FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

MEJORA DE SEGURIDAD DE INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008

PRESENTADA POR

DAVID AURELIO FERNÁNDEZ PEÑALOZA

OSCAR ALEXIS PACHECO VARGAS

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE

INGENIERO DE COMPUTACIÓN Y SISTEMAS

LIMA – PERÚ

2014

USMP
UNIVERSIDAD DE SAN MARTIN DE PORRES
FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE COMPUTACIÓN Y SISTEMAS

MEJORA DE SEGURIDAD DE INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008

TESIS

PARA OPTAR POR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

PRESENTADO POR

FERNÁNDEZ PEÑALOZA, DAVID AURELIO

PACHECO VARGAS, OSCAR ALEXIS

LIMA – PERÚ

2014

DEDICATORIA

A nuestros padres, por creer en nosotros al lograr nuestras metas.

A nuestros asesores, por apoyarnos y confiar en que lograríamos nuestros objetivos.

ÍNDICE DE CONTENIDOS

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS Y CUADROS

ÍNDICE DE ANEXOS

RESUMEN

En la Comandancia de Operaciones de Guardacostas - COMOPERGUARD - de la Dirección General de Capitanías Guardacostas – DICAPI - en la Marina de Guerra del Perú, a medida del intercambio de información ha venido creciendo esta se encuentra más vulnerables frente a los ataques externos de los cuales es víctima.

El presente proyecto consiste en diseñar un Plan de Sistema de Gestión de Seguridad de la Información con el fin de proteger los activos de información de la Comandancia, por ello se realizará un análisis situacional de los activos de información, posteriormente se hará la evaluación selectiva que nos permitirá identificar las vulnerabilidades de los activos de información, se identificará el vacío que existe entre la evaluación selectiva y la NORMA TÉCNICA PERUNA NTP-ISO/IEC 27001:2008 en la Comandancia, adecuándolo al cumpliendo de los reglamentos y estatutos dicha Comandancia.

La metodología de trabajo va ser adoptando el método Planear, Hacer, Verificar y Actuar usado por las normas NTP-ISO/IEC 27001:2008. Como resultado se espera con nuestra propuesta es de minimizar los riesgos, amenazas y vulnerabilidad de seguridad de la información en dicha comandancia.

Los resultados obtenidos fueron minimizar los riesgos, amenazas y vulnerabilidades de los activos de información como también el compromiso del personal de la Comandancia con respecto a la seguridad de información.

La conclusión es que nuestro modelo aplicado, ha permitido desarrollar el Plan de Sistema de Gestión de Seguridad de la información de la Comandancia basado en la norma NTP-ISO/IEC 27001:2008.

ABSTRACT

In Operations Command Guard - COMOPERGUARD - Direction General of Captaincy Guard - DICAPI - in the Navy of Peru, as the exchange of information has been growing this is more vulnerable to external attacks which is victim.

This project is to propose Information Security Management System Plan to protect the information assets of the Coast Guard Operations Command - COMOPERGUARD – from Captaincy Guard General Direction - DICAPI - in the Navy of Peru , for this, will perform a situational analysis of information assets, later will do a selective evaluation comparing it with NTP-ISO / IEC 27001:2008 in the Coast Guard Operations Command along with their security vulnerabilities, adapting it to comply that Command regulations..

The working methodology will be adopting the method Plan -Do-Check-Act- used by the ISO/IEC 27001:2008. As a result it's expected with our proposal is to minimize the risks, threats and vulnerabilities of information security in that Command.

The results were minimize risks, threats and vulnerabilities of information assets as well as the commitment of the staff of the Command according information security.

The conclusion of our model applied, allowed to develop the Plan of Management System of Information Security Command based on NTP-ISO / IEC 27001:2008.

INTRODUCCIÓN

A medida que las organizaciones han ido apoyando sus operaciones más confidenciales en la red de datos, la seguridad de información se va tornando una preocupación cada vez más importante. Anteriormente, los ataques a la seguridad de información eran sólo una circunstancia que provocaba pérdidas de tiempo, pero en la actualidad los riesgos para las organizaciones son más graves, ya que la mayoría de las operaciones y transacciones se manejan vía redes de datos y telecomunicaciones. Hoy en día, una violación a la Seguridad de una red cableada o inalámbrica puede provocar el caos en las operaciones más sensibles de una organización, afectando la productividad, poniendo en peligro la integridad de los datos, reduciendo la confianza de los clientes e interrumpiendo el flujo de información y llegando incluso hasta suspender las comunicaciones.

En la Comandancia de Operaciones Guardacostas se debe desarrollar dentro de un marco teórico general, su solución de Seguridad de la Información con base en un plan estratégico y cubriendo las necesidades propias de la comandancia.

Es por ello que en la Comandancia de Operaciones Guardacostas, se ve en la necesidad de diseñar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información con un Plan Sistema de Gestión de Seguridad de la Información que garantice que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando lo requieran los que

estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

La presente tesis consta de cinco capítulos:

El capítulo I muestra el marco teórico, en el que están planteadas las bases teóricas relacionadas con un sistema de gestión de seguridad de la información -SGS-, definiciones de términos básicos que sustentan el desarrollo adecuado del trabajo y antecedentes de la investigación.

En el capítulo II se define la metodología a emplear, la cual es la resultante de un estudio de distintas metodologías y de la investigación y aporte de los autores de este trabajo de investigación.

En el capítulo III contiene la etapa de desarrollo del proyecto, en la cual se muestra el proceso seguido para la realización del mismo.

El capítulo IV está destinado a la presentación de las pruebas y resultados del trabajo de investigación.

El capítulo V aborda la discusión de los resultados a manera de explicación de los mismos, teniendo en cuenta las variables expuestas en los capítulos anteriores.

A partir de los resultados obtenidos se han planteado las conclusiones y recomendaciones pertinentes, y finalmente se consigna la bibliografía utilizada y los anexos respectivos.

Es imprescindible encontrar la manera con la cual se pueda brindar una adecuada solución a los inconvenientes señalados, específicamente en las áreas de COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas, siendo esta la misión esencial de la presente tesis, además de continuar aportando de una manera u otra para proteger los activos de información permitiendo conocer, gestionar y minimizar los riesgos.

1.1 PROBLEMA PRINCIPAL

INADECUADA SEGURIDAD DE INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS-COMOPERGUARD POR NO CONTAR CON UNA NORMA COMO LA NTP-ISO/IEC 27001:2008.

1.2 OBJETIVOS GENERAL

DISEÑAR UN PLAN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS -COMOPERGUARD- BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008.

1.3 OBJETIVOS ESPECÍFICOS

1. Realizar un Análisis Situacional de los activos de información en las áreas COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas.
2. Realizar un Análisis de Riesgos de los activos de información focalizados en el Análisis Situacional.
3. Realizar una Evaluación Selectiva de los activos de información vulnerables encontrados en el Análisis de Riesgos.
4. Identificar la brecha y realizar el análisis comparativo entre la Evaluación Selectiva y la NTP-ISO/IEC 27001:2008.
5. Minimizar los riesgos, amenazas y vulnerabilidades de los activos de información.
6. Lograr el compromiso de la comandancia y sensibilización del personal en materia de seguridad de la información.

1.4 JUSTIFICACIÓN

Los activos de información son recursos que representan una gran importancia y costos vitales para La Comandancia de Operaciones Guardacostas. Si estos activos llegaran a fallar o tener un daño, quedaría fuera de línea, en especial en horarios con los que los sistemas y los procesamientos de información intervienen, y por tal razón, La Comandancia de Operaciones Guardacostas tiene el deber y obligación de preservarlos, utilizarlos y mejorarlos. Esto implica que para tomar las acciones apropiadas sobre la Seguridad de la Información y los sistemas informáticos, éstas decisiones deben ser basadas en la protección de muchas clases de amenazas y riesgos tales como fraude, sabotaje, extorsión, violación de la privacidad, hackers, interrupción de servicio, accidentes y desastres naturales que todos los activos de información están expuestos.

La Comandancia de Operaciones Guardacostas deberá realizar la protección de los activos de información de acuerdo al valor y nivel de importancia.

Otras de las razones por las que creemos conveniente el desarrollo de esta tesis, es el creciente avance de la tecnología y software en nuestro país y exigencias de La Comandancia de Operaciones Guardacostas para el monitoreo de embarcaciones ya que la población de estas mismas ha ido creciendo exponencialmente; así como también el avance en formas y manías de las amenazas de las que nuestros activos de información son vulnerables.

Para solucionar esta inadecuada seguridad de información que actualmente cuenta La Comandancia de Operaciones Guardacostas, se cree conveniente proponer mejorar la seguridad de información, enfocándonos en:

Plan de Sistema de Gestión de Seguridad de la Información; que servirá de guía para proteger los activos de información que es fundamental

para el éxito de la Comandancia de Operaciones Guardacostas basándonos en NTP-ISO/IEC 27001:2008.

1.5 ALCANCE

El presente proyecto abarcara el análisis y diseño de un Plan de Sistema de Gestión de Seguridad de Información, basado en las mejores prácticas de la NTP-ISO/IEC 27001:2008.

Por lo cual, se ha establecido el alcance en base a los siguientes criterios:

Entorno de estudio donde se contemplará el siguiente punto:

El estudio abarcará las áreas de COSPAS-SARSAT y SIMTRAC en la Dirección General de Capitanías Guardacostas de la Marina de Guerra del Perú.

Análisis de la situación actual donde se contemplará los siguientes puntos:

Levantamiento de información donde se documentará los activos de información.

Análisis de Riesgos, Evaluación Selectiva y se identificará la brecha que existe entre la Evaluación Selectiva y la NTP-ISO/IEC 27001:2008.

Diseño de la solución lo cual contemplará el siguiente punto:

Diseñar un Plan de Sistema de Gestión de Seguridad de Información para las áreas COSPAS-SARSAT y SIMTRAC de la Comandancia de Operaciones Guardacostas -COMOPERGUARD- basada en la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.

CAPÍTULO I: MARCO TEÓRICO

1.1 ANTECEDENTES DE LA COMANDANCIA DE OPERACIONES GUARDACOSTAS DE LA MARINA DE GUERRA DEL PERÚ

ORGANIZACIÓN

Actividades de la Organización Comandancia de Operaciones Guardacostas en La Marina de Guerra del Perú.

Giro de la Organización.

La Marina de Guerra del Perú en sus derechos y obligaciones tiene como resguardar LA SEGURIDAD NACIONAL; en la

regulación de normas, protección de recursos y transporte, represión de actividades ilícitas y defensa marítima, fluvial y lacustre; PROTECCIÓN DE LA VIDA HUMANA; control de naves, gente de mar, búsqueda y salvamento y comunicaciones marítimas; y LA PROTECCIÓN DEL MEDIO AMBIENTE, prevención, contención y mitigación.

Visión

Ser una organización eficiente y eficaz, con capacidad de llevar a cabo de manera sostenida, a través de operaciones guardacostas, tareas de control, vigilancia, seguridad y protección de las actividades en los ámbitos marítimo, fluvial y lacustre, garantizando la seguridad y protección de la vida humana y del medio ambiente acuático, así como el estricto cumplimiento de la normativa nacional y otros instrumentos internacionales ratificados por el Estado Peruano en su área de responsabilidad.

Misión

Planear, normar, dirigir y controlar las actividades en los ámbitos Marítimos, Fluvial y Lacustre del Territorio de la República, lo relativo al personal y material de la Marina Mercante Nacional, pesca y náutica deportiva y otras actividades afines, así como reprimir las actividades ilícitas en el ámbito de su jurisdicción, con el propósito de garantizar la seguridad, protección de la vida humana en el mar, ríos y lagos navegables, así como la protección del medio acuático, sus recursos y riquezas.

Estructura Orgánica.

Organigrama de la Comandancia de Operaciones de Guardacostas

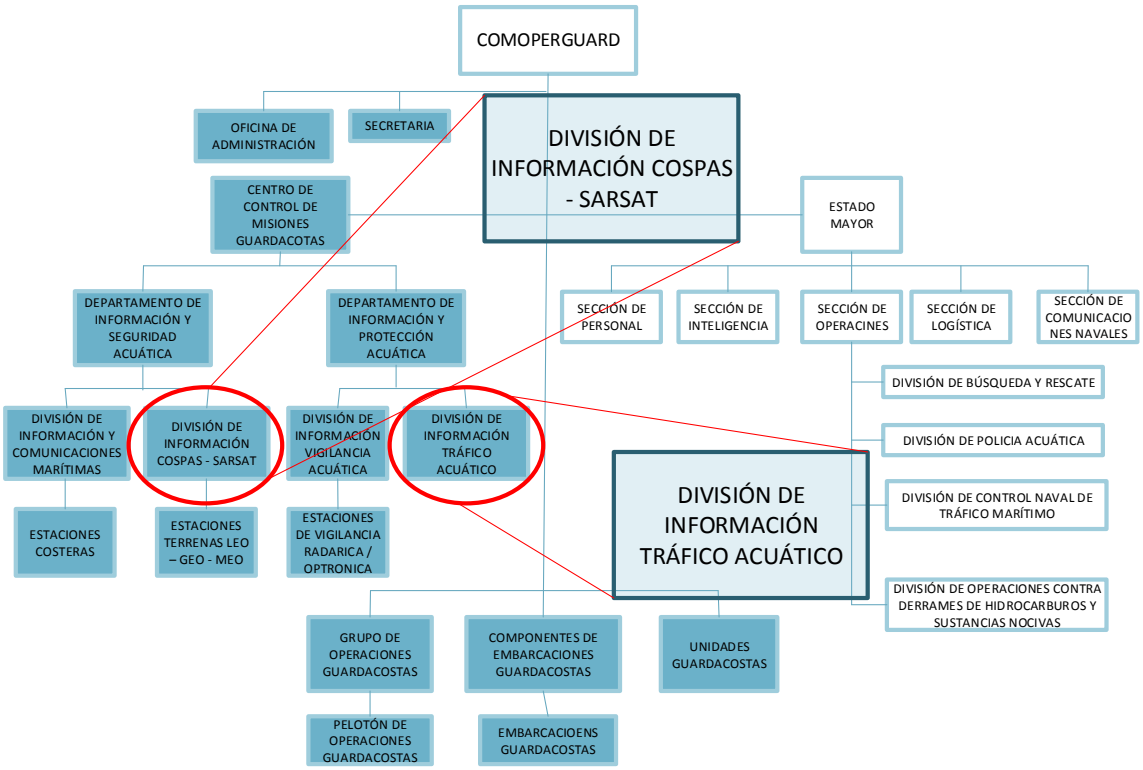

Ilustración 1: Organigrama de COMOPERGUARD

Fuente: (Marina, 2013)

Funciones.

a) Promover y desarrollar la investigación científica en el mar, ríos y lagos del territorio nacional;

b) Administrar la ejecución de todas las actividades relacionadas con la investigación científica en el mar, ríos y lagos del territorio nacional, de competencia de la Dirección de Hidrógrafa y Navegación en particular, y de la Marina de Guerra en general;

c) Administrar la ejecución de actividades técnicas desarrolladas como ayuda a la navegación en el medio marino, fluvial y lacustre de competencia de la Dirección de Hidrógrafa y Navegación en particular, y de la Marina de Guerra en general;

d) Participar en asuntos Técnico - científico de interés nacional en las áreas de su competencia; y

e) Comercializar, sin fines de lucro, cartas y publicaciones náuticas a los navegantes en general.

Objetivos.

Los objetivos de La Dirección General de Capitanías y Guardacostas – DICAPI - con La Comandancia de Operaciones Guardacostas – COMOPERGUARD - son:

- Salva guardar la vida humana en el mar.
- Evitar la depredación de la biomasa en el mar.
- Cuidar el medio ambiente.

APLICACIÓN DE LA NTP-ISO/IEC 27001:2008

INDECOPI

Unas de las instituciones del estado peruano más grande y que tomo a bien utilizar y desarrollar el Sistema de Gestión de la Seguridad de la Información es el INSTITUTO NACIONAL DE DEFENSA DE LA COMPETENCIA Y DE LA PROTECCIÓN DE LA PROPIEDAD INTELECTUAL -

INDECOPI -; que bajo los análisis y estudios necesarios establecidos por las Normas Técnicas Peruanas Desarrollo y mantiene la certificaciones ISO 27001:2008 asociada y apoyada en las normas ISO 27002 que contiene las Políticas y Controles que permitirán un mejor monitoreo y seguimiento de la Seguridad de la Información apoyada también en la norma ISO 27005 que contiene las técnicas de seguridad para la Gestión del Riesgo.

Historia

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual –INDECOPI- fue creado en noviembre de 1992, mediante el Decreto Ley N 25868.

Tiene como funciones la promoción del mercado y la protección de los derechos de los consumidores. Además, fomenta en la economía peruana una cultura de leal y honesta competencia, resguardando todas las formas de propiedad intelectual: desde los signos distintivos y los derechos de autor hasta las patentes y la biotecnología.

INDECOPI es un Organismo Público Especializado adscrito a la Presidencia del Consejo de Ministros, con personería jurídica de derecho público interno. En consecuencia, goza de autonomía funcional, técnica, económica, presupuestal y administrativa -Decreto Legislativo No 1033-.

Como resultado de su labor en la promoción de las normas de leal y honesta competencia entre los agentes de la economía peruana, el INDECOPI es concebido en la actualidad, como una entidad de servicios con marcada preocupación por impulsar una cultura de calidad para lograr la plena satisfacción de sus clientes: la ciudadanía, el empresariado y el Estado.

Misión

Propiciar el buen funcionamiento del mercado, en beneficio de los ciudadanos, consumidores y empresarios, mediante la defensa de los consumidores, la prevención y fiscalización de prácticas restrictivas de la libre y leal competencia, la protección de la propiedad intelectual y la promoción y desarrollo de una infraestructura y cultura de la calidad en el Perú.

Visión

Que los ciudadanos, consumidores y empresarios se beneficien de un mercado que opera sin distorsiones, gracias a la labor técnica, proactiva, oportuna, predecible y confiable del INDECOPI, la misma que garantiza un entorno de libre y leal competencia en el que se respetan los derechos de los consumidores, así como los derechos de propiedad intelectual, y se promueve una infraestructura y cultura de calidad.

Sistema de Gestión Seguridad de la Información

Presentación

INDECOPI, llego a la implementación de un Sistema de Gestión de Seguridad de la Información que funciona acorde con los requisitos de la Norma Técnica Peruana ISO 27001:2008, para proteger la información de los procesos, casos, trámites y demás actividades que el Estado, la ciudadanía, consumidores, autoridades y sociedad en general nos confía.

Alcance de la certificación del INDECOPI

La certificación ISO 27001 está referida a la seguridad con que la institución administra la información de los procesos, casos, trámites y demás actividades relacionadas a sus funciones encomendadas. Con esta certificación, INDECOPI se convierte en una de las entidades públicas líder en seguridad de la información. En el Perú, ocho empresas e instituciones han obtenido esta certificación de reconocimiento mundial y solo dos de ellas corresponden a entidades del Estado peruano. A continuación, las áreas involucradas en el alcance:

Áreas Funcionales

Servicio de Atención al Ciudadano.

Mesa de Partes.

Archivo Central.

Áreas de Soporte

Gerencia de Planeamiento y Gestión Institucional.

Gerencia de Tecnologías de la Información.

Gerencia de Administración y Finanzas.

Sub Gerencia de Gestión Humana.

Sub Gerencia de Finanzas y Contabilidad.

Sub Gerencia de Logística y Control Patrimonial.

