4.4.7. Correo Electrónico Externo	4.4.3. Suplantación de la identidad del usuario dentro de la empresa	4.4.3. Falta control de acceso
026SERV	4.4.7. Correo Electrónico	4.3.2. Sitio Web no disponible	4.4.4. Falta de establecimiento de una conexión segura.

Listado de Activos con sus Respectivas Vulnerabilidades y Amenazas - Categoría Personas

Nº	Activos	Amenazas	Vulnerabilidades
001EMPL	5.1.2. Jefe de la Unidad de Tecnologías de la Información	5.1.1. Errores del personal y acciones equivocadas	5.1.1. Falta de conocimiento y entrenamiento al personal.
002EMPL	5.1.1. Jefe de la Oficina de Administración	5.1.2. Divulgación de información confidencial	5.1.2. Falta de acuerdos de confidencialidad
003EMPL	5.1.2. Jefe de la Unidad de Tecnologías de la Información	5.1.1. Errores del personal y acciones equivocadas	5.1.1. Falta de conocimiento y entrenamiento al personal.
004EMPL	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.2. Divulgación de información confidencial	5.1.2. Falta de acuerdos de confidencialidad
005EMPL	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.1. Errores del personal y acciones equivocadas	5.1.1. Falta de conocimiento y entrenamiento al personal.
006EMPL	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.2. Divulgación de información confidencial	5.1.2. Falta de acuerdos de confidencialidad

ANEXO F

Listado de Riesgos con sus respectivas Medidas Preventivas y Medidas Correctivas - Categoría Datos

Nº	Activos	Riesgos	Medidas Preventivas	Medidas Correctivas	Responsable
1	1.1.1. Documentos de Procesos	1.1.1. Divulgación de información	1.1.1. -Disponibilidad de copias de seguridad de los archivos más importantes en diferentes soportes.	1.1.2. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
2	1.1.1. Documentos de Procesos	1.1.2. Pérdida de información	1.1.1. -Disponibilidad de copias de seguridad de los archivos más importantes en diferentes soportes.	1.1.2. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
3	1.1.1. Documentos de Procesos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	2.1.1. Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
4	1.1.1. Documentos de Procesos	1.1.4. Incorrecta documentación del sistema	1.1.4. -Establecimiento de planes de contingencia para salvaguardar la información y evitar daños o pérdidas de la misma.	3.1.3. -Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
5	1.1.2. Memorandos	1.1.1. Divulgación de información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
6	1.1.2. Memorandos	1.1.2. Pérdida de información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
7	1.1.2. Memorandos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	2.1.1. Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
8	1.1.2. Memorandos	1.1.4. Incorrecta documentación del sistema	1.1.4. -Establecimiento de planes de contingencia para salvaguardar la información y evitar daños o pérdidas de la misma.	3.1.3. -Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
9	1.1.3. Informes	1.1.1. Divulgación de información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
10	1.1.3. Informes	1.1.2. Pérdida de información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
11	1.1.3. Informes	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
12	1.1.3. Informes	1.1.4. Incorrecta documentación del sistema	1.1.4. -Establecimiento de planes de contingencia para salvaguardar la información y evitar daños o pérdidas de la misma.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
13	1.1.4. Oficios	1.1.1. Divulgación de información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
14	1.1.4. Oficios	1.1.2. Pérdida de información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.2. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
15	1.1.4. Oficios	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	2.1.1. Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Riesgos con sus respectivas Medidas Preventivas y Medidas Correctivas - Categoría Software

Nº	Activos	Riesgos	Medidas Preventivas	Medidas Correctivas	Responsable
1	2.1.1. Windows	2.1.1. Errores de configuración del servicio	2.1.3. -Disponer de Software de calidad y debidamente revisado.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
2	2.1.1. Windows	2.1.1. Errores de configuración del servicio	2.1.1. -Realizar periódicamente, o cuando sea requerido por el encargado de las actualizaciones para mantener al día los distintos programas y Sistemas Operativos.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
3	2.1.1. Windows	2.1.2. Virus de Computación	1.1.4. -Establecimiento de planes de contingencia para salvaguardar la información y evitar daños o pérdidas de la misma.	4.1.3. Riesgos asumibles en la empresa o áreas: -Pérdida de las comunicaciones durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
4	2.1.1. Windows	2.1.4. Perdida de Servicio	3.1.. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
5	2.1.1. Windows	2.1.5. Controles de Seguridad no cumplidos	3.1.1. -Disponibilidad de copias de seguridad de los archivos más importantes en diferentes soportes.	5.1.1. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
6	2.1.1. Windows	2.1.6. Alteración no autorizado de la configuración	2.1.4. - Establecer una política de contraseñas para acceder a los diferentes equipos de la empresa	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
8	2.1.1. Windows	2.1.7. Análisis de trafico	2.1.3. -Disponer de Software de calidad y debidamente revisado.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
7	2.1.1. Windows	2.1.8. Brechas de seguridad no detectadas	3.5.3. -Realización periódica de copias de seguridad localizadas en servidores externos a la empresa para garantizar la disponibilidad de los datos ante cualquier	3.1.4. Riesgos asumibles en la empresa o áreas: -Fallo en alguna estación PC o portátil durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
8	2.1.2. Linux	2.1.1. Errores de configuración del servicio	3.6.2. -Mantener correctamente instalados y actualizados los sistemas de seguridad Software de los que dispone la empresa.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
9	2.1.2. Linux	2.1.1. Errores de configuración del servicio	2.1.1. -Realizar periódicamente, o cuando sea requerido por el encargado de las actualizaciones para mantener al día los distintos programas y Sistemas Operativos.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
10	2.1.2. Linux	2.1.2. Virus de Computación	3.1.4. -Instalación de un servidor de almacenamiento centralizado donde se almacene toda la información generada dentro de la empresa y que garantice un acceso adecuado, y seguro, a la misma cuando sea necesario.	3.1.1. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Riesgos con sus respectivas Medidas Preventivas y Medidas Correctivas - Categoría Activos Fijos

Nº	Activos	Riesgos	Medidas Preventivas	Medidas Correctivas	Responsable
1	3.1.1. PC	3.1.1. Acceso no autorizado de las Pcys oficina	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.2. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
2	3.1.1. PC	3.1.2. Instalación no autorizada o cambios de software	3.6.2. -Mantener correctamente instalados y actualizados los sistemas de seguridad Software de los que dispone la empresa.	3.1.1. -Restauración de copias de seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
3	3.1.1. PC	3.1.3. Uso no previsto	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	2.1.1. Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
4	3.1.1. PC	3.1.4. Degradación del Hardware	3.1.5. -Disponer de copias de respaldo almacenadas en servidores exteriores a la empresa para prevenir posibles fallos de Hardware.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
5	3.1.1. PC	3.1.5. Copia de Software o Información no autorizada	2.1.1. -Realizar periódicamente, o cuando sea requerido por el encargado de las actualizaciones para mantener al día los distintos programas y Sistemas Operativos.	2.1.1. Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
6	3.1.1. PC	3.1.6. Robo	3.1.3. -Tener la alarma conectada cuando no hay personal dentro de las instalaciones de la empresa.	2.1.1. Restauración de copias de Seguridad en el caso de haberse producido una pérdida de datos.	1.3 Jefe de Proyecto y Comité de Seguridad
7	3.2.2. Hardware Portátil	3.2.1. Instalación de no autorizada o cambios de Software	3.6.2. -Mantener correctamente instalados y actualizados los sistemas de seguridad Software de los que dispone la empresa.	4.1.3. Riesgos asumibles en la empresa o áreas: -Pérdida de las comunicaciones durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
8	3.2.2. Hardware Portátil	3.2.2. Ataque destructivo	3.5.2. -Realización periódica de copias de seguridad de los datos, en especial de los datos críticos, generados en la empresa o área.	3.1.4. Riesgos asumibles en la empresa o áreas: -Fallo en alguna estación PC o portátil durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
9	3.2.2. Hardware Portátil	3.2.3. Robo	3.1.3. -Tener la alarma conectada cuando no hay personal dentro de las instalaciones de la empresa.	3.1.4. Riesgos asumibles en la empresa o áreas: -Fallo en alguna estación PC o portátil durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
10	3.2.2. Hardware Portátil	3.2.4. Incumplimiento con la legislación	3.6.4. -Establecimiento de políticas de seguridad de acceso a la red mediante el empleo de contraseñas.	4.1.3. Riesgos asumibles en la empresa o áreas: -Pérdida de las comunicaciones durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Riesgos con sus respectivas Medidas Preventivas y Medidas Correctivas - Categoría Servicios

Nº	Activos	Riesgos	Medidas Preventivas	Medidas Correctivas	Responsable
1	4.1.1. Línea telefónica	4.1.1. Degradación del servicio y equipos	4.2.1. -Revisión periódica de la instalación eléctrica.	4.1.3. Riesgos asumibles en la empresa o áreas: -Pérdida de las comunicaciones durante un periodo inferior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
2	4.1.1. Línea telefónica	4.1.2. Errores de configuración	4.2.1. -Revisión periódica de la instalación eléctrica.	3.6.3. Riesgos asumibles en la empresa o área: -Fallo en los sistemas de comunicación de red durante un periodo no superior a 24 horas.	1.3 Jefe de Proyecto y Comité de Seguridad
3	4.1.1. Línea telefónica	4.1.3. Uso no previsto	4.2.1. -Revisión periódica de la instalación eléctrica.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
4	4.1.1. Línea telefónica	4.1.4. Falla de servicios de Telefonía	4.2.4. - Instalación de dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para garantizar el suministro eléctrico en caso de caída del sistema eléctrico general.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
5	4.1.2. Central telefónica	4.1.1. Degradación del servicio y equipos	4.2.1. -Revisión periódica de la instalación eléctrica.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
6	4.1.2. Central telefónica	4.1.2. Errores de configuración	4.2.5. -Contratación de dos líneas exteriores con suministradores de Internet para garantizar siempre una conexión mínima a la red.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
7	4.1.2. Central telefónica	4.1.3. Uso no previsto	4.2.1. -Revisión periódica de la instalación eléctrica.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
8	4.1.2. Central telefónica	4.1.4. Falla de servicios de Telefonía	4.2.4. - Instalación de dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para garantizar el suministro eléctrico en caso de caída del sistema eléctrico general.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
9	4.2.3. Fuentes de energía	4.2.1. Degradación del servicio y equipos	4.2.1. -Revisión periódica de la instalación eléctrica.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
10	4.2.3. Fuentes de energía	4.2.2. Errores de configuración	4.2.1. -Revisión periódica de la instalación eléctrica.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
11	4.2.3. Fuentes de energía	4.2.3. Uso no previsto	4.2.1. -Revisión periódica de la instalación eléctrica.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
12	4.2.3. Fuentes de energía	4.2.4. Falla de servicios de Energía	4.2.4. - Instalación de dispositivos SAI (Sistemas de Alimentación Ininterrumpida) para garantizar el suministro eléctrico en caso de caída del sistema eléctrico general.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.2 Comité de Seguridad