Su aplicación es sobre toda la información producida, manejada, transmitida y almacenada en los sistemas de información de los procesos antes mencionados, incluyendo la información enviada y transmitida a externos, en cumplimiento de dispositivos legales vigentes -u otra normativa propia de la institución- en la sede principal de la Institución, ubicada en San Borja, Lima.

Involucra a todos los colaboradores, contratistas y terceros que tengan acceso o que estén desarrollando, adquiriendo o usando cualquier forma de los sistemas de información y/o datos relacionados con los procesos mencionados. (Indecopi, 2014)

1.2 BASES TEÓRICAS

SEGURIDAD DE LA INFORMACIÓN

La seguridad de información, como disciplina trata de establecer metodologías para determinar 4 características que son deseables para algunas circunstancias -Confidencialidad, Integridad, Autenticidad, Disponibilidad-, y de encontrar la forma de lograr que se apliquen. (Daltabuit, 2007)

La seguridad de la información es un proceso en que involucra gran número de elementos, como: aspectos tecnológicos, de gestión-organizacionales, de recursos humanos, de índole económica, de negocios, de tipo legal, de cumplimiento, etc.; abarcando no solo aspectos informáticos y telecomunicaciones sino también aspectos físicos, medioambientales, humanos, etc. (Areitio, 2008)

Se define la seguridad como la ausencia de riesgos o tener confianza en algo o de alguna persona o cosa; pero si esta palabras se asocia a alguna área o campo o algo específico sufriría cambios de connotación y de significado; podemos definirla entonces como el sentimiento de bienestar que siente una persona en algún aspecto cotidiano de su vida diaria.

Conceptualicemos la información como un conjunto de datos procesados que envían un mensaje cambiando un conocimiento a la persona o sistema.

Por lo tanto la seguridad de la información podemos definirla como el conjunto de medidas antes que ocurra algo preventivo y mientras ocurra algo correctivo que toda organización en sus sistemas información resguardaría y protegería continuando con su confidencialidad, disponibilidad e integridad.

Los sistemas de información y sistemas informáticos; la seguridad de los sistemas informáticos se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

ENFOQUES DE LA SEGURIDAD DE LA INFORMACIÓN

Se inicia la seguridad de la información señalando que su manejo está basado en lo tecnológico y sabiendo que puede ser confidencial: la información como tal en un solo lugar que puede tener un alto valor. Es divulgada, puede ser mal utilizada, robada, borrada o saboteada. Así recaería directamente en su disponibilidad poniéndola en un gran riesgo. La información da poder, y de acuerdo a lo que ofrezca estratégicas daría acceso a información, que podríamos clasificar de la siguiente manera:

Crítica: Que es indispensable para la operación de la organización.

Valiosa: Es un activo de la organización y muy valioso.

Sensible: Debe de ser conocida por las personas autorizadas.

Utilizamos para estos efectos dos palabras muy importantes que son:

Riesgo: Materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de la organización.

Seguridad: La forma de protección contra los riesgos.

La seguridad de la información abarca diversos campos conceptuales tales como la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

La reducción o eliminación de los riesgos de una cierta información está directamente ligado a la seguridad de la información y la seguridad informática. Pero la seguridad de la información tiene como objeto de los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles; situadas en el enfoque, las metodologías utilizadas, y las zonas de concentración. La seguridad de la información involucra la implementación de estrategias que concentran a los procesos en donde la información es el activo principal. Las estrategias deben tener como inicio el establecimiento de políticas, controles de

seguridad, tecnologías y procedimientos para detectar las amenazas que puedan explotar las vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. La seguridad de la información está en todas partes como en los gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

En caso de que la información confidencial de una empresa, sus clientes, sus decisiones, su estado financiero o nueva línea de productos caigan en manos de un competidor; se vuelva pública de forma no autorizada, podría ser causa de la pérdida de credibilidad de los clientes, pérdida de negocios, demandas legales o incluso la quiebra de la misma.

Por muchos años la Seguridad de la Información ha declarado que la confidencialidad, integridad y disponibilidad son los principios básicos de la seguridad de la información.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que puedan mantener la confidencialidad, integridad y disponibilidad de la información, si alguna de estas características falla no hay nada seguro. Es importante anotar, que la seguridad no es ninguna marca en ningún punto en especial, es por otra parte un proceso continuo que hay que gestionar conociendo siempre las vulnerabilidades y las amenazas que se adhieren sobre cualquier información, teniendo siempre en consideración las causas de riesgo y la probabilidad de que ocurran, así como el impacto que puede tener.

Acotamos entonces que:

Confidencialidad; es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes

rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

Por ejemplo, una transacción de tarjeta de crédito en Internet requiere que el número de tarjeta de crédito a ser transmitida desde el comprador al comerciante y el comerciante de a una red de procesamiento de transacciones. El sistema intenta hacer valer la confidencialidad mediante el cifrado del número de la tarjeta y los datos que contiene la banda magnética durante la transmisión de los mismos. Si una parte no autorizada obtiene el número de la tarjeta en modo alguno, se ha producido una violación de la confidencialidad.

La pérdida de la confidencialidad de la información puede adoptar muchas formas. Cuando alguien mira por encima de su hombro, mientras usted tiene información confidencial en la pantalla, cuando se pública información privada, cuando un laptop con información sensible sobre una empresa es robado, cuando se divulga información confidencial a través del teléfono, etc. Todos estos casos pueden constituir una violación de la confidencialidad.

Integridad; es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. A groso modo, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

La violación de integridad se presenta cuando un empleado, programa o proceso -por accidente o con mala intención- modifica o borra los datos importantes que son parte de la información, así mismo hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada, asegurando su precisión y confiabilidad. La integridad de un mensaje se obtiene adjuntándole otro conjunto de datos de comprobación de la integridad: la firma digital Es uno de los pilares fundamentales de la seguridad de la información

Disponibilidad; la disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

En el caso de los sistemas informáticos utilizados para almacenar y procesar la información, los controles de seguridad utilizados para protegerlo, y los canales de comunicación protegidos que se utilizan para acceder a ella deben estar funcionando correctamente. La alta disponibilidad de sistemas objetivo debe estar disponible en todo momento, evitando interrupciones del servicio debido a cortes de energía, fallos de hardware, y actualizaciones del sistema.

Garantizar la disponibilidad implica también la prevención de ataque de denegación de servicio. Para poder manejar con mayor facilidad la seguridad de la información, las organizaciones o negocios se pueden ayudar con un sistema de gestión que permita conocer, administrar y minimizar los posibles riesgos que atenten contra la seguridad de la información del negocio.

La disponibilidad además de ser importante en el proceso de seguridad de la información, es variada en el sentido de que existen diferentes mecanismos para cumplir con los niveles de servicio que se requiera. Tales mecanismos se implementan en infraestructura tecnológica, servidores de correo electrónico, de bases de datos, de web entre otros, mediante el uso de clusters o arreglos de discos, equipos de alta disponibilidad a nivel de red, servidores espejo, replicación de datos, redes de almacenamiento, enlaces redundantes, entre otros. La gama de posibilidades dependerá de lo que queremos proteger y el nivel de servicio que se quiera proporcionar.

Autenticación o autentificación; es la propiedad que permite identificar el generador de la información. Por ejemplo al recibir un mensaje de alguien, estar seguro que es de ese alguien el que lo ha mandado,

y no una tercera persona haciéndose pasar por la otra suplantando su identidad. En un sistema informático se suele conseguir este factor con el uso de cuentas de usuario y contraseñas de acceso.

Esta propiedad se puede considerar como un aspecto de la integridad -si está firmado por alguien, está realmente enviado por el mismo- y así figura en la literatura anglosajona.

Servicios de seguridad

El objetivo de un servicio de seguridad es mejorar la seguridad de los sistemas de procesamiento de datos y la transferencia de información en las organizaciones. Los servicios de seguridad están diseñados para contrarrestar los ataques a la seguridad y hacen uso de uno o más mecanismos de seguridad para proporcionar el servicio.

No repudio

Nos proporciona protección contra la interrupción, por parte de alguna de las entidades implicadas en la comunicación, de haber participado en toda o parte de la comunicación. El servicio de Seguridad de No repudio o irrenunciabilidad está estandarizado en la ISO-7498-2.

No Repudio de origen: El emisor no puede negar que envío porque el destinatario tiene pruebas del envío, el receptor recibe una prueba infalsificable del origen del envío, lo cual evita que el emisor, de negar tal envío, tenga éxito ante el juicio de terceros. En este caso la prueba la crea el propio emisor y la recibe el destinatario.

Prueba que el mensaje fue enviado por la parte específica.

No Repudio de destino: El receptor no puede negar que recibió el mensaje porque el emisor tiene pruebas de la recepción. Este servicio proporciona al emisor la prueba de que el destinatario legítimo de un envío, realmente lo recibió, evitando que el receptor lo niegue posteriormente. En este caso la prueba irrefutable la crea el receptor y la recibe el emisor.

Prueba que el mensaje fue recibido por la parte específica.

Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el no repudio prueba que el autor envió la comunicación - no repudio en origen - y que el destinatario la recibió - no repudio en destino -. El no repudio evita que el emisor o el receptor nieguen la transmisión de un mensaje. Así, cuando se envía un mensaje, el receptor puede comprobar que, efectivamente, el supuesto emisor envió el mensaje. De forma similar, cuando se recibe un mensaje, el emisor puede verificar que, de hecho, el supuesto receptor recibió el mensaje. Definición según la recomendación X.509 de la UIT-T Servicio que suministra la prueba de la integridad y del origen de los datos- ambos en una relación infalsificable que pueden ser verificados por un tercero en cualquier momento.

Protocolos de Seguridad de la Información

Estos protocolos de seguridad son un conjunto de reglas que gobiernan dentro de la transmisión de datos entre la comunicación de dispositivos para ejercer una confidencialidad, integridad, autenticación y el no repudio de la información. Están compuestos de los siguientes ítems:

Criptografía - Cifrado de datos - Se ocupa del cifrado de mensajes un mensaje es enviado por el emisor lo que hace es transposición u ocultar el mensaje hasta que llega a su destino y puede ser descifrado por el receptor.

Lógica - Estructura y secuencia - Llevar un orden en el cual se agrupan los datos del mensaje el significado del mensaje y saber cuándo se va enviar el mensaje.

Identificación - Autenticación - Es una validación de identificación es la técnica mediante la cual un proceso comprueba que el compañero de comunicación es quien se supone que es y no se trata de un impostor.

Planificación de la seguridad

Por estos tiempos la rápida evolución del entorno tecnológico requiere que las organizaciones adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito del plan de seguridad del sistema es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles en el lugar o los previstos para cumplir esos requisitos. El plan de seguridad del sistema también delimita o encamina las responsabilidades y el comportamiento esperado de todos los individuos que acceden al sistema. Debe reflejar las aportaciones de distintos gestores con responsabilidades sobre el sistema, incluidos los propietarios de la información, el propietario de la red, y el alto funcionario de la agencia de información de seguridad – SAISO -.

Los administradores de programas, los propietarios del sistema, y personal de seguridad en la organización debe entender el sistema de seguridad en el proceso de planificación. Los responsables de la ejecución y gestión de sistemas de información deben participar en el tratamiento de los controles de seguridad que deben aplicarse a sus sistemas.

Creación de un plan de respuesta a incidentes

Es importante diseñar un plan de respuestas a incidentes, soportarlo a lo largo de la organización y probarlo regularmente. Un buen plan de respuestas a incidentes puede no sólo minimizar los efectos de una violación sino también, reducir la publicidad que está en contra de la organización.

Desde la perspectiva de un equipo de seguridad, no importa si ocurre una violación o abertura - pues tales eventos son una parte eventual de cuando se hacen negocios usando un método de poca confianza como lo es Internet -, sino más bien cuando ocurre. El aspecto positivo de entender la inevitabilidad de una violación a los sistemas - cualquier sistema donde se procese información confidencial, no está limitado a servicios informáticos - es que permite al equipo de seguridad desarrollar un camino a seguir para las acciones de minimizar los daños potenciales. Combinando estas acciones con la experiencia le permite al equipo responder a condiciones adversas de una manera formal y oportuna.

El plan de respuesta a incidentes puede ser dividido en cuatro fases:

- Acción inmediata pueden detener o minimizar el incidente.
- Investigación del incidente.
- Restauración de los recursos afectados.
- Reporte del incidente a los canales apropiados.

Una respuesta a incidentes debe ser decisiva y ejecutarse rápidamente. Debido a que hay muy poco espacio para errores, es crítico que se efectúen prácticas de emergencias y se midan los tiempos de respuesta. De esta forma, es posible desarrollar una metodología que fomenta la velocidad y la precisión, minimizando el impacto de la indisponibilidad de los recursos y el daño potencial causado por el sistema en peligro.

Un plan de respuesta a incidentes puede tener un sin número de requerimientos; y estos deben incluir:

- Un equipo de expertos locales.
- Una estrategia legal revisada y aprobada.
- Soporte financiero de la organización.
- Soporte ejecutivo de la gerencia superior.
- Un plan de acción factible y probada.
- Recursos físicos, tal como almacenamiento redundante, sistemas en stand by y servicios de respaldo.

Consideraciones legales

Otros a tomar en consideración en una respuesta a incidentes son las ramificaciones legales. Los planes de seguridad deberían ser desarrollados con miembros del equipo de asesoría jurídica o alguna forma de consultoría general. De la misma forma en que cada organización debería tener su propia política de seguridad corporativa, cada organización tiene su forma particular de manejar incidentes desde la perspectiva legal. Las regulaciones locales, de estado o federales están más allá del ámbito de este documento, pero se mencionan debido a que la metodología para llevar a cabo el análisis post-mortem, será dictado, al menos en parte, por la consultoría jurídica. La consultoría general puede alertar al personal técnico de las ramificaciones legales de una violación; los peligros de que se escape información personal de un cliente, registros médicos o financieros; y la importancia de restaurar el servicio en ambientes de misión crítica tales como hospitales y bancos.

Planes de acción

Ya creado un plan de acción, debe ser aceptado e implementado activamente. Cualquier aspecto del plan que sea cuestionado durante la implementación activa lo más seguro es que resulte en un tiempo de respuesta pobre y tiempo fuera de servicio en el evento de una violación. Aquí es donde los ejercicios prácticos son invalorables. La implementación del plan debería ser acordada entre todas las partes relacionadas y ejecutada con seguridad, a menos que se llame la atención con respecto a algo antes de que el plan sea colocado en producción.

La respuesta a incidentes debe ir acompañada con recolección de información siempre que esto sea posible. Los procesos en ejecución, conexiones de red, archivos, directorios y mucho más deberían ser auditados activamente en tiempo real. Puede ser muy útil tener una toma instantánea de los recursos de producción al hacer un seguimiento de servicios o procesos maliciosos. Los miembros de CERT y los expertos internos serán recursos excelentes para seguir tales anomalías en un sistema.

El manejo de riesgos

La seguridad en la información se hace con la clasificación de las alternativas para manejar los posibles riegos que un activo o bien puede tener dentro de los procesos de organización. Esta clasificación lleva el nombre de manejo de riegos. El manejo de riesgos, conlleva una estructura bien definida, con un control adecuado y su manejo, habiéndolos identificado, priorizados y analizados, a través de acciones factibles y efectivas. Para ello se cuenta con las siguientes técnicas de manejo del riesgo:

Evitar. El riesgo es evitado cuando la organización rechaza aceptarlo, es decir, no se permite ningún tipo de exposición. Esto se logra

simplemente con no comprometerse a realizar la acción que origine el riesgo. Esta técnica tiene más desventajas que ventajas, ya que la empresa podría abstenerse de aprovechar muchas oportunidades. Ejemplo:

No instalar empresas en zonas sísmicas

Reducir. Cuando el riesgo no puede evitarse por tener varias dificultades de tipo operacional, la alternativa puede ser su reducción hasta el nivel más bajo posible. Esta opción es la más económica y sencilla. Se consigue optimizando los procedimientos, la implementación de controles y su monitoreo constante. Ejemplo:

No fumar en ciertas áreas, instalaciones eléctricas anti flama, planes de contingencia.

Retener, Asumir o Aceptar el riesgo. Es uno de los métodos más comunes del manejo de riesgos, es la decisión de aceptar las consecuencias de la ocurrencia del evento. Puede ser voluntaria o involuntaria, la voluntaria se caracteriza por el reconocimiento de la existencia del riesgo y el acuerdo de asumir las perdidas involucradas, esta decisión se da por falta de alternativas. La retención involuntaria se da cuando el riesgo es retenido inconscientemente. Ejemplo de asumir el riesgo:

Con recursos propios se financian las pérdidas.

Transferir. Es buscar un respaldo y compartir el riesgo con otros controles o entidades. Esta técnica se usa ya sea para eliminar un riesgo de un lugar y transferirlo a otro, o para minimizar el mismo, compartiéndolo con otras entidades. Ejemplo:

Transferir los costos a la compañía aseguradora

Medios de transmisión de ataques a los sistemas de seguridad

El mejor en soluciones de su clase permite una respuesta rápida a las amenazas emergentes, tales como:

- Malware y spam propagado por e-mail.
- La propagación de malware y botnets.
- Los ataques de phishing alojados en sitios web.
- Los ataques contra el aumento de lenguaje de marcado extensible – XML - de tráfico, arquitectura orientada a servicios – SOA - y servicios web.

Estas soluciones ofrecen un camino a la migración y la integración. Como las amenazas emergentes, cada vez más generalizada, estos productos se vuelven más integrados en un enfoque de sistemas.

Un enfoque de sistemas de configuración, la política, y el seguimiento se reúne cumplimiento de las normativas en curso y permite a los sistemas rentables de gestión. El enfoque de sistemas de gestión de la seguridad, dispone:

- Configuración de la política común de todos los productos
- Amenaza la inteligencia y la colaboración de eventos
- Reducción de la complejidad de configuración
- Análisis de riesgos eficaces y operativos de control

En la actualidad gracias a la gran cantidad posibilidades que se tiene para tener acceso a los recursos de manera remota y al gran incremento en las conexiones a internet los delitos en el ámbito de TI se han visto incrementado, bajo estas circunstancias los riesgos informáticos son más latentes. Los delitos cometidos mediante el uso de la computadora han crecido en tamaño, forma y variedad. Los principales delitos hechos por computadora o por medio de computadoras son:

1. Fraudes
2. Falsificación
3. Venta de información

Entre los hechos criminales más famosos en los Estados Unidos están:

El caso del Banco Wells Fargo donde se evidenció que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.

El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.

El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyó gran cantidad de archivos.

También se menciona el caso de un estudiante de una escuela que ingreso a una red canadiense con un procedimiento de admirable sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una pérdida de USD 3 millones.

También el caso de estudiantes de Ingeniería electrónica donde accedieron al sistema de una Universidad de Colombia y cambiaron las notas de sus compañeros generando estragos en esta Universidad y retrasando labores, lo cual dejó grandes pérdidas económicas y de tiempo.2

Los virus, troyanos, spyware, malware y demás código llamado malicioso - por las funciones que realiza y no por tratarse de un código erróneo -, tienen como objetivo principal el ejecutar acciones no solicitadas por el usuario, las cuales pueden ser desde, el acceso a una página no deseada, el

re direccionamiento de algunas páginas de internet, suplantación de identidad o incluso la destrucción o daño temporal a los registros del sistemas, archivos y/o carpetas propias. El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través cualquier medio extraíble y transportable o de la misma red en la que se encuentre un equipo infectado, causando diversos tipos de daños a los sistemas.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba de un virus que fue se distribuyó desde un BBS y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica EGA, pero al ejecutarlo salía la presentación pero al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía "Caíste".