Listado de Riesgos con sus respectivas Medidas Preventivas y Medidas Correctivas - Categoría Personas

Nº	Activos	Riesgos	Medidas Preventivas	Medidas Correctivas	Reponsable
1	5.1.1. Jefe de la Oficina de Administración	5.1.1. Errores del personal y acciones equivocadas	1.1.2. -Instalación de bases de datos centralizadas donde se almacenen todos los datos importantes generados por la empresa o área para facilitar el almacenamiento, accesibilidad y seguridad de los datos.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
2	5.1.1. Jefe de la Oficina de Administración	5.1.2. Divulgación de información confidencial	5.1.1. -Conseguir una adecuada concienciación del personal de la empresa o área sobre lo importante que es mantener un cierto nivel de seguridad en los procesos que se realizan dentro de la empresa. Así como establecer una adecuada política de respaldo de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
3	5.1.2. Jefe de la Unidad de Tecnologías de la Información	5.1.1. Errores del personal y acciones equivocadas	1.1.3. -Establecimiento de procedimientos de seguridad que establezcan las acciones a realizar en caso de pérdidas de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
4	5.1.2. Jefe de la Unidad de Tecnologías de la Información	5.1.2. Divulgación de información confidencial	2.1.1. -Realizar periódicamente, o cuando sea requerido por el encargado de las actualizaciones para mantener al día los distintos programas y Sistemas Operativos.	3.1.2. -Tener contratado un buen servicio técnico que asegure una rápida reparación y puesta en marcha de los equipos si se produce un fallo.	1.3 Jefe de Proyecto y Comité de Seguridad
5	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.1. Errores del personal y acciones equivocadas	5.1.1. -Conseguir una adecuada concienciación del personal de la empresa o área sobre lo importante que es mantener un cierto nivel de seguridad en los procesos que se realizan dentro de la empresa. Así como establecer una adecuada política de respaldo de información.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad
6	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.2. Divulgación de información confidencial	5.1.3. -Establecer una política de contraseñas para el acceso a los recursos del sistema.	1.1.3. -Seguimiento del plan de contingencia especificado para cada caso.	1.3 Jefe de Proyecto y Comité de Seguridad

ANEXO G

Listado de Controles en la Categoría de Datos

Nº	Activos	Amenazas	Vulnerabilidades	Nombre de Control	Objetivo del Control	Sugerencias del Control	Observaciones	Responsable
001	1.1.1. Documentos de Procesos	2.1.1. Errores de configuración del servicio	1.1.1. Información no protegida	A.6 Gestión de Comunicaciones y Operaciones	A.6.9Objetivo: Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
002	1.1.1. Documentos de Procesos	1.1.2. Pérdida de información	1.1.2. Errores por el personal	A.4.Seguridad en Recursos Humanos	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal	A4.2.2bConcientización, educación y entrenamiento en la seguridad de información		1.3 Jefe de Proyecto y Comité de Seguridad
003	1.1.1. Documentos de Procesos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	A.6 Gestión de Comunicaciones y Operaciones	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
004	1.1.1. Documentos de Procesos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	A.6 Gestión de Comunicaciones y Operaciones	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
005	1.1.2. Memorandos	1.1.1. Divulgación de información	1.1.1. Información no protegida	A.6 Gestión de Comunicaciones y Operaciones	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
006	1.1.2. Memorandos	1.1.2. Pérdida de información	1.1.2. Errores por el personal	A.4.Seguridad en Recursos Humanos	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.2.2bConcientización, educación y entrenamiento en la seguridad de información		1.3 Jefe de Proyecto y Comité de Seguridad
007	1.1.2. Memorandos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	A.4.Seguridad en Recursos Humanos	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
008	1.1.2. Memorandos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	A.6 Gestión de Comunicaciones y Operaciones	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
009	1.1.3. Informes	1.1.1. Divulgación de información	1.1.1. Información no protegida	A.6 Gestión de Comunicaciones y Operaciones	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
010	1.1.3. Informes	1.1.2. Pérdida de información	1.1.2. Errores por el personal	A.4.Seguridad en Recursos Humanos	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Controles en la Categoría de software

Nº	Activos	Amenazas	Vulnerabilidades	Nombre de Control	Objetivo del Control	Sugerencias del Control	Observaciones	Responsable
001	2.1.1. Windows	2.1.1. Errores de configuración del	2.1.1. Falta de capacitación del administrador.	A.7. Control de Accesos	A.7.5Objetivo: Prevenir accesos no autorizados a los sistemas operativos	Uso de los programas utilitarios del sistema.		1.3 Jefe de Proyecto y Comité de Seguridad
002	2.1.1. Windows	2.1.1. Errores de configuración del servicio	2.1.2. Incompleto o incorrecto documentación del sistema.	A.7. Control de Accesos	A7.2Objetivo: Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
003	2.1.1. Windows	2.1.2. Virus de Computación	2.1.3. Falta de Protección a los equipos	A.6 Gestión de Comunicaciones y Operaciones	A.6.4Objetivo: Proteger la integridad del software y de la información	A.6.4aControles contra software malicioso		1.3 Jefe de Proyecto y Comité de Seguridad
004	2.1.1. Windows	2.1.4. Perdida de Servicio	2.1.5. Actualizaciones incorrectas.	A.7. Control de Accesos	A7.2Objetivo: Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
005	2.1.1. Windows	2.1.4. Perdida de Servicio	2.1.6. Instalación de software no autorizado	A.6 Gestión de Comunicaciones y Operaciones	A.6.1Objetivo: Asegurar la operación correcta y asegura de los recursos de procesamiento de información.	A.6.1dSeparación de las instalaciones de desarrollo, prueba y operación		1.3 Jefe de Proyecto y Comité de Seguridad
006	2.1.1. Windows	2.1.5. Controles de Seguridad no cumplidos	2.1.7. Falta de políticas de Seguridad	A.4.Seguridad en Recursos Humanos	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
007	2.1.1. Windows	2.1.6. Alteración no autorizado de la configuración	2.1.8. Falta de control de acceso	A.4.Seguridad en Recursos Humanos	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
008	2.1.1. Windows	2.1.7. Análisis de trafico	2.1.9. Falta de establecimiento de una conexión segura	A.4.Seguridad en Recursos Humanos	A.6.3Objetivo: Minimizar el riesgo de fallas de los sistemas.	A.6.3aGestión de la capacidad		1.3 Jefe de Proyecto y Comité de Seguridad
009	2.1.1. Windows	2.1.8. Brechas de seguridad no detectadas	2.1.10. Falta de monitoreo de la red.	A.7. Control de Accesos	A.7.4Objetivo: Prevenir el acceso no autorizado a los servicios de red	Controles de red		1.3 Jefe de Proyecto y Comité de Seguridad
010	2.1.2. Linux	2.1.1. Errores de configuración del servicio	2.1.1. Falta de capacitación del administrador.	A.8. Adquisición de sistemas de información, desarrollo y mantenimiento	A.8.5Objetivo: Mantener la seguridad del software de aplicación y la información	Sistema de gestión de contraseñas		1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Controles en la Categoría de Activos Fijos

Nº	Activos	Amenazas	Vulnerabilidades	Nombre de Control	Objetivo del Control	Sugerencias del Control	Observaciones	Responsable
001	3.1.1. PC	3.1.1. Acceso no autorizado de las Pcys oficina	3.1.1. Falta de protección a los equipos de cada área de la empresa/entidad	A.7. Control de Accesos	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
002	3.1.1. PC	3.1.2. Instalación no autorizada o cambios de software	3.1.2. Falta de control y de revisión de los software de la	A.6 Gestión de Comunicaciones y Operaciones	A.6.9Objetivo: Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
003	3.1.1. PC	3.1.3. Uso no previsto	3.1.3. Falta de conocimientos de	A.7. Control de Accesos	A7.1Objetivo: Controlar los accesos a la información.	Procedimientos de manipulación de la información		y Comité de Seguridad
004	3.1.1. PC	3.1.4. Degradación del Hardware	3.1.4. Falta de mantenimiento adecuado	A.5. Seguridad Física y del Entorno	A5.2.2Objetivo: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización	A5.2.2aUbicación y protección de equipos		1.3 Jefe de Proyecto y Comité de Seguridad
005	3.1.1. PC	3.1.5. Copia de Software o Información no autorizada	3.1.5. Falta de políticas	A.1.Política de Seguridad	A.2.1.2Gestionar la seguridad de la Información dentro de la organización.	A1.1.1b Revisión de la Política de Seguridad de información		1.3 Jefe de Proyecto y Comité de Seguridad
006	3.1.1. PC	3.1.6. Robo	3.1.6. Falta de protección física para	A.7. Control de Accesos	A7.6Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas	Procedimientos de manipulación de la información		y Comité de Seguridad
007	3.2.2. Hardware Portátil	3.2.1. Instalación de no autorizada o cambios de Software	3.2.1. Falta de control de acceso	A.7. Control de Accesos	A7.6Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
008	3.2.2. Hardware Portátil	3.2.2. Ataque destructivo	3.2.2. Falta de protección física	A.7. Control de Accesos	A7.2Objetivo: Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.	Políticas y procedimientos para el intercambio de información		1.3 Jefe de Proyecto y Comité de Seguridad
009	3.2.2. Hardware Portátil	3.2.3. Robo	3.2.3. Falta de protección física adecuada	A.7. Control de Accesos	A7.6Objetivo: Evitar el acceso no autorizado a la información contenida en los sistemas	Procedimientos de manipulación de la información		1.3 Jefe de Proyecto y Comité de Seguridad
010	3.2.2. Hardware Portátil	3.2.4. Incumplimiento con la legislación	3.2.4. Falta de conocimiento de protección de derechos de SW por parte del empleado.	A.4.Seguridad en Recursos Humanos	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.2.2aGestión de responsabilidades		1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Controles en la Categoría de Servicios