Este dato se considera como el nacimiento de su nombre, ya que los programas con código integrado, diseñados para hacer cosas inesperadas han existido desde que existen las propias computadoras. Las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipament Corporation – DEC - empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

Actores que amenazan la seguridad

Un hacker es cualquier persona con amplios conocimientos en tecnología, bien puede ser informática, electrónica o comunicaciones, mantiene permanentemente actualizado y conoce a fondo todo lo relacionado con programación y sistemas complejos; es un investigador nato que se inclina ante todo por conocer lo relacionado con cadenas de datos cifrados y las posibilidades de acceder a cualquier tipo de "información segura". Su formación y las habilidades que poseen les dan una experticia mayor que les permite

acceder a sistemas de información seguros, sin ser descubiertos, y también les da la posibilidad de difundir sus conocimientos para que las demás personas se enteren de cómo es que realmente funciona la tecnología y conozcan las debilidades de sus propios sistemas de información.

Un cracker es aquella persona con comportamiento compulsivo, que alardea de su capacidad para reventar sistemas electrónicos e informáticos. Un cracker es un hábil conocedor de programación de Software y Hardware; diseña y fabrica programas de guerra y hardware para reventar software y comunicaciones como el teléfono, el correo electrónico o el control de otros computadores remotos.

Un lamer es una persona que alardea de pirata informático, cracker o hacker y solo intenta utilizar programas de FÁCIL manejo realizados por auténticos hackers.

Un copyhacker es una persona dedicada a falsificar y crackear hardware, específicamente en el sector de tarjetas inteligentes. Su estrategia radica en establecer amistad con los verdaderos Hackers, para copiarles los métodos de ruptura y después venderlos los bucaneros. Los copyhackers se interesan por poseer conocimientos de tecnología, son aficionados a las revistas técnicas y a leer todo lo que hay en la red. Su principal motivación es el dinero.

Un bucanero es un comerciante que depende exclusivamente de la red para su actividad. Los "bucaneros" no poseen ningún tipo de formación en el área de los sistemas, si poseen un amplio conocimiento en área de los negocios.

Un phreaker se caracterizan por poseer vastos conocimientos en el área de telefonía terrestre y móvil, incluso más que los propios técnicos de las compañías telefónicas; recientemente con el auge de los teléfonos móviles, han tenido que entrar también en el mundo de la informática y del procesamiento de datos.

Un newbie o novato de red; es un individuo que sin proponérselo tropieza con una página de hacking y descubre que en ella existen áreas de descarga de buenos programas de hackeo, baja todo lo que puede y empieza a trabajar con ellos.

Un script kiddie o skid kiddie es un simple usuario de Internet, sin conocimientos sobre hackeo o crackeo que, aunque aficionado a estos tema, no los conoce en profundidad limitándose a recopilar información de la red y a buscar programas que luego ejecuta, infectando en algunos casos de virus a sus propios equipos.

Un tonto o descuidado es un simple usuario de la información, con o sin conocimientos sobre hackeo o crackeo que accidentalmente borra daña o modifica la información, ya sea en un mantenimiento de rutina o supervisión.

Otros conceptos

Otros conceptos relacionados son:

Auditabilidad: Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Identificación: Verificación de una persona o cosa; reconocimiento.

Autenticación: Proporcionar una prueba de identidad; puede ser algo que se sabe, que se es, se tiene o una combinación de todas.

Autorización: Lo que se permite cuando se ha otorgado acceso.

No repudio: No se puede negar un evento o una transacción.

Seguridad en capas: La defensa a profundidad que contenga la inestabilidad.

Control de Acceso: limitar el acceso autorizado solo a entidades autenticadas.

Métricas de Seguridad y Monitoreo: Medición de actividades de seguridad.

Gobierno: Proporcionar control y dirección a las actividades.

Estrategia: Los pasos que se requieren para alcanzar un objetivo.

Arquitectura: El diseño de la estructura y las relaciones de sus elementos.

Gerencia: Vigilar las actividades para garantizar que se alcancen los objetivos.

Riesgo: La explotación de una vulnerabilidad por parte de una amenaza.

Exposiciones: Áreas que son vulnerables a un impacto por parte de una amenaza.

Vulnerabilidades: Deficiencias que pueden ser explotadas por amenazas.

Amenazas: Cualquier acción o evento que puede ocasionar consecuencias adversas.

Riesgo residual: El riesgo que permanece después de que se han implementado contra medidas y controles.

Impacto: Los resultados y consecuencias de que se materialice un riesgo.

Criticidad: La importancia que tiene un recurso para el negocio.

Sensibilidad: El nivel de impacto que tendría una divulgación no autorizada.

Análisis de impacto al negocio: evaluar los resultados y las consecuencias de la inestabilidad.

Controles: Cualquier acción o proceso que se utiliza para mitigar el riesgo.

Contra medidas: Cualquier acción o proceso que reduce la vulnerabilidad.

Políticas: Declaración de alto nivel sobre la intención y la dirección de la gerencia.

Normas: Establecer los límites permisibles de acciones y procesos para cumplir con las políticas.

Ataques: Tipos y naturaleza de inestabilidad en la seguridad.

Clasificación de datos: El proceso de determinar la sensibilidad y Criticidad de la información.

Gobierno de la Seguridad de la Información

Un término a tomar en cuenta en el área de la seguridad de la información es su Gobierno dentro de alguna organización empezando por determinar los riesgos que le atañen y su forma de reducir y/o mitigar impactos adversos a un nivel aceptable mediante el establecimiento de un programa amplio y conciso en seguridad de la información y el uso efectivo de recursos cuya guía principal sean los objetivos del negocio, es decir, un programa que asegure una dirección estratégica enfocada a los objetivos de una organización y la protección de su información.

Tecnologías

Las principales tecnologías referentes a la seguridad de la información en informática son:

Cortafuegos

Administración de cuentas de usuarios

Detección y prevención de intrusos

Antivirus

Infraestructura de llave pública

Capas de Socket Segura –SSL-

Conexión única "Single Sign on- SSO"

Biométria

Cifrado

Cumplimiento de privacidad

Acceso remoto

Firma digital

Intercambio electrónico de Datos "EDI" y Transferencia Electrónica de Fondos "EFT"

Redes Virtuales Privadas "VPNs"

Transferencia Electrónica Segura "SET"

Informática Forense

Recuperación de datos

Tecnologías de monitoreo

Estándares de seguridad de la información

ISO/IEC 27000-series

ISO/IEC 27001

ISO/IEC 27002

Otros estándares relacionados

COBIT

ITIL

ISO/IEC 20000: Tecnología de la información, Gestión del servicio. BSI fue pionera con el desarrollo de la BS 15000 en 2002, norma en la que se basó la ISO 20000.

Certificaciones

CISM: Certified Information Security Manager

CISSP: Security Professional Certification

GIAC: Global Information Assurance Certification

CPTE Certified Penetration Testing Engineer

CPTC: Certified Penetration Testing Consultant

CPEH: Certified Professional Ethical Hacker

CISSO: Certified Information Systems Security Officer

CSLO: Certified Security Leadership Officer

Certificaciones independientes en seguridad de la información

CISA: Certified Information Systems Auditor, ISACA

CISM: Certified Information Security Manager, ISACA

Lead Auditor ISO27001- Lead Auditor ISO 27001, BSI

CISSP: Certified Information Systems Security Professional, ISC2

COMPTia: Computing Technology Industry Association

CEH: Certified Ethical Hacker

PCI DSS: PCI Data Security Standard (Gómez Vieites, 2006)

NORMAS DE SEGURIDAD

LAS NORMAS DE SEGURIDAD ISO

La ISO - International Standarization Organization - es la entidad internacional encargada de favorecer la normalización en el mundo. Con sede en Ginebra, es una federación de organismos nacionales, éstos, a su vez, son oficinas de normalización que actúan de delegadas en cada país, como por ejemplo: AENOR en España, AFNOR en Francia, DIN en Alemania, etc. con comités técnicos que llevan a término las normas. Se creó para dar más eficacia a las normas nacionales.

Las normas son un modelo, un patrón, ejemplo o criterio a seguir. Una norma es una fórmula que tiene valor de regla y tiene por finalidad definir las características que debe poseer un objeto y los productos que han de tener una compatibilidad para ser usados a nivel internacional.

Pongamos, por ejemplo, el problema que ocasiona a muchos usuarios los distintos modelos de enchufes que existen a escala internacional para poder acoplar pequeñas máquinas de uso personal: secadores de cabello, máquinas de afeitar, etc. cuando se viaja. La incompatibilidad repercute en muchos campos. La normalización de los productos es, pues, importante.

La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir menores costes y efectividad.

Tiene valor indicativo y de guía. Actualmente su uso se va extendiendo y hay un gran interés en seguir las normas existentes porque desde el punto de vista económico reduce costes, tiempo y trabajo. Criterios de eficacia y de capacidad de respuesta a los cambios. Por eso, las normas que presentemos, del campo de la información y documentación, son de gran utilidad porque dan respuesta al reto de las nuevas tecnologías.

ISO 27000

La información es un activo es vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización.

Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización.

ISO/IEC 27000 es un conjunto de estándares desarrollados - o en fase de desarrollo - por ISO - International Organization for Standardization - e IEC - International Electrotechnical Commission -, que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

En este apartado resumiremos las distintas normas que componen la serie ISO 27000 y se indica cómo puede una organización implantar un sistema de gestión de seguridad de la información – SGSI - basado en ISO 27001.

ORIGEN

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI - British Standards Institución, la organización británica equivalente a AENOR en España - es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa - británica o no - un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma - BS 7799-1 - es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte - BS 7799-2 -, publicada por primera vez en 1998, la que establece los requisitos de un sistema de seguridad de la información – SGSI - para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

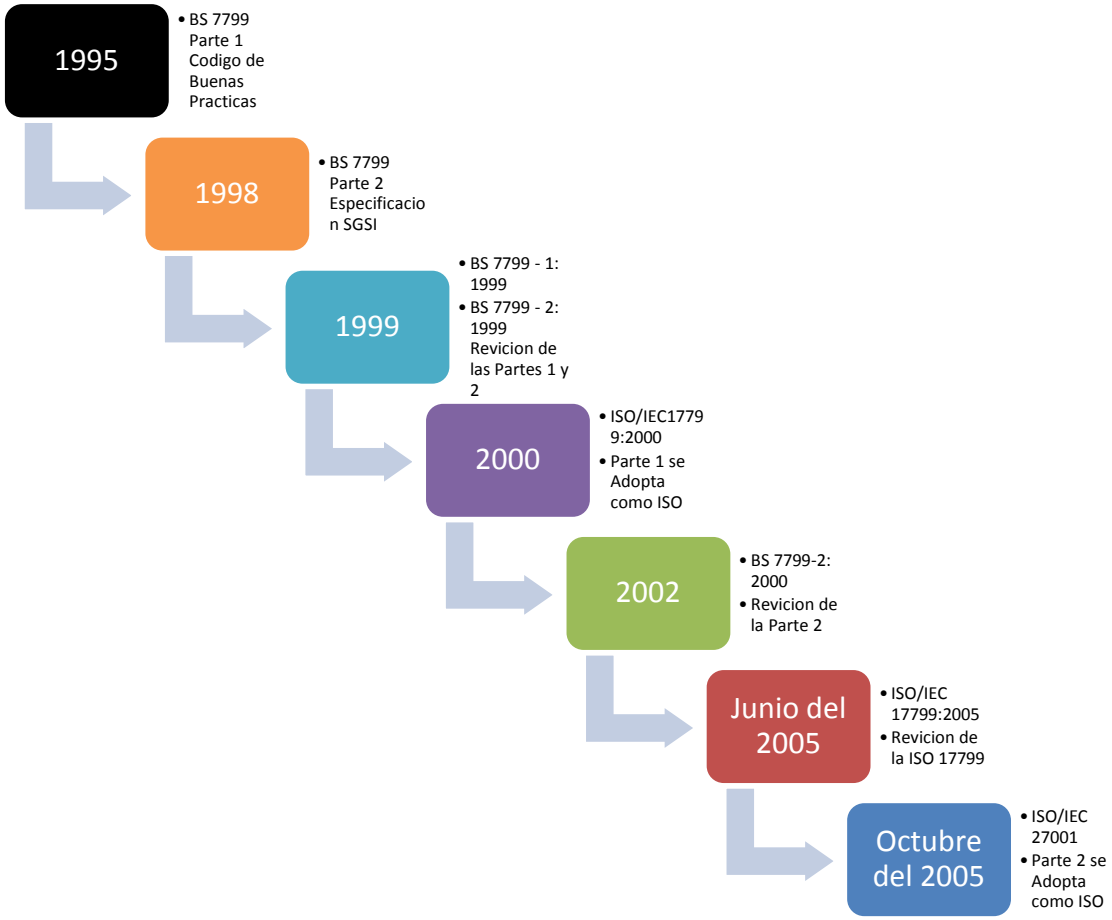

Ilustración 2: Historia del ISO

Fuente: (PriteshGupta, 2012)

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

En marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

LA SERIE 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

• ISO 27000: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Contendrá términos y definiciones que se emplean en toda la serie 27000. La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión. Esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.

• ISO 27001: Publicada el 15 de Octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo F, enumera en forma de resumen las clausulas, objetivos de control y controles que desarrolla la ISO 27002:2005 - nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007 -, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007 y puede adquirirse online en AENOR. Otros países donde también está publicada en español son, por ejemplo, Colombia, Venezuela y Argentina.

• ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida - previsiblemente, a lo largo de 2008.

• ISO 27003: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2009. Consistirá en una guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

• ISO 27004: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008. Especificará las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” - Implementar y Utilizar - del ciclo PDCA.

• ISO 27005: Publicada el 4 de Junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es

importante para un completo entendimiento de la norma ISO/IEC 27005:2008, que es aplicable a todo tipo de organizaciones -por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro- que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. Su publicación revisa y retira las normas ISO/IEC TR 13335-3:1998 y ISO/IEC TR 13335-4:2000. En España, esta norma aún no está traducida.

• ISO 27006: Publicada el 13 de Febrero de 2007. Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 - Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs - que añade a ISO/IEC 17021 - Requisitos para las entidades de auditoría y certificación de sistemas de gestión - los requisitos específicos relacionados con ISO 27001 y los SGSIs. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021 cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida.

• ISO 27007: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de auditoría de un SGSI.

• ISO 27011: En fase de desarrollo; su fecha prevista de publicación es finales de 2008. Consistirá en una guía de gestión de seguridad de la información específica para telecomunicaciones, elaborada conjuntamente con la ITU - Unión Internacional de Telecomunicaciones -.

• ISO 27031: En fase de desarrollo; su fecha prevista de publicación es Mayo de 2010. Consistirá en una guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

• ISO 27032: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía relativa a la ciber-seguridad.

• ISO 27033: En fase de desarrollo; su fecha prevista de publicación es entre 2010 y 2011. Es una norma consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes. Provendrá de la revisión, ampliación y re numeración de ISO 18028.

• ISO 27034: En fase de desarrollo; su fecha prevista de publicación es Febrero de 2009. Consistirá en una guía de seguridad en aplicaciones.

• ISO 27799: Publicada el 12 de Junio de 2008. Es un estándar de gestión de 5 seguridades de la información en el sector sanitario aplicando ISO 17799 - actual ISO 27002 -. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma. ISO 27799:2008 especifica un conjunto detallado de controles y directrices de buenas prácticas para la gestión de la salud y la seguridad de la información por organizaciones sanitarias y otros custodios de la información sanitaria en base a garantizar un

mínimo nivel necesario de seguridad apropiado para la organización y circunstancias que van a mantener la confidencialidad, integridad y disponibilidad de información personal de salud. ISO 27799:2008 se aplica a la información en salud en todos sus aspectos y en cualquiera de sus formas, toma la información - palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas -, sea cual fuere el medio utilizado para almacenar - de impresión o de escritura en papel o electrónicos de almacenamiento - y sea cual fuere el medio utilizado para transmitirlo - a mano, por fax, por redes informáticas o por correo -, ya que la información siempre debe estar adecuadamente protegida.

CONTENIDO

En esta sección se hace un breve resumen del contenido de las normas ISO 27001, ISO 27002, ISO 27006 e ISO 27799. Si desea acceder a las normas completas, debe saber que éstas no son de libre difusión sino que han de ser adquiridas.

Para los originales en inglés, puede hacerlo online en la tienda virtual de la propia organización:

http://www.iso.org/iso/en/prods-services/ISOstore/store.html

Las normas en español pueden adquirirse en España en AENOR - vea en la sección Serie 27000 cuáles están ya traducidas:

http://www.aenor.es/desarrollo/normalizacion/normas/buscadornormas.asp

Las entidades de normalización responsables de la publicación y venta de normas en cada país hispanoamericano; es decir, las

homólogas del AENOR español las puede encontrar listadas en nuestra sección de Enlaces, bajo Acreditación y Normalización.

ISO 27001:2005

• Introducción: generalidades e introducción al método PDCA.

• Objeto y campo de aplicación: se especifica el objetivo, la aplicación y el tratamiento de exclusiones.

• Normas para consulta: otras normas que sirven de referencia.

• Términos y definiciones: breve descripción de los términos más usados en la norma.

• Sistema de gestión de la seguridad de la información: cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.

• Responsabilidad de la dirección: en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.

• Auditorías internas del SGSI: cómo realizar las auditorías internas de control y cumplimiento.

• Revisión del SGSI por la dirección: cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.

• Mejora del SGSI: mejora continua, acciones correctivas y acciones preventivas.

• Objetivos de control y controles: anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.

• Relación con los Principios de la OCDE: anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.

• Correspondencia con otras normas: anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.

• Bibliografía: normas y publicaciones de referencia.

ISO 27002:2005 -ANTERIOR ISO 17799:2005-

• Introducción: conceptos generales de seguridad de la información y SGSI.

• Campo de aplicación: se especifica el objetivo de la norma.

• Términos y definiciones: breve descripción de los términos más usados en la norma.

• Estructura del estándar: descripción de la estructura de la norma.

• Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

• Política de seguridad: documento de política de seguridad y su gestión.

• Aspectos organizativos de la seguridad de la información: organización interna; terceros.

• Gestión de activos: responsabilidad sobre los activos; clasificación de la información.

• Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

• Seguridad física y ambiental: áreas seguras; seguridad de los equipos.

• Gestión de comunicaciones y operaciones: responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.

• Control de acceso: requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a la información y a las aplicaciones; ordenadores portátiles y teletrabajo.

• Adquisición, desarrollo y mantenimiento de los sistemas de información: requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

• Gestión de incidentes de seguridad de la información: notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.

• Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio.

• Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

• Bibliografía: normas y publicaciones de referencia.

ISO 27005:2008

Esta norma establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales

especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.

- Preámbulo
- Introducción
- Referencias normativas
- Términos y definiciones
- Breve descripción de los términos más usados en la norma.
- Estructura del estándar
- Descripción de la estructura de la norma.
- Fundamentos del proceso de gestión de riesgos –ISRM-
- Indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- Establecimiento del contexto
- Evaluación de riesgos –ISRA-
- Tratamiento de riesgos
- Aceptación del riesgo
- Comunicación del riesgo
- Monitorización y revisión del riesgo
- Anexo A: De la norma Definiendo el ámbito del proceso
- Anexo B: De la norma Valoración de activos y evaluación de impacto

- Anexo C: De la norma Ejemplos de amenazas más comunes
- Anexo D: De la norma Vulnerabilidades y métodos de evaluación
- Anexo E: De la norma Aproximación a ISRA

ISO 27006:2007

Esta norma referencia directamente a muchas cláusulas de ISO 17021 requisitos de entidades de auditoría y certificación de sistemas de gestión.