Nº	Activos	Amenazas	Vulnerabilidades	Nombre de Control	Objetivo del Control	Sugerencias del Control	Observaciones	Responsable
001	4.1.1. Línea telefónica	4.1.1. Degradación del servicio y equipos	4.1.1. Falta de mantenimiento adecuado	A.5.2 Seguridad de los Equipos	A5.2.2Objetivo: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización	A5.2.2dMantenimiento de equipos		1.3 Jefe de Proyecto y Comité de Seguridad
002	4.1.1. Línea telefónica	4.1.2. Errores de configuración	4.1.2. Falta de conocimiento del administrador	A.5.2 Seguridad de los Equipos	A5.2.2Objetivo: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización	A5.2.2aUbicación y protección de equipos		1.3 Jefe de Proyecto y Comité de Seguridad
003	4.1.1. Línea telefónica	4.1.3. Uso no previsto	4.1.3. Falta de políticas	A.1.1 Política de la Seguridad de Información	A.2.1.2Gestionar la seguridad de la Información dentro de la organización.	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
004	4.1.1. Línea telefónica	4.1.4. Falla de servicios de Telefonía	4.1.4. Falta de acuerdos bien definidos con terceras partes	A.5.2 Seguridad de los Equipos	A5.2.2Objetivo: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización	A5.2.2aUbicación y protección de equipos		1.3 Jefe de Proyecto y Comité de Seguridad
005	4.1.2. Central telefónica	4.1.1. Degradación del servicio y equipos	4.1.1. Falta de mantenimiento adecuado	A.5. Seguridad Física y del Entorno	A5.2.2Objetivo: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización	A5.2.2aUbicación y protección de equipos		1.3 Jefe de Proyecto y Comité de Seguridad
006	4.1.2. Central telefónica	4.1.2. Errores de configuración	4.1.2. Falta de conocimiento del administrador	A.3.2 Clasificación de la Información	A3.1.1Objetivo: Mantener la protección apropiada de los activos de la organización.	A3.2.1bEtiquetado y tratamiento de la información		1.3 Jefe de Proyecto y Comité de Seguridad
007	4.1.2. Central telefónica	4.1.3. Uso no previsto	4.1.3. Falta de políticas	A.2.1 Organización Interna	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
008	4.1.2. Central telefónica	4.1.4. Falla de servicios de Telefonía	4.1.4. Falta de acuerdos bien definidos con terceras partes	A.5.2 Seguridad de los Equipos	A5.1.1Objetivo: Prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización	A5.2.2dMantenimiento de equipos		1.3 Jefe de Proyecto y Comité de Seguridad
009	4.2.3. Fuentes de energía	4.2.1. Degradación del servicio y equipos	4.2.1. Falta de mantenimiento adecuado	A.2.1 Organización Interna	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
010	4.2.3. Fuentes de energía	4.2.2. Errores de configuración	4.2.2. Falta de conocimiento del Personal de Mantenimiento o	A.3.2 Clasificación de la Información	A3.1.1Objetivo: Mantener la protección apropiada de los activos de la organización.	A3.2.1bEtiquetado y tratamiento de la información		1.3 Jefe de Proyecto y Comité de Seguridad
011	4.2.3. Fuentes de energía	4.2.3. Uso no previsto	4.2.3. Falta de políticas	A.1.1 Política de la Seguridad de Información	A.2.1.2Gestionar la seguridad de la Información dentro de la organización.	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad
012	4.2.3. Fuentes de energía	4.2.4. Falla de servicios de Energía	4.2.4. Falta de acuerdos bien definidos con terceras partes	A.2.1 Organización Interna	A7.3Objetivo: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento	A1.1.1bCoordinación de la seguridad de la información		1.3 Jefe de Proyecto y Comité de Seguridad

Listado de Controles en la Categoría de Personas

Nº	Activos	Amenazas	Vulnerabilidades	Nombre de Control	Objetivo del Control	Sugerencias del Control	Observaciones	Responsable
001	5.1.2. Jefe de la Unidad de Tecnologías de la Información	5.1.1. Errores del personal y acciones equivocadas	5.1.1. Falta de conocimiento y entrenamiento al personal.	A.4.2 Durante el empleo	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.1.1.cTérminos y condiciones de la relación laboral		1.3 Jefe de Proyecto y Comité de Seguridad
002	5.1.1. Jefe de la Oficina de Administración	5.1.2. Divulgación de información confidencial	5.1.2. Falta de acuerdos de confidencialidad	A.4.1 Previo al Empleo	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.1.1.aRoles y responsabilidades		1.3 Jefe de Proyecto y Comité de Seguridad
003	5.1.2. Jefe de la Unidad de Tecnologías de la Información	5.1.1. Errores del personal y acciones equivocadas	5.1.1. Falta de conocimiento y entrenamiento al personal.	A.4.2 Durante el empleo	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.1.1.cTérminos y condiciones de la relación laboral		1.3 Jefe de Proyecto y Comité de Seguridad
004	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.2. Divulgación de información confidencial	5.1.2. Falta de acuerdos de confidencialidad	A.4.1 Previo al Empleo	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.1.1.aRoles y responsabilidades		1.3 Jefe de Proyecto y Comité de Seguridad
005	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.1. Errores del personal y acciones equivocadas	5.1.1. Falta de conocimiento y entrenamiento al personal.	A.4.2 Durante el empleo	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.1.1.cTérminos y condiciones de la relación laboral		1.3 Jefe de Proyecto y Comité de Seguridad
006	5.1.3. Jefe de la Unidad de Recursos Humanos	5.1.2. Divulgación de información confidencial	5.1.2. Falta de acuerdos de confidencialidad	A.4.1 Previo al Empleo	A.4.1.1Objetivo: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones que puedan afectar a la empresa	A4.1.1.aRoles y responsabilidades		1.3 Jefe de Proyecto y Comité de Seguridad

ANEXO H

Matriz de Riesgos

N°	Activo	Amenaza	Vulnerabilidades	PROBABILIDAD DE OCURRENCIA		NIVEL DE IMPACTO		NIVEL DE RIESGO		Mitigacion	Responsable
1	1.1.1. Documentos de Procesos	1.1.1. Divulgación de información	1.1.1. Información no protegida	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
2	1.1.1. Documentos de Procesos	1.1.2. Pérdida de información	1.1.2. Errores por el personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
3	1.1.1. Documentos de Procesos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	MEDIO	2	MEDIO	2	MEDIO	4	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
4	1.1.1. Documentos de Procesos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	MEDIO	2	BAJA	1	BAJA	2	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
5	1.1.2. Memorandos	1.1.1. Divulgación de información	1.1.1. Información no protegida	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
6	1.1.2. Memorandos	1.1.2. Pérdida de información	1.1.2. Errores por el personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
7	1.1.2. Memorandos	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
8	1.1.2. Memorandos	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	MEDIO	2	MEDIO	2	MEDIO	4	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
9	1.1.3. Informes	1.1.1. Divulgación de información	1.1.1. Información no protegida	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
10	1.1.3. Informes	1.1.2. Pérdida de información	1.1.2. Errores por el personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
11	1.1.3. Informes	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
12	1.1.3. Informes	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	ALTA	3	MEDIO	2	ALTA	6	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
13	1.1.4. Oficios	1.1.1. Divulgación de información	1.1.1. Información no protegida	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
14	1.1.4. Oficios	1.1.2. Pérdida de información	1.1.2. Errores por el personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
15	1.1.4. Oficios	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	ALTA	3	MEDIO	2	ALTA	6	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
16	1.1.4. Oficios	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	MEDIO	2	MEDIO	2	MEDIO	4	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
17	1.1.5. Actas	1.1.1. Divulgación de información	1.1.1. Información no protegida	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
18	1.1.5. Actas	1.1.2. Pérdida de información	1.1.2. Errores por el personal	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
19	1.1.5. Actas	1.1.3. Incumplimiento de normas por el personal a cuanto a la información	1.1.3. Falta de conocimiento del personal	MEDIO	2	ALTA	3	ALTA	6	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad
20	1.1.5. Actas	1.1.4. Incorrecta documentación del sistema	1.1.4. Falta de documentación actualizada del sistema.	BAJA	1	BAJA	1	BAJA	1	Por Definir	1.3 Jefe de Proyecto y Comité de Seguridad