- Preámbulo: presentación de las organizaciones ISO e IEC y sus actividades.
- Introducción: antecedentes de ISO 27006 y guía de uso para la norma.
- Campo de aplicación: a quién aplica este estándar.
- Referencias normativas: otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- Principios: principios que rigen esta norma.
- Requisitos generales: aspectos generales que deben cumplir las entidades de certificación de SGSI.
- Requisitos estructurales: estructura organizativa que deben tener las entidades de certificación de SGSI.
- Requisitos en cuanto a recursos: competencias requeridas para el personal de dirección, administración y auditoría de la entidad de certificación, así como para auditores externos, expertos técnicos externos y subcontratas.

• Requisitos de información: información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre la entidad de certificación y sus clientes.

• Requisitos del proceso: requisitos generales del proceso de certificación, auditoría inicial y certificación, auditorías de seguimiento, recertificación, auditorías especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.

• Requisitos del sistema de gestión de entidades de certificación: opciones, opción 1 -requisitos del sistema de gestión de acuerdo con ISO 9001- y opción 2 requisitos del sistema de gestión general-.

• Anexo A de la norma: Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector potencial de riesgo de la organización (tabla orientativa) y categorías de riesgo de la seguridad de la información específicas del sector de actividad.

• Anexo B de la norma: Áreas de ejemplo de competencia del auditor consideraciones de competencia general y consideraciones de competencia específica conocimiento de los controles del Anexo A de ISO 27001:2005 y conocimientos sobre SGSI.

• Anexo C de la norma: Tiempos de auditoría: introducción, procedimiento para determinar la duración de la auditoría y tabla de tiempos de auditoría -incluyendo comparativa con tiempos de auditoría de sistemas de calidad ISO 9001 y medioambientales ISO 14001-.

• Anexo D de la norma: Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005: tabla de apoyo para el auditor sobre cómo auditar los controles, sean organizativos o técnicos.

ISO 27799:2008

Publicada el 12 de Junio de 2008. Es un estándar de gestión de seguridad de la información en el sector sanitario aplicando ISO 17799 -actual ISO 27002-. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215. ISO 27799:2008 define directrices para apoyar la interpretación y aplicación en la salud informática de la norma ISO / IEC 27002 y es un complemento de esa norma.

• Alcance

• Referencias –Normativas-

• Terminología

• Simbología

• Seguridad de la información sanitaria -Objetivos; Seguridad en el gobierno de la información; Información sanitara a proteger; Amenazas y vulnerabilidades-

• Plan de acción práctico para implantar ISO 17799/27002 -Taxonomía; acuerdo de la dirección; establecimiento, operación, mantenimiento y mejora de un SGSI; “Planning”, “Doing”, “Checking”, “Auditin”-.

• Implicaciones sanitarias de ISO 17799/27002 -Política de seguridad de la información; Organización; gestión de activos; RRHH; Físicos; Comunicaciones; Accesos; Adquisición; Gestión de Incidentes; Continuidad de negocio; Cumplimiento legal-

• Anexo A de la norma: Amenazas

• Anexo B de la norma: Tareas y documentación de un SGSI

• Anexo C de la norma: Beneficios potenciales y atributos de herramientas

• Anexo D de la norma: Estándares relacionados

BENEFICIOS

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

• Reducción del riesgo de pérdida, robo o corrupción de información.

• Los clientes tienen acceso a la información a través medidas de seguridad.

• Los riesgos y sus controles son continuamente revisados.

• Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.

• Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.

• Posibilidad de integrarse con otros sistemas de gestión -ISO 9001, ISO 14001, OHSAS 18001L-.

• Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.

• Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.

• Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.

• Confianza y reglas claras para las personas de la organización.

• Reducción de costes y mejora de los procesos y servicio.

• Aumento de la motivación y satisfacción del personal.

• Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías. Fuente: (ISO, 2012)

ISO 27001

La información es uno de los activos más importantes en cualquier organización y siempre ha estado amenazada, ya desde la antigüedad se era consciente de la existencia de las amenazas a la que está expuesta la información y se utilizaban medios para protegerlos. Prueba de ello, es que Julio Cesar ya cifraba sus mensajes con el conocido procedimiento que lleva su nombre, pero el auge en la implantación de las tecnologías de información y las telecomunicaciones-TIC- ha incrementado el número de amenazas de las que está expuesto, así como la probabilidad de materialización de dichas amenazas.

Para proteger la información, que en sí es algo inmaterial pero que reside en diferentes tipos de soporte, como pueden ser las personas, los documentos escritos o los sistemas informáticos, es necesario tomar las medidas de seguridad apropiadas para garantizar el nivel de seguridad de la información que requiere nuestra organización.

La seguridad de la información debe formar parte de todos los procesos de negocios, tanto si los procesos son manuales o automáticos, ya que en todos ellos intervienen la información de la organización como parte fundamental, teniendo en cuenta que dichos procesos involucran a personas, a tecnología y a relaciones con socios de negocios, clientes o terceros. (Merino Bada, 2011)

EVOLUCIÓN DE LA NORMA ISO 27001

Su origen es británico, hasta que en el año 2005, la Organización Internacional para la Normalización –ISO- la oficializó como norma.

El ISO 27001:2005 es el único estándar certificable, aceptado internacionalmente de manera global para la gestión de la seguridad de la información; aplica a todo tipo de organizaciones, tanto por su tamaño como por su actividad.

La siguiente tabla ISO 27001 muestra la evolución en el tiempo de las normas permitiéndonos conoces como han ido mejorando gradualmente con las mejores prácticas hasta nuestros días.

Evolución de las Normativas

EVOLUCIÓN NORMATIVA
1995 BS 7799-1: 1995 -Norma británica-
1999 BS 7799-2: 1999 -Norma británica-
1999 Revisión BS 7799-1: 1999
2000 ISO/IEC 17799: 2000 -Norma Internacional código de prácticas-
2002 Revisión BS 7799-2: 2002
2004 UNE 71502 -Norma española-
2005 Revisión ISO/IEC 17799:2005
2005 Revisión BS 7799:2005
2005 ISO/IEC 27001:2005 -Norma internacional certificable-

Tabla 1: ISO 27001

Fuente: (Mantilla, 2009)

NATURALEZA DE LA NORMA

La norma ISO 27001, actúa bajo el enfoque de procesos. La aplicación de un sistema de procesos, dentro de la organización, junto con la identificación y las interacciones de estos procesos, así como su gestión, puede denominarse como enfoque basado en procesos.

El enfoque basado en procesos para la gestión de la seguridad de la información presentada en esta norma, enfatiza a los usuarios, la importancia de:

A) La comprensión de los requisitos de seguridad de la información de una organización y la necesidad de establecer la política y objetivos para la seguridad de la información.

B) Implementar y operar controles para dirigir los riesgos de seguridad de la información de una organización en el contexto de los riesgos globales del negocio de la organización.

C) Realizar seguimiento y revisar el desempeño y la eficacia del SGSI; y

D) La mejora continua con base en mediciones objetivas.

Situación simple ⟶ Solución simple para el SGSI

Orientación a procesos:

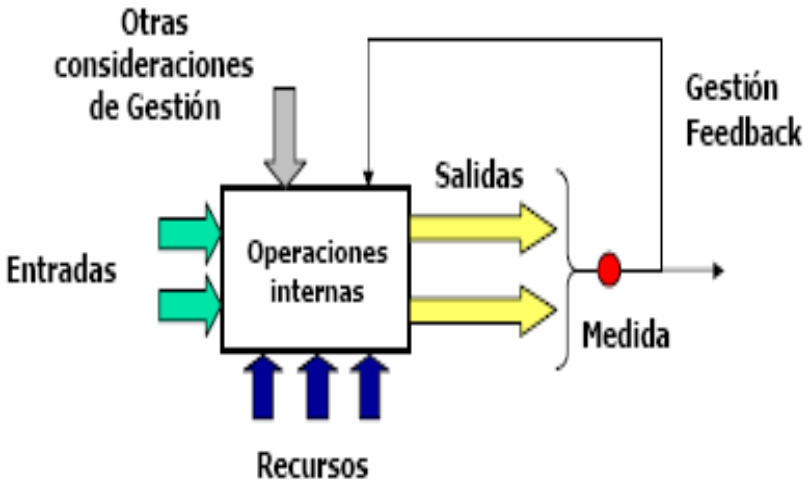

Ilustración 3: Simple SGSI

Fuente: (Mantilla, 2009)

Esta Norma adopta el modelo Planificar, Hacer, Verificar, Actuar - PDCA en inglés -, el cual se aplica para estructurar todos los procesos del SGSI, y tiene por objeto: establecer, gestionar y documentar el SGSI, responsabilizando a la Dirección, incluso en el monitoreo, auditoria y mejoramiento continuo.

Para cumplir con este objetivo, la norma ISO 27001 ha sido estructurada de forma metodológica con cláusulas y anexos, que incluyen objetivos de control y controles, así como también su relación con otras normas ISO. Como punto de partida, la norma en referencia presenta un prefacio, de manera seguida se presentan las cláusulas y anexos. En la tabla siguiente se muestra esta estructura:

Clausulas, Objetivos de Control y Controles

CLÁUSULA	Nº	SECCIÓN	SUBSECCIÓN
INTRODUCCIÓN	0		
OBJETO	1		
REFERENCIAS NORMATIVAS	2		
TÉRMINOS Y DEFINICIONES	3		
SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	4	4.1Requisitos Generales	
		4.2 Establecer y Gestionar el SGSI	4.2.1 Establecer el SGSI
			4.2.2 Implementar y operar el SGSI
			4.2.3 Monitorear y revisar el SGSI
			4.2.4 Mantener y mejorar el SGSI
		4.3 Documentar el SGSI	4.3.1 Generalidades
			4.3.2 Controlar documentos
			4.3.3 Controlar los registros
RESPONSABILIDAD DE LA DIRECCIÓN	5	5.1 Compromiso de la dirección	
		5.2 Gestionar los recursos	5.2.1 Provisión de recursos
			5.2.2 Capacitación y entrenamiento
AUDITORÍAS INTERNAS DEL SGSI	6		
		7.1 Generalidades	

CLÁUSULA	Nº	SECCIÓN	SUBSECCIÓN
REVISIÓN POR LA DIRECCIÓN DEL SGSI	7	7.2 Elementos de entrada para revisión	
		7.3 Resultados de la revisión	
MEJORA DEL SGSI	8	8.1Mejoramiento continuo	
		8.2 Acción correctiva	
		8.3 Acción preventiva	
ANEXOS		A. Normativo	
		B. Informativo	
		C. Informativo	

Tabla 2: Estructura de la Norma ISO 27001

Fuente: (Mantilla, 2009)

Los objetivos de control y sus controles respectivos normativos de la norma ISO 27001 - enfocan la Seguridad de la Información a través de 11 áreas fundamentales para la organización, estas son:

A) Política de seguridad

B) Organización de la seguridad de la información

C) Gestión de activos

D) Seguridad de los recursos humanos

E) Seguridad física y del entorno

F) Gestión de las comunicaciones y operaciones

G) Control de accesos

H) Adquisición, desarrollo y mantenimiento de sistemas de información

I) Gestión de los incidentes de seguridad

J) Gestión de la continuidad del negocio

K) Cumplimiento normativo -legales, de estándares, técnicas y auditorias-

En la siguiente figura, puede verse como el objetivo final de la norma ISO 27001 es preservar la disponibilidad, la confidencialidad, la integridad, y el no repudio de la información.

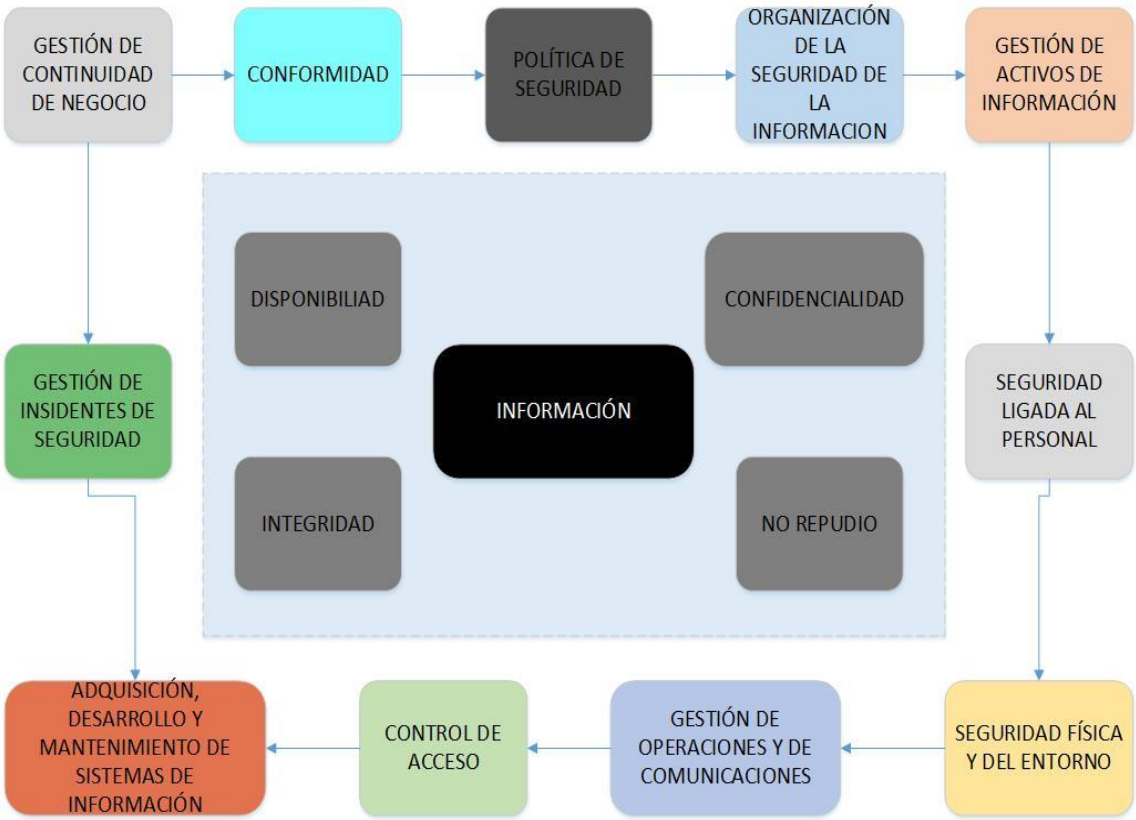

Ilustración 4: Enfoque de los controles de la norma ISO 27001

Fuente: (Mantilla, 2009)

A continuación por la importancia que tienen estas 11 áreas de control, se detalla a qué refieren cada una de ellas:

Política de seguridad

Se necesita una política que refleje las expectativas de la organización en materia de seguridad con el fin de suministrar administración con dirección y soporte, la cual también se puede utilizar como base para el estudio y evaluación en curso.

Organización de la seguridad de la información

Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

Gestión de activos

Muestra la necesidad de un inventario de los recursos de información de la organización y con base en este conocimiento, asegurar que se brinde un nivel adecuado de protección.

Seguridad de los recursos humanos

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad

y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la CAC o se debe implementar un plan para reportar los incidentes.

Seguridad física y del entorno

Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

Gestión de las comunicaciones y operaciones

Los objetivos de esta sección son:

- Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.
- Minimizar el riesgo de falla de los sistemas.
- Proteger la integridad del software y la información.
- Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
- Garantizar la protección de la información en las redes y de la infraestructura de soporte.
- Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
- Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

Control de accesos

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

Adquisición, desarrollo y mantenimiento de sistemas de información Recuerda que en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

Gestión de incidentes de seguridad

Asegura que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.

Gestión de continuidad del negocio

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes, en caso de una falla grave o desastre.

Cumplimiento Normativo - legales, de estándares, técnicas y auditorías - Imparte instrucciones para que se verifique si el cumplimiento con la norma técnica ISO 27001 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de

auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio. (Mantilla, 2009)

ACTIVIDADES PARA ALCANZAR CERTIFICACIÓN ISO 27001

Para alcanzar la certificación internacional, las organizaciones deben realizar una serie de actividades, para posteriormente tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoria para su primera certificación. El proceso para la certificación bebería efectuarse de la manera que indica en la siguiente figura:

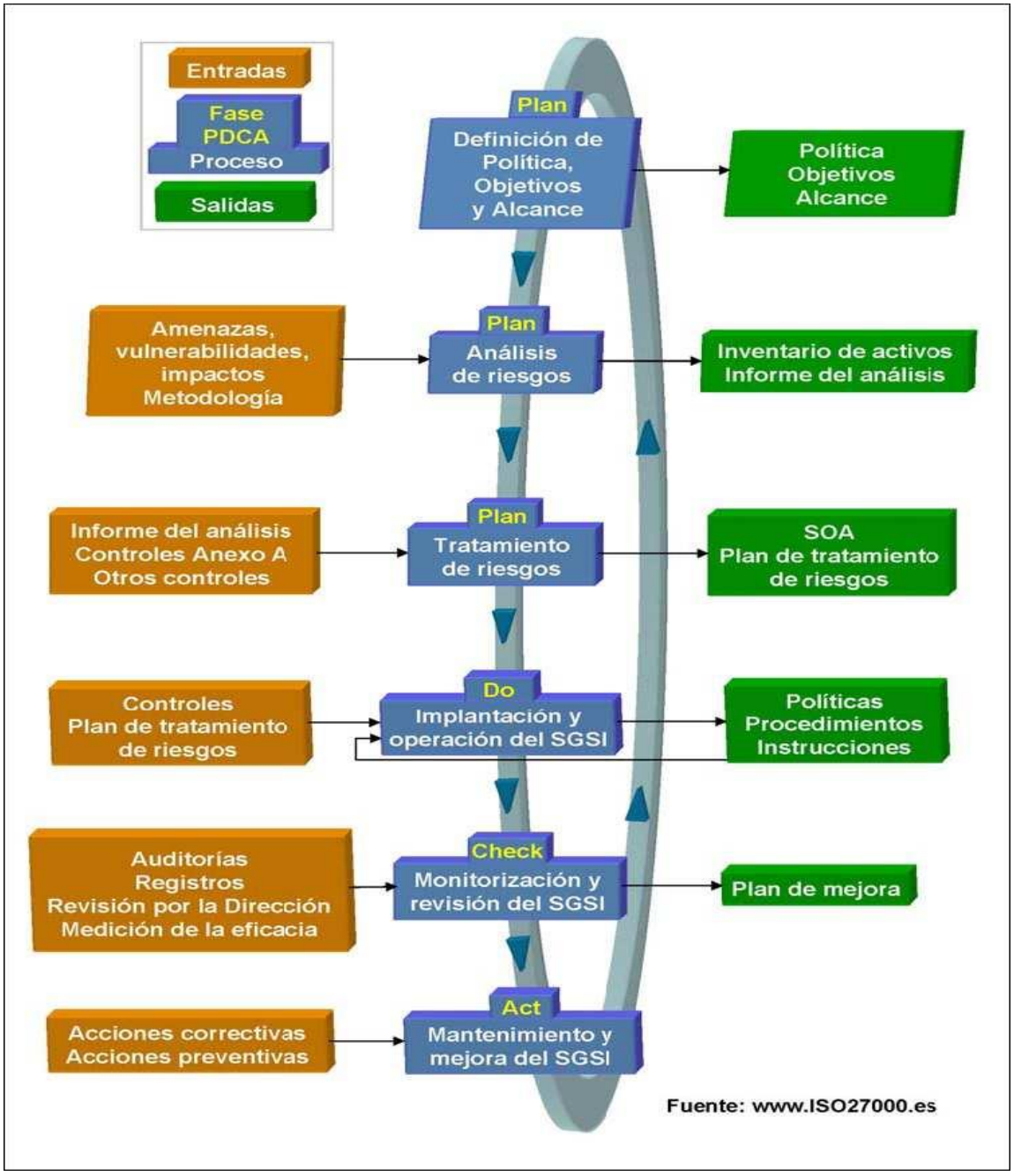

Ilustración 5: Actividades para alcanzar la certificación ISO 27001 del SGSI

Fuente: (Mantilla, 2009)