ANEXO I

Formato de ficha de Actualización del Cronograma

Codigo	Fases y Sub-Actividad	Fecha (DD/MM/AAAA)	Hora Inicio (HH:MM)	Hora Fin (HH:MM)	Predecesor de la Actividad	Sucesor de la Actvidad	Responsable
1	Fase de Planteamiento	lunes, 03/02/2014	08:30	09:30	Organización del SGSI	Fase de Planteamiento	1.3 Jefe del Proyeto y Comité de Seguridad
2	Alcance del Proyecto	lunes, 03/02/2014	09:30	10:30	Alcance del Proyecto	Elaborar EDT del proyecto	1.3 Jefe del Proyeto y Comité de Seguridad
3	Elaborar EDT del proyecto	lunes, 03/02/2014	10:30	11:30	Alcance del Proyecto	Elaborar EDT del proyecto	1.3 Jefe del Proyeto y Comité de Seguridad
4	Elaborar Recursos del RBS	lunes, 03/02/2014	11:30	12:30	Elaborar EDT del proyecto	Elaborar Recursos del RBS	1.3 Jefe del Proyeto y Comité de Seguridad
5	Elaborar Recursos del RBS	lunes, 03/02/2014	13:30	14:30	Elaborar EDT del proyecto	Elaborar Recursos del RBS	1.3 Jefe del Proyeto y Comité de Seguridad
6	Elaborar Recursos del RBS	lunes, 03/02/2014	14:30	15:30	Elaborar Recursos del RBS	Elaborar Recursos del RBS	1.3 Jefe del Proyeto y Comité de Seguridad
7	Elaborar el Plan de SGSI	lunes, 03/02/2014	15:30	16:30	Elaborar el Plan de SGSI	Elaborar el Plan de SGSI	1.3 Jefe del Proyeto y Comité de Seguridad
8	Elaborar el Plan de SGSI	lunes, 03/02/2014	16:30	17:30	Elaborar Plan de Identificación de Activos	Elaborar Plan de Gestión de Tiempo	1.3 Jefe del Proyeto y Comité de Seguridad
9	Elaborar el Plan de SGSI	lunes, 03/02/2014	17:30	18:15	Elaborar Plan de Identificación de Activos	Elaborar Plan de Gestión de Tiempo	1.3 Jefe del Proyeto y Comité de Seguridad
10	Elaborar el Plan de SGSI	martes, 04/02/2014	08:30	09:30	Elaborar Plan de Identificación de Activos	Elaborar Plan de Gestión de Tiempo	1.3 Jefe del Proyeto y Comité de Seguridad
11	Elaborar Plan de Gestión de Tiempo	martes, 04/02/2014	09:30	10:30	Elaborar Plan de Identificación de Activos	Elaborar Plan de Gestión de Tiempo	1.3 Jefe del Proyeto y Comité de Seguridad
12	Elaborar Plan de Gestión de Tiempo	martes, 04/02/2014	10:30	11:30	Elaborar Plan de Identificación de Activos	Elaborar Plan de Gestión de Tiempo	1.3 Jefe del Proyeto y Comité de Seguridad
13	Elaborar Plan de Gestión de Tiempo	martes, 04/02/2014	11:30	12:30	Elaborar Plan de Gestión de Tiempo	Elaborar Plan de Gestión de Costos	1.3 Jefe del Proyeto y Comité de Seguridad
14	Elaborar Plan de Gestión de Tiempo	martes, 04/02/2014	13:30	14:30	Elaborar Plan de Gestión de Costos	Elaborar Plan de Gestión de Comunicaciones	1.3 Jefe del Proyeto y Comité de Seguridad
15	Elaborar EDT del proyecto	martes, 04/02/2014	14:30	15:30	Elaborar Plan de Gestión de Comunicaciones	Elaboración de Plan de Riesgos	1.3 Jefe del Proyeto y Comité de Seguridad
16	Elaborar EDT del proyecto	martes, 04/02/2014	15:30	16:30	Elaboración de Plan de Riesgos	Elaboración de Plan de Riesgos	1.3 Jefe del Proyeto y Comité de Seguridad
17	Elaborar EDT del proyecto	martes, 04/02/2014	16:30	17:30	Elaboración de Plan de Riesgos	Elaboración de Plan de Riesgos	1.3 Jefe del Proyeto y Comité de Seguridad
18	Elaborar EDT del proyecto	martes, 04/02/2014	17:30	18:15	Elaboración de Plan de Riesgos	Elaboración de Plan de Riesgos	1.3 Jefe del Proyeto y Comité de Seguridad

ANEXO J

Formato de Actividades

Codigo	Fecha (DD/MM/AAAA)	Hora Inicio (HH:MM)	Hora Fin (HH:MM)	Responsable	Actividades del Cronograma	Estado de la Actividad	Observaciones
1	lunes, 03/02/2014	08:30	09:30	1.2 Comité de Seguridad	Fase de Planteamiento	1.3 Completo	
2	lunes, 03/02/2014	09:30	10:30	1.2 Comité de Seguridad	Organización del SGSI	1.3 Completo	
3	lunes, 03/02/2014	10:30	11:30	1.2 Comité de Seguridad	Elaborar el Cuadro de Integrantes del Proyecto	1.3 Completo	
4	lunes, 03/02/2014	11:30	12:30	1.2 Comité de Seguridad	Elaborar EDT del proyecto	1.3 Completo	
5	lunes, 03/02/2014	13:30	14:30	1.1 Jefe del Proyecto	Elaborar EDT del proyecto	1.3 Completo	
6	lunes, 03/02/2014	14:30	15:30	1.2 Comité de Seguridad	Elaborar Recursos del RBS	1.3 Completo	
7	lunes, 03/02/2014	15:30	16:30	.3 Jefe del Proyeto y Comité de Segurida	Elaborar Recursos del RBS	1.3 Completo	
8	lunes, 03/02/2014	16:30	17:30	1.2 Comité de Seguridad	Fase de Planteamiento	1.3 Completo	
9	lunes, 03/02/2014	17:30	18:15	1.2 Comité de Seguridad	Elaborar Plan de Identificación de Activos	1.3 Completo	
10	martes, 04/02/2014	08:30	09:30	1.2 Comité de Seguridad	Elaborar Plan de Identificación de Activos	1.3 Completo	
11	martes, 04/02/2014	09:30	10:30	1.2 Comité de Seguridad	Elaborar Plan de Gestión de Costos	1.3 Completo	
12	martes, 04/02/2014	10:30	11:30	1.2 Comité de Seguridad	Elaborar Plan de Gestión de Comunicaciones	1.3 Completo	
13	martes, 04/02/2014	11:30	12:30	1.2 Comité de Seguridad	Elaboración de Plan de Riesgos	1.3 Completo	
14	martes, 04/02/2014	13:30	14:30	1.2 Comité de Seguridad	Fase de Planteamiento	1.3 Completo	
15	martes, 04/02/2014	14:30	15:30	1.2 Comité de Seguridad	Elaboración de Plan de Riesgos	1.3 Completo	