ISO 27002

ISO 27002:2005 -Anterior ISO 17799:2005-

Esta norma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. En este se pretende abordar los principales contenidos de la norma (mostrados de manera gráfica en el siguiente esquema:

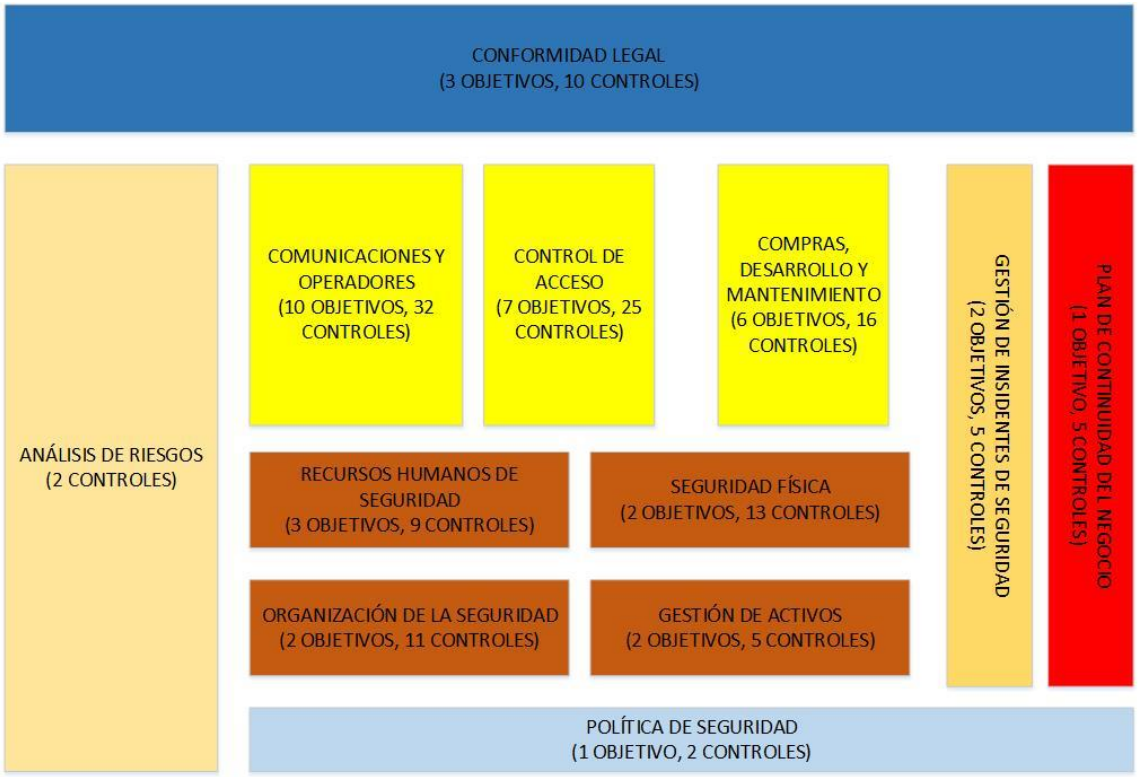

Ilustración 6: ISO 27002:2005

FUENTE: (Getion-calidad, 2009)

Introducción: conceptos generales de seguridad de la información y SGSI.

Campo de aplicación: se especifica el objetivo de la norma.

Términos y definiciones: breve descripción de los términos más usados en la norma.

Estructura del estándar: descripción de la estructura de la norma.

Evaluación y tratamiento del riesgo: indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.

Política de seguridad: documento de política de seguridad y su gestión.

- Aprobada por la Alta dirección.
- Distribuida a los empleados y terceros.
- La Política de seguridad debe revisarse a intervalos o cuando se den cambios significativos.

Aspectos organizativos de la seguridad de la información: organización interna; terceros.

- Creación de un Comité de Gestión de seguridad de la información.
- Definición y asignación de responsabilidades relativas a seguridad.
- Revisión de acuerdos de confidencialidad.
- Identificación de los riesgos del acceso de terceros.
- Tratamiento de la seguridad en la relación con sus clientes.
- La relación de seguridad en contratos con terceros.

Gestión de activos: responsabilidad sobre los activos estableciendo las medidas necesarias para la protección de éstos. Resulta imprescindible:

- Identificación e inventario de los activos de la organización.
- La identificación de un propietario
- Documentar el uso de los activos de la organización.

Seguridad ligada a los recursos humanos: antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.

- Antes del empleo.
    - Asegurar que los empleados, los contratistas y los terceros son adecuados para las funciones que desempeñan.
    - Documentar las funciones de seguridad de los empleados, investigación de antecedentes y las Responsabilidades con respecto a la seguridad de la información.
- Durante el empleo.
    - Asegurar que los empleados, los contratistas y los terceros cumplen con las responsabilidades de seguridad durante su trabajo habitual.
    - Implicación de la dirección, formación y concienciación periódica tanto del personal como de los terceros, etc.
- Cese del empleo
    - Asegurar que los empleados, los contratistas y los terceros abandonan la organización de forma controlada
    - Las responsabilidades en el cese del empleo, devolución de los activos, retirada de los derechos de acceso.

Seguridad física y ambiental: áreas seguras; seguridad de los equipos.

- Prevenir y controlar los accesos físicos en las instalaciones de la organización.
    - Perímetros de seguridad de las instalaciones, controles físicos de entrada, seguridad de oficinas despachos e instalaciones, protección contra las amenazas de origen ambiental, directrices de trabajo en áreas seguras, control de las áreas de acceso público y de carga y descarga.
- Se deben de establecer las medidas necesarias para evitar perjuicios en los activos de la organización.

- Emplazamiento y protección de equipos, instalaciones de suministro eléctrico, seguridad del cableado, mantenimiento de los equipos, seguridad de los equipos fuera de las instalaciones, retirada de materiales propiedad de la organización.

Gestión de comunicaciones y operaciones: se establecen las siguientes disposiciones:

- Responsabilidades y procedimientos de operaciones. Se debe asegurar el funcionamiento correcto y seguro de los procedimientos de seguridad establecidos.
  - Documentación de los procedimientos de operación, gestión de cambios, segregación de tareas, separación de los recursos de desarrollo, prueba y operación.
- Gestión de los servicios prestados por terceros. Se deben de definir los niveles de seguridad apropiados en relación con la seguridad de la información en los servicios prestados por terceros.
  - Comprobación del cumplimiento de los Acuerdos de nivel de servicio acordados con el proveedor, revisión periódica de los servicios prestados por terceros, gestión de cambios de los servicios prestados por terceros.
- Planificación y aceptación del sistema, para minimizar los riesgos de fallos en los sistemas.
  - Gestión de la capacidad monitorizando la capacidad actual y planificando la capacidad futura, aceptación de los sistemas.
- Protección contra código malicioso y descargables para mantener la integridad del software y de la información.
  - Controles contra el código malicioso, controles contra el código descargado en el cliente.
- Copias de seguridad. Mantener la integridad y confidencialidad de la información de la organización.
  - Política de Copias de seguridad documentada.

- Gestión de la seguridad de las redes.
    - Controles de red, seguridad de los servicios de red.
- Manipulación de los soportes para evitar la pérdida de confidencialidad o destrucción no autorizada de activos.
    - Gestión de soportes extraíbles, Procedimiento de retirada de soportes, procedimientos de manipulación de la información, seguridad en la documentación del sistema.
- Intercambio de información. Debe Protegerse la información tanto dentro de la organización como externamente.
    - Políticas y procedimiento de intercambios de información, acuerdos de intercambio, soportes físicos en tránsito, mensajería electrónica.
- Servicios de comercio electrónico. Debe asegurarse la seguridad de los servicios prestados de comercio electrónico.
    - Comercio electrónico, Transacciones en línea.
- Supervisión. Deben controlarse las actividades de procesamiento de la información no autorizadas.
    - Registros de auditoria, procedimiento de supervisión del uso del sistema, protección de la información de los registros, registro de fallos, sincronización de relojes.

Control de acceso: se establecen una serie de controles referidos a:

- Requisitos de negocio para el control de accesos, persiguiendo controlar el acceso a la información.
    - Establecer una política de control de accesos.
- Gestión de acceso de usuarios para asegurar el acceso de los usuarios autorizados.
    - Registro de usuario, gestión de privilegios, gestión de contraseñas de usuarios.
- Responsabilidades de usuario para evitar accesos no autorizados.

    - Uso de contraseña, equipo de usuario desatendido, Política de puesto despejado y mesa limpia.
- Control de acceso a la red evitando así accesos no autorizados a la red.
    - Política de uso de los servicios en la red, autenticación de los usuarios para conexiones externas, identificación de los equipos en las redes, segregación de las redes.
- Control de acceso al sistema operativo para prevenir accesos no autorizados al mismo.
    - Procedimiento seguro de inicio de sesión, identificar y autentificación de usuarios, sistemas de gestión de contraseñas, desconexión automática de sesión, limitación del tiempo de conexión.
- Control de acceso a las aplicaciones y a la información para evitar accesos no autorizados.
    - Restricciones de acceso a la información, aislamientos de sistemas sencillos.
- Ordenadores portátiles y teletrabajo, garantizando la información de los ordenadores portátiles.
    - Política formal de ordenadores portátiles y comunicaciones móviles. Teletrabajo.

Adquisición, desarrollo y mantenimiento de los sistemas de información: este apartado de la norma está referido a:

- Requisitos de negocio para el control de accesos con el objetivo de controlar la seguridad en los sistemas de información.
    - Análisis y especificación de los requisitos de seguridad.
- Tratamiento correcto de las aplicaciones para evitar errores, pérdidas y modificaciones no autorizadas.
    - Validación de los datos de entrada, control del procesamiento interno, integridad de los mensajes, validación de los datos de salida.

- Controles criptográficos. Este punto se centra en proteger la integridad, la autenticidad y confidencialidad por medios criptográficos.
    - Política de uso de controles criptográficos, gestión de claves.
- Seguridad de los archivos de sistemas para asegurar la integridad de los mismos.
    - Procedimiento de control de software en explotación, protección de los datos del sistema y control al código fuente de los programas.
- Seguridad en los procesos de desarrollo y soporte con el fin de asegurar la seguridad de las aplicaciones y software de la organización.
    - Procedimiento de control de cambios, revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo, control de la subcontratación del desarrollo del software.
- Gestión de vulnerabilidades técnica con el objetivo de reducir los riesgos de la explotación de las mismas.
    - Control de las vulnerabilidades técnicas.

Gestión de incidentes de seguridad de la información: como en muchas otras normas ISO éste punto resulta de vital importancia. En él se establecen controles referidos a:

- Notificación de eventos y puntos débiles de la seguridad de la información con el fin de asegurar que se comunican las vulnerabilidades de seguridad para poder emprender acciones correctivas y preventivas para solucionar los incidentes de seguridad detectados.
    - Notificación de los eventos de seguridad, notificación de los puntos débiles de seguridad.
- Gestión de incidentes de seguridad de la información y mejoras para garantizar el tratamiento de la gestión de los mismos.
    - Procedimiento para la gestión de los incidentes de seguridad, analizar las incidencias de seguridad, recopilación de evidencias.

Gestión de la continuidad del negocio: aspectos de la seguridad de la información en la gestión de la continuidad del negocio. Con este apartado se pretende contrarrestar las interrupciones que puedan afectar al negocio ante fallos importantes en los sistemas y garantizar la oportunidad de reanudarlos.

- Desarrollo y mantenimiento de un proceso para la continuidad del negocio, relacionado con el análisis de riesgos, desarrollo de planes para la vuelta a la situación anterior lo antes posible, coherencia entre los diferentes planes de continuidad del negocio, realización de pruebas de los planes de continuidad del negocio.

Cumplimiento: cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.

- Identificación de los requisitos legales, procedimiento control de los derechos de propiedad intelectual, protección de los procedimientos de la organización, cumplimiento de la LOPD, regulación de legislación criptográfica.
- Cumplimiento de las políticas y normas, comprobación cumplimiento técnico. (Getion-calidad, 2009)

MÉTODO PDCA

Parte integral del método de mejora continua es conocida por los japoneses por la rueda Deming o el ciclo Deming. El ciclo Deming o ciclo Planear-Hacer-Estudiar-Actuar, puede tener un sentido intuitivo para muchos, puesto que se deriva del método científico. Pero para hacer que todo mundo lo use para mejorar los procesos, debemos definirlo operativamente, como dice el doctor Deming. En *The Deming Route to Quality and Productivity* hice una breve descripción del ciclo Deming. La descripción

que hago va mucho más allá que de mis trabajos anteriores. Debemos definir operativamente el ciclo Deming, fijando una serie de 8 pasos de acción. Son los suficientemente genéricos para que cualquiera vea sus relevancias, y lo suficientemente específicos para que lo siga cualquier gerente de procesos. (Scherkenbach, 1994).

La tabla 3 - tres - muestra los pasos del ciclo de Deming fácilmente entendibles:

Pasos del Ciclo de Deming

PASOS DEL CICLO DE DEMING	
	I. PLAN
	Desarrolle un Plan para mejorar
Paso 1:	Identifique la oportunidad de mejora.
Paso 2:	Documente el proceso presente.
Paso 3:	Cree una visión del proceso mejorado.
Paso 4:	Defina los limites-scope- del esfuerzo de mejora.
	II. HACER
	Lleve a cabo el plan
Paso 5:	Con clientes, y durante algún tiempo, haga una pequeña escala piloto de los cambios propuestos.
	III. VERIFICAR
	Estudie los resultados
Paso 6.	Observe lo apropiado acerca de la mejora del proceso.
	IV. ACTUAR
	Ajuste el proceso basado en sus nuevos conocimientos.
Paso 7:	Haga operativa la nueva mezcla de recursos.
Paso 8:	Repita los pasos-ciclo- en la primera oportunidad.

Tabla 3: Pasos del Ciclo de DEMING

Fuente: (Scherkenbach, 1994)

El Método PHVA -PDCA en inglés- es una metodología de mejora continua, diseñada por el Dr. Walter Shewhart en 1920 y presentada por Deming a partir del año 1950, la cual se basa en un ciclo de cuatro -4- pasos: Planificar –Plan-, Hacer –Do-, Verificar –Check- y Actuar –Act-.

Ilustración 7: PDCA

Fuente: (ISO, 2012)

PLANIFICACIÓN

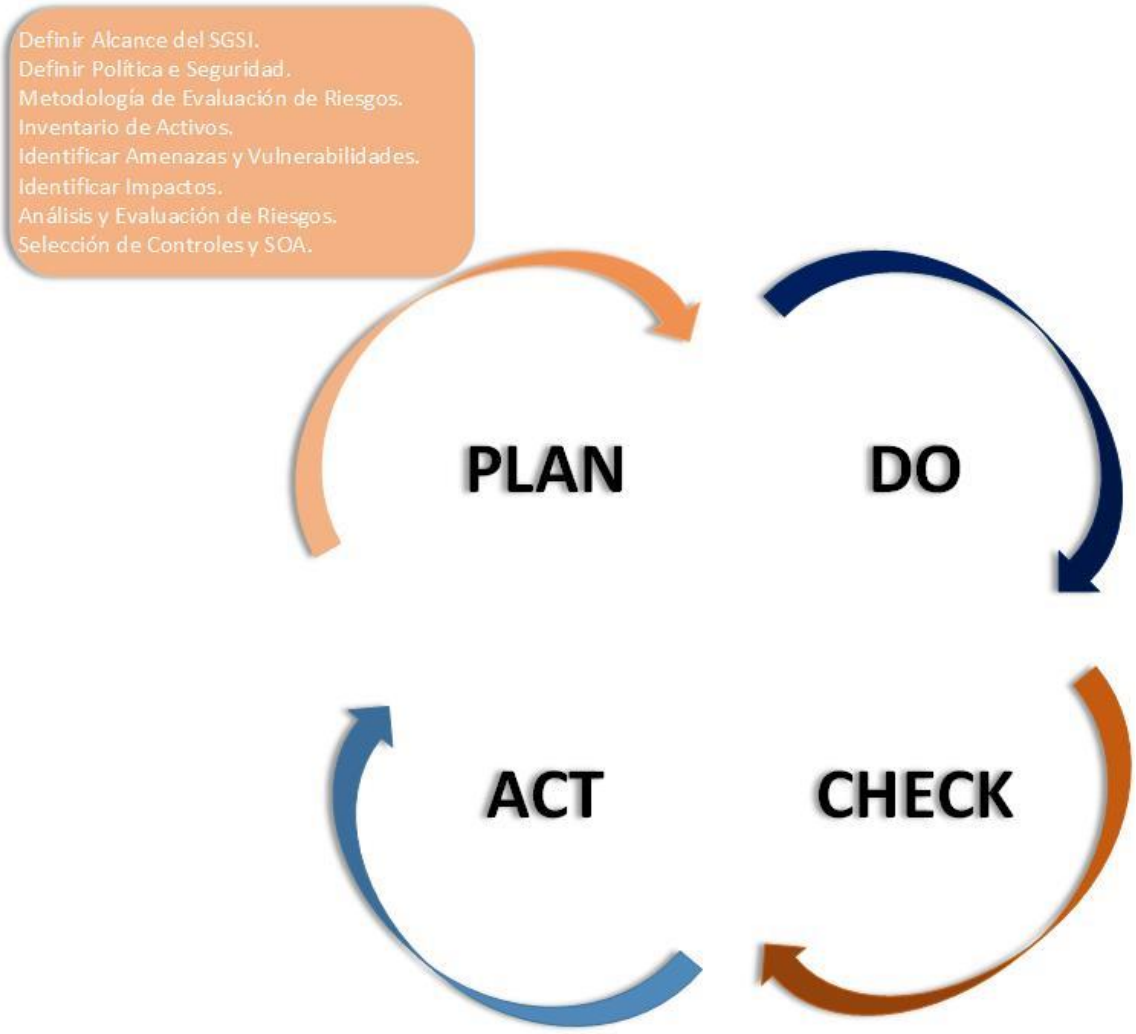

Ilustración 8: Planear

Fuente: (ISO, 2012)

• Definir alcance del SGSI: en función de características del negocio, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI -el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado-.

• Definir política de seguridad: que incluya el marco general y los objetivos de seguridad de la información de la organización, tenga en cuenta los requisitos de negocio, legales y contractuales en cuanto a seguridad, esté alineada con la gestión de riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de declaración de intenciones de la Dirección, por lo que no pasará de dos o tres páginas.

• Definir el enfoque de evaluación de riesgos: definir una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla -en el futuro, ISO 27005 proporcionará ayuda en este sentido-. El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

• Inventario de activos: todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

• Identificar amenazas y vulnerabilidades: todas las que afectan a los activos del inventario.

• Identificar los impactos: los que podría suponer una pérdida de la confidencialidad, la integridad o la disponibilidad de cada uno de los activos.

• Análisis y evaluación de los riesgos: evaluar el daño resultante de un fallo de seguridad -es decir, que una amenaza explote una vulnerabilidad- y la probabilidad de ocurrencia del fallo; estimar el nivel de riesgo resultante y determinar si el riesgo es aceptable -en función de los niveles definidos previamente- o requiere tratamiento.

• Identificar y evaluar opciones para el tratamiento del riesgo: el riesgo puede reducido -mitigado mediante controles-, eliminado -p. ej., eliminando el activo-, aceptado -de forma consciente- o transferido -p. ej., con un seguro o un contrato de outsourcing-.

• Selección de controles: seleccionar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 -teniendo en cuenta que las exclusiones habrán de ser justificadas- y otros controles adicionales si se consideran necesarios.

• Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles -el "riesgo cero" no existe prácticamente en ningún caso-.

• Confeccionar una Declaración de Aplicabilidad: la llamada SOA -Statement of Applicability- es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

IMPLEMENTACIÓN

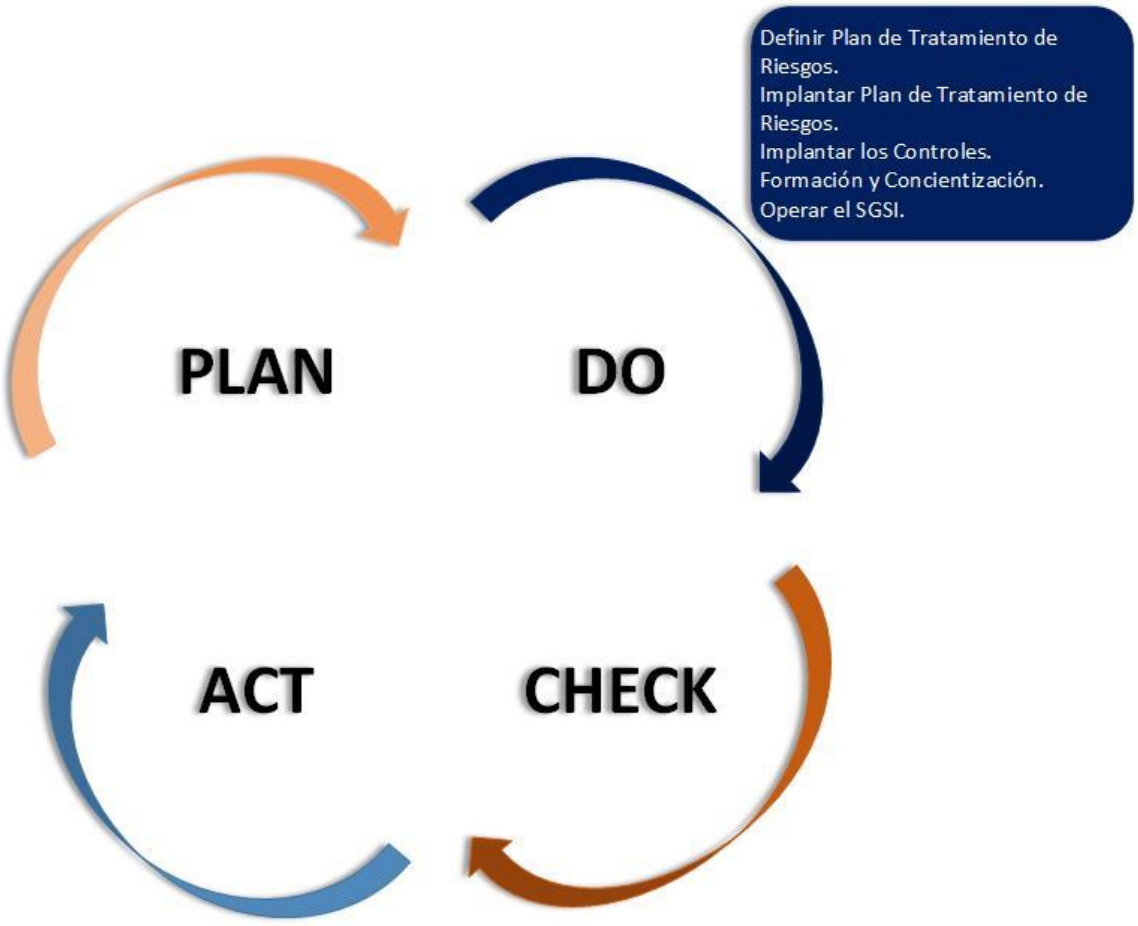

Ilustración 9: HACER

Fuente: (ISO, 2012)

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

• Implantar plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.

• Implementar los controles: todos los que se seleccionaron en la fase anterior.

• Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.

• Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

• Gestionar las operaciones del SGSI y todos los recursos que se le asignen.

• Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

SEGUIMIENTO

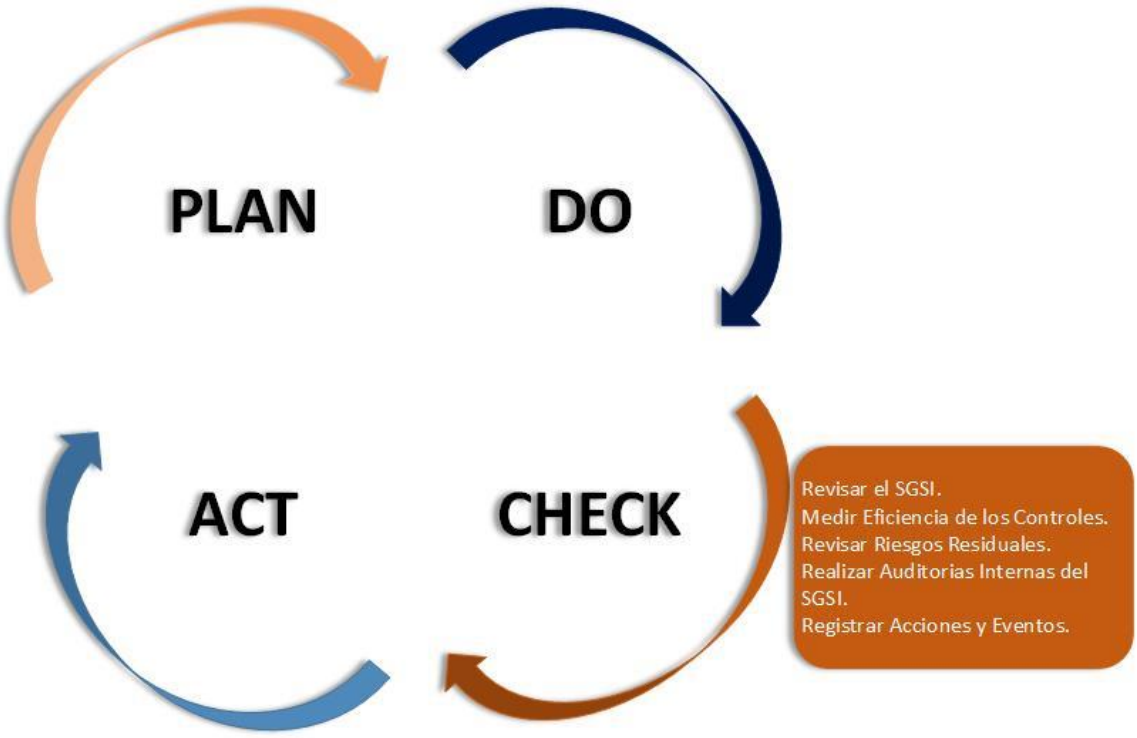

Ilustración 10: Verificar

Fuente: (ISO, 2012)

• Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.

• Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

• Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad.

•Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

• Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con los requisitos de ISO 27001, el entorno legal y los requisitos y objetivos de seguridad de la organización, están implementados y mantenidos con eficacia y tienen el rendimiento esperado.

• Revisar regularmente el SGSI por parte de la Dirección: para determinar si el alcance definido sigue siendo el adecuado, identificar mejoras al proceso del SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

• Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización y las revisiones.

• Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

MEJORA CONTINUA

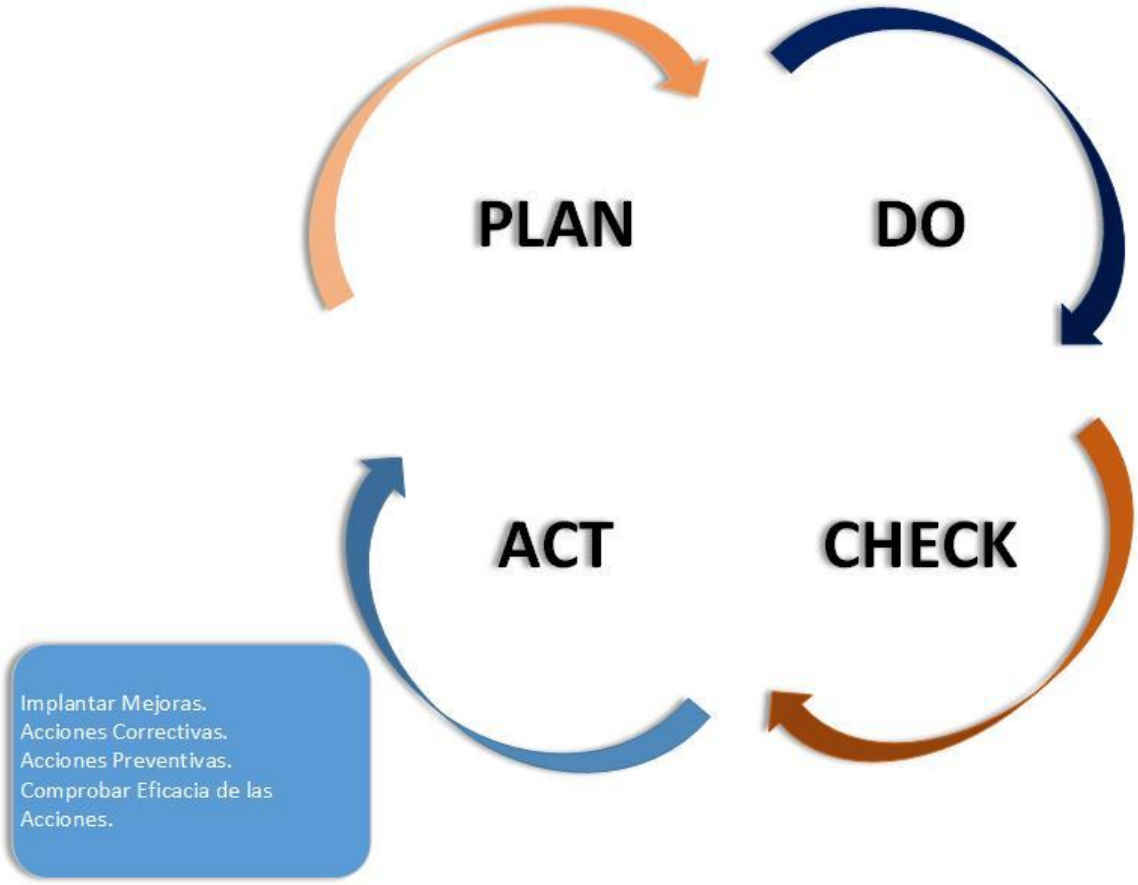

Ilustración 11: ACTUAR

Fuente: (ISO, 2012)

• Implantar mejoras: poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

• Acciones correctivas: para solucionar no conformidades detectadas.

• Acciones preventivas: para prevenir potenciales no conformidades.

• Comunicar las acciones y mejoras: a todos los interesados y con el nivel adecuado de detalle.

• Asegurarse de que las mejoras alcanzan los objetivos pretendidos: la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

1.3 DEFINICIÓN DE TÉRMINOS BÁSICOS

SIMTRAC: Sistema de Información y Monitoreo de Trafico Acuático.

COSPAS SARSAT – COSPAS: Sistema Espacial para la Búsqueda de Buques en Peligro y SARSAT Rescate por Satélite de Seguimiento Asistido.

Amenaza: Es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir daño -material o inmaterial- sobre los elementos -activos, recursos- de un sistema.

Ataque: Es una amenaza que se convirtió en realidad, es decir cuando un evento se realizó. No dice nada si o no el evento fue exitoso.

Autenticidad: La legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable.

Confidencialidad: Datos solo pueden ser legibles y modificados por personas autorizados, tanto en el acceso a datos almacenados como también durante la transferencia de ellos.

Disponibilidad: Acceso a los datos debe ser garantizado en el momento necesario. Hay que evitar fallas del sistema y proveer el acceso adecuado a los datos.

Elementos de Información: También Activos o Recursos de una institución que requieren protección, para evitar su pérdida, modificación o el uso inadecuado de su contenido, para impedir daños para la institución y las personas que salen en la información. Se distingue y divide tres grupos, a) Datos e Información, b) Sistemas e Infraestructura y c) Personal.

Gestión de Riesgo: Método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. Está compuesta por cuatro fases: 1) Análisis, 2) Clasificación, 3) Reducción y 4) Control de Riesgo.

Integridad: Datos son completos, non-modificados y todos los cambios son reproducibles -se conoce el autor y el momento del cambio-.

Seguridad Informática: Procesos, actividades, mecanismos que consideran las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

Vulnerabilidad: Son la capacidad, las condiciones y características del sistema mismo -incluyendo la entidad que lo maneja-, que lo hace susceptible a amenazas, con el resultado de sufrir algún daño.

ISO: International Organization for Standarization -Organización Internacional para la Estandarización. (ISO, The International Organization for Standardization, 2014)

SGSI: Sistema de Gestión de Seguridad de la Información

NTC-ISO/IEC 27001:2006 estándar para la seguridad de la información Information technology - Security techniques - Information security management systems – Requirements-; aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Norma ISO 9001:2008 elaborada por la Organización Internacional para la Estandarización –ISO-, determina los requisitos para un Sistema de gestión de la calidad –SGC- (Vinca, 2011)

RTO -Tiempo de Retorno Objetivo-

IRAM: Instituto Argentino de Normalización (IRAM, 2014)

La confidencialidad: garantiza que la información sea accesible sólo por aquellas personas autorizadas.

La integridad: garantiza la exactitud y totalidad de la información y los métodos de procesamiento.

La disponibilidad: garantiza que los usuarios autorizados tengan siempre acceso a la información y a los recursos relacionados con ella

La norma ISO 15408 es una norma que contiene criterios de evaluación de la seguridad de tecnologías de la información -Information technology -- Security techniques -- Evaluation Criteria for IT security- (commoncriteria, 2013)

Activos de Información: Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información como lo puede ser Bases de Datos con usuarios, contraseñas, números de cuentas, etc.

Seria crítico que a una entidad que maneja alta información confidencial, los intrusos pudieran acceder a ella afectando así la confidencialidad, la disponibilidad y la integridad de dicha información por eso algunas de tantas entidades adoptan un plan de seguridad para los activos de información y así no tener la desgracia de que los datos se fuguen, se modifiquen o se pierdan. (WordPress, 2013).

Matriz RACI: La matriz de la asignación de responsabilidades -RACI por las iniciales de los tipos de responsabilidad- se utiliza en la gestión del personal para relacionar actividades con los individuos. De esta manera se logra

asegurar que cada uno de los componentes del alcance esté asignado a un individuo o grupo de individuos. Fuente: (Netec, 2014)

PDA: Procesamiento de Datos.

CAPÍTULO II: METODOLOGÍA

En este capítulo tiene como objetivos determinar el material a ser usado y especificar la metodología a utilizar, para realizar la investigación de la tesis.

2.1 MATERIAL

Se listara a continuación los materiales informáticos que ayudaron a la elaboración de la tesis en todas sus fases del PDCA fueron los siguientes:

Microsoft Office 2013 en las siguientes herramientas

Procesador de texto Microsoft Word

Procesador de Cálculos Excel

Diseñador de Procesos Visio

Procesador de texto PDF.

Adobe Acrobat.

2.2 MÉTODO

Serán los procedimientos a seguir que nos permita elaborar los pasos para desarrollar esta tesis.

PLANEAMIENTO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN USANDO LA NORMA TÉCNICA PERUANA -ISO/IEC 27001:2008

En el desarrollo del Plan de SGSI utilizamos la metodología propuesta dividida en tres partes: La primera son las entradas que corresponden al Talento Humano, los Recursos Tecnológicos y Sistemas de Información; la segunda son los procedimientos basado en la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 que promueve la adopción del método PHVA – Planear, Hacer, Verificar y Actuar o PDCA en sus siglas en inglés – Plan, Do, Check and Act -; en la que enmarcaremos cada una de las etapas para mejorar la Seguridad de la Información en la organización y finalmente la tercera es la salida con el Plan de SGSI para la organización.

Gráfico de la Metodología usando PDCA de la NORMA TÉCNICA PERUANA - ISO/IEC 27001:2008.

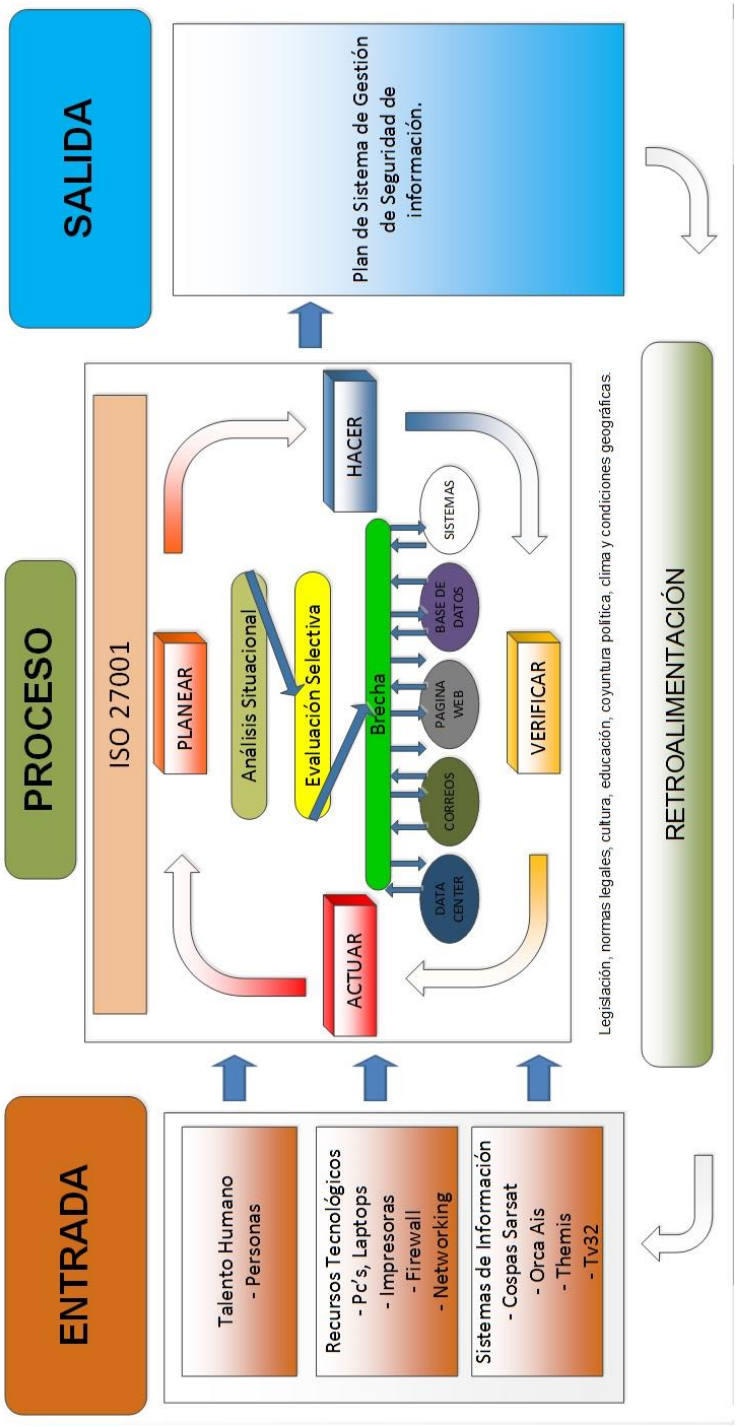

Ilustración 12: Método Propio usando PDCA

Fuente: Elaborado por los Autores

La ilustración 12 – doce – se muestra la metodología a emplear para esta tesis; consta de tres grandes partes:

ENTRADAS

Las Entradas son requerimientos indispensables para el proceso a realizar como base para la metodología propuesta.