ANEXO K

PLAN DE CONTINUIDAD DEL NEGOCIO

Un plan de continuidad de negocio debe contener quienes son los responsables de cada actividad y tarea, y permitirá la recuperación y restauración de los activos de información de la institución.

El comité de seguridad debe desarrollar e implementar planes para proteger y recuperar la información en los activos de información, ante una interrupción o pérdida en la institución del estado.

El plan de continuidad del negocio debe contener toda la documentación, por lo cual debe contener los objetivos, el propósito del proyecto, las actividades del proyecto.

FASE DE ACTIVACION

La fase de activación define medidas, cuando se presenta una emergencia o una interrupción, en cual se notificara a los empleados para la recuperación, evaluar los daños y un aplicar un plan de continuidad. En la fase de activación debe contener la evaluación de los daños que puedan afectar al proyecto, tal como:

- Identificar la causa de la emergencia o la interrupción que se presenten en los activos de información.
- Tener un inventario y estado de los activos de información.
- Tener presente el nivel de riesgo que afectan a los activos de información que puedan ocasionar perdidas de información.

FASE DE RECUPERACION

En la fase de recuperación contiene procedimientos para restaurar el proyecto. Debe contener los siguientes puntos:

- Tener la autorización para acceder a las instalaciones dañadas.
- Tener notificados a los interesados internos y externos asociados con el proyecto
- Restaurar información de los activos de información

FASE DE RECONSTITUCION

La fase de reconstitución debe especificar los responsables de la restauración y/o sustitución. Las siguientes actividades se producen en esta fase:

- Lograr el apoyo para la recuperación de la información de los activos de la institución.
- Tener una instalación de sistema de hardware, software ante posibles riesgos que se presenten.
- Protección, eliminación y/o reubicación de todos los activos sensibles de la institución
- La institución debe entrenar al personal para la recuperación de información en caso de pérdida.

ENCUESTA

El objetivo de esta encuesta es identificar el alcance de la propuesta metodológica de Seguridad de la Información.

- Esta encuesta tiene 13 preguntas

- Lea atentamente cada una de ellas y responda marcando con una X la alternativa que mejor identifiqué su parecer.

- Si se equivoca o desea corregir su respuesta solicite al encuestador una nueva encuesta, la anterior se destruirá.

- No ponga su nombre, ni ninguna identificación suya en esta encuesta.

- Si no le corresponde llenar la encuesta por favor devuélvala al encuestador.

1. ¿Se ha aplicado un sistema de gestión de seguridad de la información para la protección a los activos de la información para la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

2. Se ha realizado procedimientos de identificación y protección de activos de información en la empresa?

Si	( )
No	( )

3. Si la respuesta anterior ha sido afirmativa ¿Cómo califica el resultado?

Muy bueno	( )
Bueno	( )
Regular	( )
Malo	( )

4. ¿En qué medida se ha aplicado el ciclo de Deming para garantizar los procedimientos en el Sistema de Gestión de Seguridad de Información de la propuesta metodológica?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

5. ¿En qué medida el Sistema de Gestión de Seguridad de Información contribuirá a mejorar y conservar la información en la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

6. ¿En qué medida la estructura metodológica establecida en la empresa del estado mejora la protección de los activos de información?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

7. Respecto a los activos de información ¿En qué medida está debidamente protegido de las vulnerabilidades y amenazas dentro de la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

8 ¿En qué medida un Sistema de Gestión de Seguridad de Información determina la mitigación de los riesgos que presenten los activos de información en la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

9. ¿En qué medida una guía metodológica garantiza la protección de los activos de información de la empresa?

Completamente	( )
En su mayor parte	( )
Regularmente	( )
Poco o nada	( )

10. ¿En qué medida la propuesta metodológica está dividida apropiadamente en fases y procedimientos? (estructurada)

Altamente estructurada	( )
Bien estructurada	( )
Poco estructurada	( )
Nada estructurada	( )

11. ¿En qué medida la propuesta metodológica ha sido de fácil uso para emplearlo en el SGSI y Gestión de Riesgos? (usabilidad)

Altamente usable	( )
Bien usable	( )
Poco usable	( )
Nada usable	( )

12. ¿En qué medida el uso del modelo PDCA facilito el entendimiento de las fases y procedimientos de la propuesta metodológica? (usabilidad)

Altamente usable	( )
Bien usable	( )
Poco usable	( )
Nada usable	( )

13. ¿En qué medida la propuesta metodológica ayuda cambiar o gestionar el alcance del SGSI en la empresa? (amplitud)

Altamente amplia	( )
Bien amplia	( )
Poco amplia	( )
Nada amplia	( )