Plantilla para el Talento Humano

Esta plantilla nos mostrara los principales campos característicos de las personas que laboran en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología y luego poder procesarla.

Personas

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
Número de orden	Grado militar	Especialidad militar	Apellidos y nombres del personal	Número del Código de identidad	Área de destaque del personal militar	Cargo que ejerce en el área de destaque

Tabla 4: Plantilla Personas

Fuente: Elaborado por los Autores

Plantilla para los Recursos Tecnológicos

Esta plantilla nos mostrara los principales campos característicos de los recursos tecnológicos que se encuentran en la Comandancia de Operaciones Guardacostas; necesarios para las labores cotidianas y es requerimiento de entrada para nuestra metodología para luego poder procesarla.

Recursos Tecnológicos

Num	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
Número de orden	Marca del recurso tecnológico	Velocidad del procesamiento	Especio de almacenamiento	Memoria física del recurso tecnológico	Sistema operativo del recurso tecnológico	Servicio que brinda el recurso tecnológico	Sistema o aplicación que se encuentra en el recurso tecnológico	Fecha de ingreso a la comandancia	Estado en que se encuentra el recurso tecnológico

Tabla 5: Plantilla Recursos Tecnológicos

Fuente: Elaborado por los Autores

Plantilla para los Sistemas de Información

Esta plantilla nos mostrara los principales campos característicos de los sistemas de información que se encuentran en la Comandancia de Operaciones Guardacostas; necesarios para las labores cotidianas y es requerimiento de entrada para nuestra metodología y luego poder procesarla.

Sistemas de Información

Número	Tipo de sistema	Nombre	Proveedor	Versión	Responsable	Fecha Ingreso	Estado
Número de orden	Aplicativos / base de datos / web	Nombre del sistema de información	Proveedor del sistema de información de quien fue adquirido	Versión del sistema de información	Persona responsable del sistema de información	Fecha de adquisición del sistema de información	Estado en que se encuentra el sistema de información

Tabla 6: Plantilla Sistemas de Información

Fuente: Elaborado por los Autores

NOTA: El resumen de los totales se encuentra en el apartado 10.1

PROCESOS

Los procesos dentro de la metodología propuesta están basados en el ciclo de vida Deming o conocido también con el nombre de Ciclo PDCA por

sus siglas en inglés o PHVA en castellano – Planear, Hacer, Verificar y Actuar.

El Plan de SGSI coge el Ciclo de Deming para su desarrollo y este análisis se realizara en la página 124.

Se analizará y diseñará en base a la metodología vista en los puntos:

Bases Metodológicas

Capítulo 2 – Página 124	**Fases PDCA**
Página 131	Planear
Página 148	Hacer
Página 179	Verificar
Página 187	Actuar

Tabla 7: Procesos (Capítulos y Fases)

Fuente: Elaborado por los Autores

De la metodología propuesta en esta parte del Proceso se desprende el análisis que nos permite realizar un nexo entre las deficiencias encontradas con las clausulas, objetivos de control y controles de la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 que ayudaran a mitigar dichas deficiencias; esto se muestra en la ilustración 13 – trece-.

Gráfico del Análisis y Diseño del cruce de información de las deficiencias encontradas y los objetivos de control y controles de la NORMA TÉCNICA PERUANA -ISO/IEC 27001:2008.

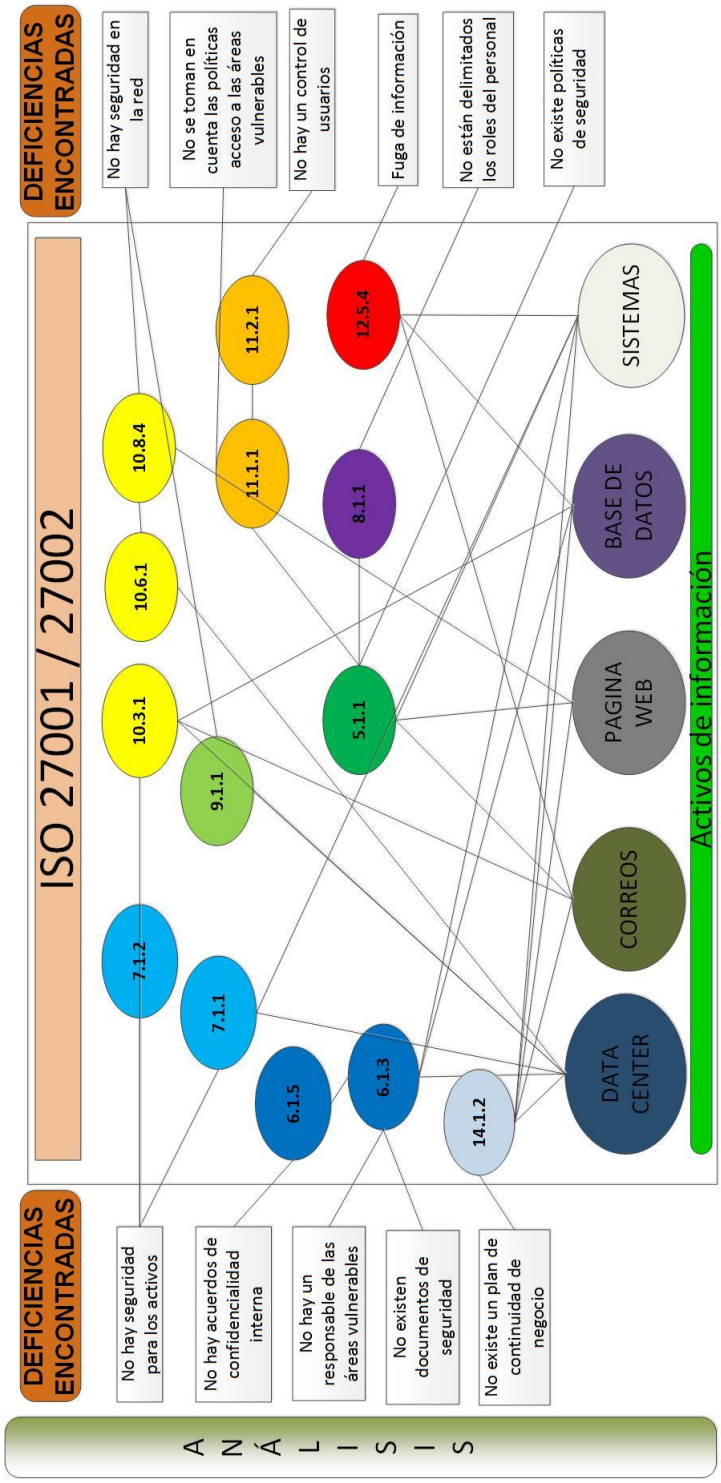

Ilustración 13: Deficiencias Encontradas vs Objetivos de Control y Controles NTP -ISO/IEC 27001:2008.

Fuente: Elaborado por los Autores

En la ilustración 13, se encuentra un resumen general de la metodología propuesta, se cruzan las deficiencias encontradas con las clausulas, objetivos de control y controles asociándolas con los activos de información; en el análisis y diseño de la tesis, se profundiza en cada punto de la metodología de las diferentes etapas del ciclo de Deming, ayudándonos a analizar y diseñar herramientas para cumplir los requisitos exigidos por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008.

SALIDAS

Al finalizar los procesos dentro de la metodología propuesta se tendrá un producto como salida que será el Plan de Sistema de Gestión de Seguridad de la Información SGSI.

Este Plan se analizará y diseñará en base a la metodología vista en los puntos.

Plan de Sistema de Gestión de Seguridad

Capítulo 2 – Página 124	**HACER**
Página 148	Controles para las áreas del SIMTRAC y cosas – SARSAT establecidos en la norma técnica peruana NTP-ISO/IEC 27001:2008

Tabla 8: Plantilla Plan de SGSI

Fuente: Elaborado por los Autores

Ciclo PDCA para el SGSI

El diseño metodológico de esta tesis se basa en la metodología PDCA de la norma ISO 27001 para el Plan de SGSI, en la siguiente figura se pone

en contexto la metodología propuesta en este documento dentro de cada etapa del ciclo.

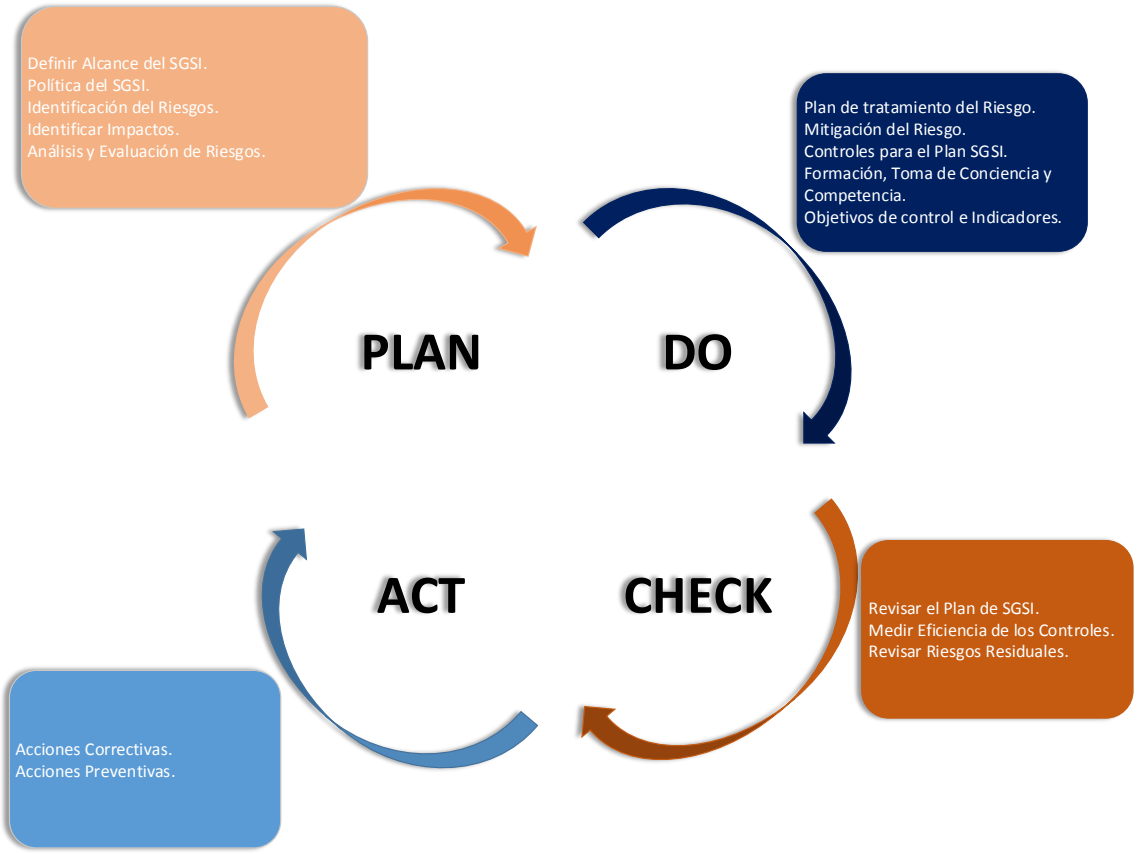

Ilustración 14: Ciclo PDCA para el Plan SGSI

Fuente: (ISO, 2012)

En esta figura contiene un resumen general de la metodología propuesta, basada en el Modelo de aplicación, y en Método PDCA en el desarrollo de la tesis, se profundiza en cada entregable de las diferentes etapas del ciclo, ayudándonos a desarrollar herramientas para cumplir los requisitos exigidos por la Norma ISO 27001.

PLAN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Tabla de correlación de las normas ISO 27001 y 27002 que se utilizara para el análisis y diseño del Plan de Sistema de Gestión de Seguridad de la Información.

Correlación de las Normas ISO 27001 y 27002

METODOLOGÍA	CAPÍTULO ISO 27001	CAPÍTULO ISO 27002
PLANEAR	4.2.1	
HACER	4.2.2 Y 5.2.2	5. A 15
VERIFICAR	4.2.3, 6 Y 7	
ACTUAR	4.2.4 Y 8	

Tabla 9: Correlación de las Normas ISO 27001 / 27002

Fuente: Elaborado por los Autores

PLANEAR

En la fase de Planear de la Metodología se analiza el alcance del Plan del SGSI; las políticas y lineamientos sobre los que se desarrollará; también se presentaran herramientas para la identificación del riesgo, del impacto y se analizará y evaluaran los riesgos, según el tipo de activo de información que se afectaría.

Entrada:

- Requerimiento del Cliente.
- Necesidades del Cliente.

Salida:

- Plan Estratégico.

Ilustración 15: Proceso Planear

FUENTE: Elaborado por los Autores

ALCANCE DEL PLAN SGSI

En primera medida la organización debe establecer el alcance del Plan Sistema de Gestión de Seguridad en la Información -SGSI-, el alcance no implica abarcar toda la organización; es recomendable empezar por un alcance limitado, en el que se involucren los procesos core o que contengan la información más relevante para la organización.

Es importante en el momento de definir el alcance, los requisitos legales y contractuales relacionados con la seguridad de la información deben quedar contemplados también dentro del alcance del sistema.

Cualquier otro proceso que la organización considere incluir dentro del Plan del SGSI es válido, lo que se recomienda es que la decisión de incluir más procesos sea con base en un análisis que en efecto sugiera la importancia de incluir dicho proceso, no se quiere hacer un Plan de SGSI muy robusto y poco efectivo, por el contrario, hacerlo lo más simple posible es una buena práctica, más aun cuando la organización empieza desde ceros el desarrollo del Sistema.

POLÍTICA DEL PLAN SGSI

Considerando los objetivos de la organización se elaborará el Plan de SGSI.

No es parte de esta tesis establecer los lineamientos para el desarrollo de la planeación estrategia; es por eso que se asumirá su existencia. En caso que no existiese, se recomienda establecerlo previamente y se sugiere consultar la norma ISO9001:2008.

La política del Plan del SGSI entonces, debe estar alineada con los objetivos organizacionales, es allí donde la jefatura de la comandancia debe establecer un marco de referencia para posteriormente fijar objetivos específicos de control por cada proceso de la compañía, los cuales deben establecerse en conjunto con el líder de cada proceso.

Ilustración 16: Política del SGSI

Fuente: Elaborado por los Autores.

La política del Plan SGSI debe tener en cuenta el marco legal de la Resolución del Consejo Nacional de la Magistratura:

- Nro.246-2007-PCM Resolución Ministerial para el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de Seguridad de la Información.
- Nro. 129-2012-PCM; Resolución Ministerial para el uso obligatorio de las NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información; Técnicas de

Seguridad; Sistemas de Gestión de Seguridad de la Información. Cuyos controles deberán se implementados a las recomendaciones de las NTP-ISO/IEC 17799:2007.

- Nro. 219 -2013-P-CNM; Normas y Procedimientos para la Administración de Cuentas y Claves de Acceso a los Usuarios y el Uso de los Servicios de Correo Electrónico e Internet en el Consejo Nacional de la Magistratura.

Se debe dejar en claro que el impacto de los objetivos genera mayor claridad de la razón de ser de los mismos y un mayor compromiso por parte de los responsables.

La gestión de riesgo en la seguridad de la información, inicia al establecer el contexto, este se refiere a la definición del alcance, límites y la política del Plan SGSI, con el fin de asegurar que todos los activos de información de la organización se contemplen en el Plan SGSI. Es importante tener en consideración para los límites y criterios de aceptación de los riesgos: el tiempo, costo, recursos, impactos y requisitos legales para implementar los controles.

IDENTIFICACIÓN DEL RIESGO

La identificación del riesgo contempla inicialmente la determinación de los activos de información dentro del alcance del Plan del SGSI, teniendo en cuenta la ubicación, responsable y funciones. De igual manera se deben determinar las amenazas, vulnerabilidades e impactos en la organización, por las posibles pérdidas de confiabilidad, integridad y disponibilidad sobre los activos.

De acuerdo a lo anterior se realiza un inventario de activos de información relacionando cada proceso de la organización contemplado en el alcance del Plan SGSI (Anexo B), los activos hacen referencia a: personal de

la organización, información, sistemas de información, procesos, aplicaciones y el entorno físico.

Se estableció el Inventario de activos de información para las áreas de COSPAS SARSAT y SIMTRAC de acuerdo al formato diseñado en el anexo B. En el numeral 3.1.1.4 se realiza la identificación del impacto para completar el formato.

La tabla 10 - diez - muestra este formato aun sin llenar los datos requeridos como los riesgos que influyen directamente a los activos ni tampoco su Confidencialidad, Integridad y Disponibilidad.

Inventario de Activos de Información

INVENTARIO DE ACTIVOS DE INFORMACIÓN								
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
Componentes del Servicio	Personal Destacado al Área		Usuario	Jefe del Área	Pool de Operaciones			
	Instalaciones físicas		Organización	Jefe de la Comandancia	Coordenadas de la Organización			
	Sistemas Operativos		Software	PDA	Oficinas			
	Estaciones de Trabajo		Hardware	PDA	Oficinas y Pool de Operaciones			
	Servidores		Hardware	Administrador de Servidores	Salas de Servidores			
	Sistemas de Información Servidores		Software	Administrador de Servidores	Salas de Servidores			
	Imagen Organizacional		Organización	Relaciones Publicas	Área de Relaciones Publicas			
	Información de Embarcaciones		Información	Técnico a Cargo	Base de Datos			

INVENTARIO DE ACTIVOS DE INFORMACIÓN									
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
	Informe de Operaciones		Información	Oficial a Cargo	Estación de Trabajo			
	Equipos de Comunicación		Hardware y Red	Jefe de Electrónica	Área de Electrónica			

Tabla 10: Inventario de Activos de Información

Fuente: Elaborado por los Autores

Leyenda C, I y D

C:	Confidencialidad
I:	Integridad
D:	Disponibilidad

Tabla 11: Leyenda Inventario de Activos de Información

Fuente: Elaborado por los Autores

Los conceptos de amenaza y vulnerabilidad es recomendado tenerlos claros; estos se encuentran en el apartado 1.3 DEFINICIONES DE TÉRMINOS BÁSICOS.

En el análisis de las amenazas y vulnerabilidades se requiere:

- Realizar una lista de las amenazas que puedan presentarse en forma accidental o intencional en la organización con relación a los activos de información.
- Identificar los riesgos internos.
- Identificar los riesgos externos.
- Realizar un análisis del entorno en los fenómenos naturales, el ambiente político y el ambiente tecnológico que rodea a la organización para definir las amenazas a las que pueden estar expuestos los activos.

Ilustración 17: Amenazas y riesgos identificados en la organización

Fuente: Elaborado por los Autores

IDENTIFICACIÓN DEL IMPACTO

Conociendo los activos de información de la organización, se analizará el impacto que tendría en cuestión de pérdida o alteración de cada uno de los activos identificados.

Se comprenderá el impacto como el grado en el que se ve afectado determinado activo de información, al alterar uno de sus componentes, para este caso activos de información. Cuanto más grande sea la correlación del resultado y la alteración del activo, el impacto de ese activo será mayor. La evaluación del impacto viene de criterios subjetivos de los conocedores del

sistema, acá se proponen 3 –tres- requisitos de los activos de información de una organización, como lo describe la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 -Confidencialidad, Integridad y Disponibilidad-, de los cuales se cuantificara el impacto que tiene dentro de su sistema.

Establecimos 3 niveles de impacto -bajo, mediano y alto- según se comporte el activo de información, en el momento de decidir cuál de los 3 niveles aplica para cada categoría, se conforma un grupo interdisciplinario y se da un espacio abierto para la discusión, la cuantificación final debe salir de un acuerdo general de este equipo interdisciplinario, esto debe hacerse tomando activo por activo, evaluando los 3 requisitos antes de continuar con el siguiente.

A continuación se describen los requisitos para hacer la identificación del impacto; Identificando el valor del Activo, la clase del activo y una breve descripción del mismo en las tablas siguientes de Requisitos de Confidencialidad – C -; Requisitos de Integridad – I – y Requisitos de Disponibilidad – D - respectivamente:

Requisitos de Conformidad (C)

REQUISITOS DE CONFIDENCIALIDAD (C)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Disponible al público	La información no sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles para el público.

REQUISITOS DE CONFIDENCIALIDAD (C)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
2. MEDIANO	Para uso interno exclusivamente o uso restringido solamente	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público o la información restringida y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles dentro de la organización con restricciones variadas con base en las necesidades de la empresa.
3. ALTO	Confidencial o estrictamente confidencial	La información sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles sólo sobre la base de la necesidad del conocimiento, o la información sensible y las instalaciones de procesamiento de información y los recursos del sistema están disponibles sólo sobre la base de la necesidad estricta del conocimiento.

Tabla 12: Requisitos de Confidencialidad

Fuente: (ISO, 2012)

Requisitos de Integridad (I)

REQUISITOS DE INTEGRIDAD (I)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Baja integridad	El daño o modificación no autorizada no es crítico para las aplicaciones organizacionales y el impacto en la organización es insignificante o menor.
2. MEDIANO	Integridad mediana	El daño o modificación no autorizada no es crítico pero si es notorio para las aplicaciones organizacionales y el

REQUISITOS DE INTEGRIDAD (I)		
VALOR DEL	CLASE	DESCRIPCIÓN
		impacto en la organización es significativo.
3. ALTO	Integridad alta o muy alta	El daño o modificación no autorizada es crítica para las aplicaciones organizacionales y el impacto en la organización es importante y podría conllevar a la falta grave o total de la aplicación empresarial.

Tabla 13: Requisitos de Integridad

Fuente: (ISO, 2012)

Requisitos de Disponibilidad (D)

REQUISITOS DE DISPONIBILIDAD (D)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
1. BAJO	Disponible al público	La información no sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles para el público.
2. MEDIANO	Para uso interno exclusivamente o uso restringido solamente mediana	La información no sensible está restringida para uso interno exclusivamente, es decir, no está disponible para el público o la información restringida y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles dentro de la organización con restricciones variadas con base en las necesidades de la empresa.
3. ALTO	Confidencial o estrictamente confidencial	La información sensible y las instalaciones de procesamiento de la información y los recursos del sistema están disponibles sólo sobre la base de la necesidad del conocimiento, o la información sensible y las instalaciones de procesamiento de información y los recursos del sistema están

REQUISITOS DE DISPONIBILIDAD (D)		
VALOR DEL ACTIVO	CLASE	DESCRIPCIÓN
		disponibles sólo sobre la base de la necesidad estricta del conocimiento.

Tabla 14: Requisitos de Disponibilidad

Fuente: (ISO, 2012)

Se debe tener en cuenta los controles existentes en la organización para reducir los riesgos, ya que esto puede variar la valoración del impacto y las consecuencias sobre un activo de información. Por ejemplo, se analizan las condiciones de instalaciones físicas de la organización, construcción, ubicación y alrededores, esto debe generar cierta seguridad que puede extenderse a los activos de información, y de esta manera la valoración del impacto es diferente.

Cuanto más exacto sea el análisis considerando la realidad actual de la organización más provechoso será el resultado de evaluación del impacto.

Para el formato propuesto en el Anexo B del inventario de activos, se realizó la identificación del impacto a los activos de las áreas del COSPAS SARSAT y del SIMTRAC, evaluando los requisitos de confidencialidad, integridad y disponibilidad; esta identificación se realiza en el apartado 3.1.1.4 del CAPíTULO DE DESARROLLO DEL PROYECTO.

ANÁLISIS Y EVALUACIÓN DEL RIESGO

La estimación del riesgo es un paso muy importante, lo cual debemos valorar y determinar su importancia; puede ser cuantitativa al definir escalas de ocurrencia o cualitativa al usar escalas numéricas. El objetivo de esta etapa es obtener una lista de riesgos identificados de acuerdo a la probabilidad de ocurrencia de una amenaza y de sus consecuencias de los impactos, ligadas a las vulnerabilidades existentes a los activos de información. El Riesgo se compone de tres elementos. (Moreno, 2009)

Riesgo= activo de información + probabilidad + impacto

Para la estimación del riesgo, se empleará la matriz de Análisis Modal de Fallos y Efectos AMFE. Esta herramienta es una de las conocidas, empleadas en el ámbito de la Calidad para la identificación y análisis de principales desviaciones de funcionamiento o fallos. Se trata de un método cualitativo que por sus características, resulta de utilidad para identificar los puntos de fallo potenciales, y elaborar planes de acción para combatir los riesgos, y facilitar acciones en prevención de riesgos. (Bestratén M. Orriols, 2010)

A continuación, detallaremos conceptos de cómo funciona el método:

Detectabilidad

Si durante el componente de servicio se produce un fallo o cualquier output defectuoso, se trata de averiguar la probabilidad que no lo detectemos, pasando a etapas posteriores en el componente de servicio, generando los consiguientes problemas y llegando en último término a afectar al usuario final, en este caso al propietario del activo de información y si es el caso a toda la organización. Cuanto más difícil sea detectar el fallo existente y más se tarde en

detectarlo más importantes pueden ser las consecuencias del mismo; es decir el impacto del riesgo generado en el activo es mayor cuando no se detecta a tiempo (Bestratén M. Orriols, 2010)

Esta tabla 15 muestra los niveles de Detectabilidad; el criterio que será empleado para estos niveles y la valoración que se está considerando bajos los criterios establecidos.

Detectabilidad

DETECTABILIDAD	CRITERIO	VALOR
Muy Alta	Detección obvia	1
Alta	Fácilmente detectable con un control	2
Media	Detectable después de varios controles	3
Mínima	Difícil detección	4
Improbable	No puede detectarse	5

Tabla 15: Clasificación de la facilidad de detección del riesgo

Fuente: (MINSA, 2012)

Frecuencia

Mide la repetitividad potencial u ocurrencia de un determinado fallo, es lo que en términos de fiabilidad o de prevención llamamos la probabilidad de aparición del fallo. (Bestratén M. Orriols, 2010)

Esta tabla 16 muestra los niveles de Frecuencia; el criterio que será empleado para estos niveles y la valoración que se está considerando bajos lo criterios establecidos.

Frecuencia

FRECUENCIA	CRITERIO	VALOR
Muy Baja(Improbable)	Es concebible. No se ha	1

FRECUENCIA	CRITERIO	VALOR
	presentado	
Baja	Es poco probable, aunque se puede dar en el sistema	2
Moderada	Ocasionalmente	3
Alta	Se ha presentado con cierta frecuencia	4
Muy Alta	Frecuentemente	5

Tabla 16: Clasificación de la frecuencia o probabilidad de ocurrencia

Fuente: (MINSA, 2012)

Gravedad

Mide el daño usualmente esperado que provoca el fallo en cuestión, según la percepción del propietario del activo y del equipo del Plan de SGSI, para que no sea subjetivo el análisis. También cabe considerar el daño máximo esperado, el cual iría asociado también a su probabilidad de generación. (Bestratén M. Orriols, 2010)

Esta tabla 17 muestra los niveles de Gravedad; el criterio que será empleado para estos niveles y la valoración que se está considerando bajos lo criterios establecidos.

Gravedad

GRAVEDAD	CRITERIO	VALOR
Muy Baja(Improbable)	Fallo de menor importancia	1
Baja	Repercusiones irrelevantes apenas perceptible	2
Moderada	Repercusiones de relativa importancia	3
Alta	Repercusión elevada, crítica	4
Muy Alta	Muy crítico, serio	5

Tabla 17: Clasificación de Gravedad del riesgo

Fuente: (MINSA, 2012)

Índice de Prioridad de Riesgo (IPR)

El índice de prioridad del AMFE incorpora el factor detectabilidad. Por tanto, tal índice es el producto de la frecuencia por la gravedad y por la detectabilidad, siendo tales factores traducibles a un código numérico adimensional que permite priorizar la urgencia de la intervención, así como el orden de las acciones de control o tratamiento en este caso de seguridad de la información. Por tanto debe ser calculado para todas las causas de fallo. (Bestratén M. Orriols, 2010)

IPR = D.G.F

El IPR es el producto de los tres factores que lo determinan. Suele llamarse Índice de Prioridad del Riesgo. Es calculado para todas las causas de fallo. No obstante un IPR inferior a 100 ó 50 según los límites del Plan SGSI no requeriría intervención salvo que la mejora fuera fácil de introducir y contribuyera a mejorar aspectos de calidad del componente de servicio. Es importante que la organización evalué y establezca en el contexto del Plan de SGSI y los límites del IPR, para decidir en la matriz AMFE cuales riesgos necesitan tratamiento; por que el IPR ofrece una primera aproximación de la importancia del riesgo, lo que ha de facilitar la toma de decisiones para determinar el control o tratamiento del riesgo. (Bestratén M. Orriols, 2010)

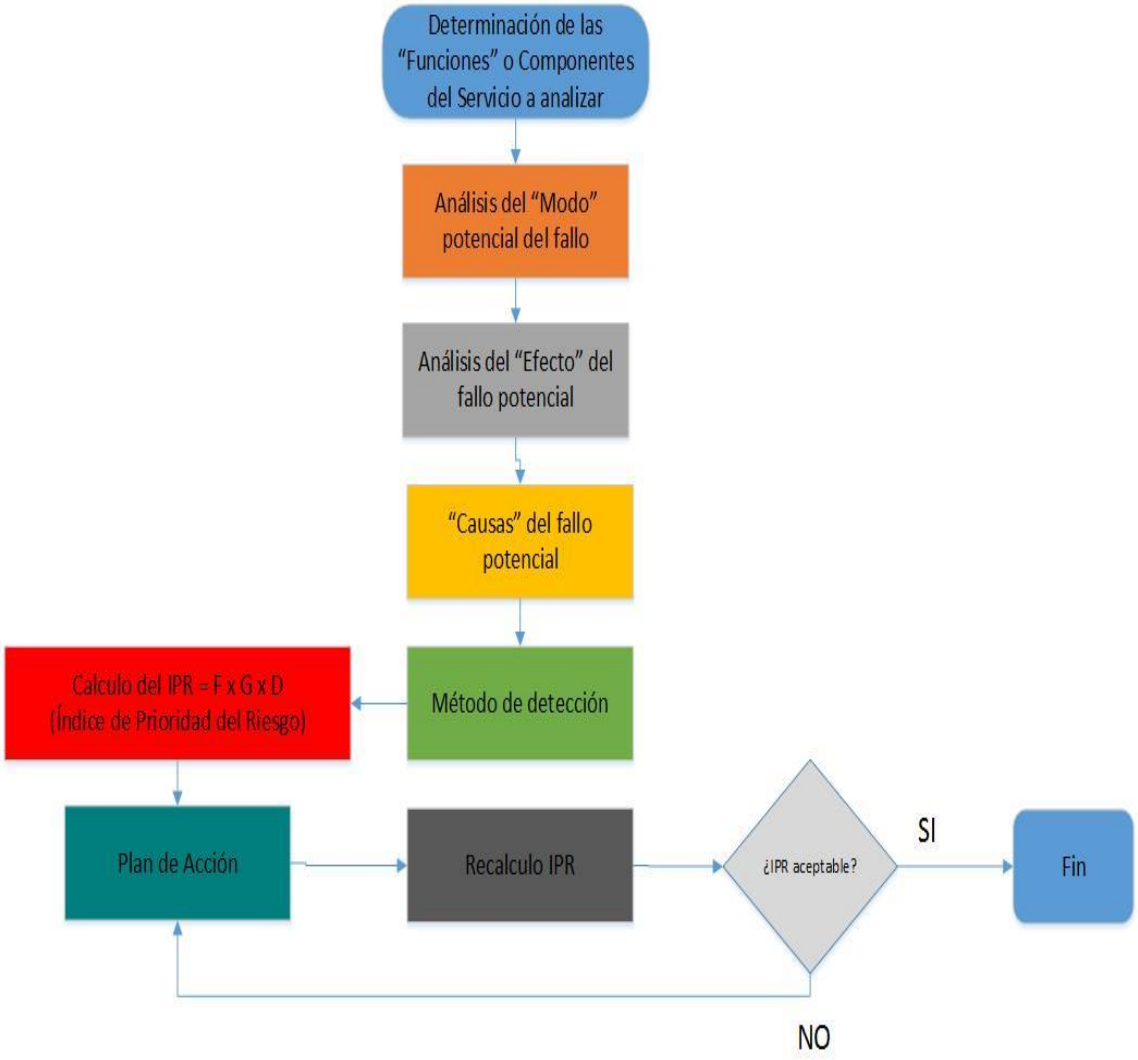

Ilustración 18: Diagrama de Flujo para Elaborar un AMFE

Fuente: (MINSA, 2012)

En la aplicación de la matriz AMFE, el termino fallo o modo de fallo hace referencia al riesgo potencial que es identificado en el componente de servicio o en una actividad específica del mismo; ya que el objetivo es identificar los riesgos en todo el despliegue de los componentes de servicio. El concepto causa a modo de fallo, describe la amenaza, es decir lo que puede causar el daño o pérdida del activo por medio de la explotación de las vulnerabilidades

del activo de información; esta matriz está desarrollada en el apartado 3.1.1.5 del CAPíTULO DE DESARROLLO DEL PROYECTO.

HACER

En esta fase se visualizaran los lineamentos y herramientas que nos permitirán un tratamiento de los riesgos, una mitigación de los riesgos; los controles necesarios para las áreas en estudio; la formación, toma de conciencia y competencias; y los objetivos de control e indicadores que apoyaran al Plan de SGSI.

Entrada:

- Plan Estratégico.

Salida:

- Plan SGSI.

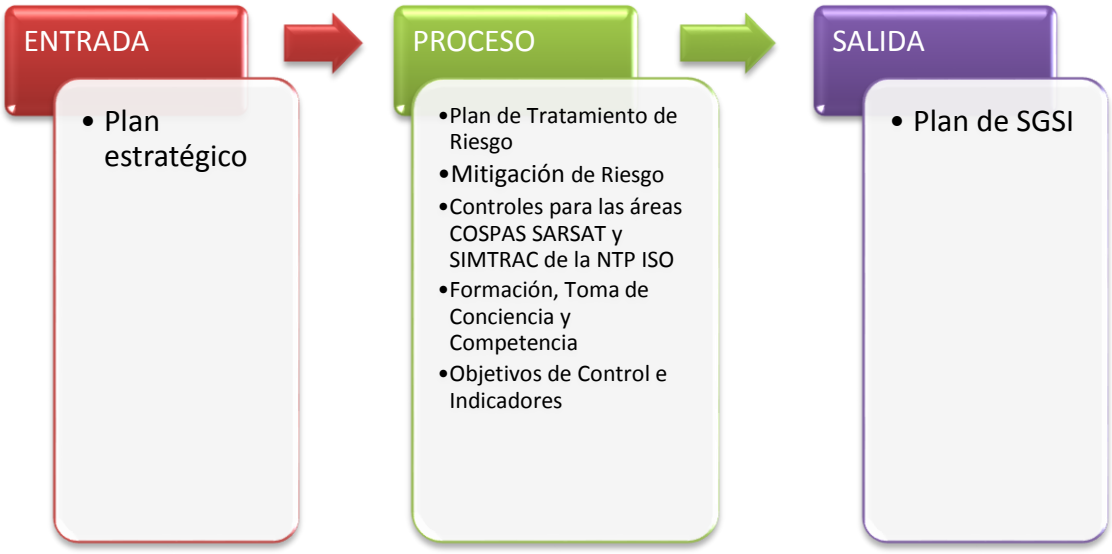

Ilustración 19: Proceso Hacer

FUENTE: Elaborado por los Autores

PLAN DE TRATAMIENTO DEL RIESGO

La gestión de los riesgos es un proceso que implementa medidas técnicas organizativas necesarias para impedir, mitigar o controlar los riesgos analizados e identificados, de forma que las consecuencias que puedan generar sean eliminadas o, si esto no es posible, se puedan reducir lo máximo posible. Un resultado del análisis de riesgos es el criterio para determinar los niveles de riesgo aceptables y en consecuencia, cuáles son los niveles inaceptables y que por lo tanto serán gestionados. El objetivo es mitigar los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización. (Poveda, 2011)

Ilustración 20: Tratamiento del riesgo en el SGSI

(Poveda, 2011)

Una vez se han analizados los riesgos de la organización se realizara al tratamiento de los mismos, que deben recibir los activos y se deben tomar las acciones necesarias. Existen cuatro tipos de tratamiento de riesgos que requieren de diferentes acciones:

§ **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, se debe seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

§ **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han

asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

§ **Transferir el riesgo a un tercero:** Transferir el riesgo a un proveedor o ente especializado con experiencia ha dicho riesgo. Se debe evaluar las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia -no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero-.

§ **Eliminar el riesgo:** Es una opción peligrosa y se debe contar con mucha experiencia para eliminar dicho riesgo. No suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

La organización no debe ignorar sus riesgos, sino daría lugar a un incidente de seguridad. Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo tanto todos los riesgos residuales sean aceptados por la Dirección. (Poveda, J. Gestión y tratamiento de los riesgos. (Poveda, 2011)

MITIGACIÓN DEL RIESGO

Reconocidos los requisitos y los riesgos de seguridad y tomado las decisiones para el tratamiento de los riesgos, se recomienda seleccionar e implementar los controles para lograr la reducción de los riesgos hasta un nivel manejable. Los controles se pueden seleccionar a partir de la

NORMA TÉCNICA PERUANA NTP ISO 27002:2008 - ver Anexo A. - o crear controles nuevos o controles específicos para la organización. La selección de los controles de seguridad dependerá de la organización usando como criterios para la aceptación del riesgo y estas deberían estar sujeta a toda la legislación y los reglamentos institucionales correspondientes.

Un camino para reducir el riesgo:

- Seleccionar los controles apropiados para los riesgos que se han analizado según el Catálogo de Buenas Prácticas de la NORMA TÉCNICA PERUANA NTP ISO/IEC 27002 - 133 controles posibles, pero pueden añadirse otros que en la comandancia se considere necesario.
- Implantar los controles aunque sean controles técnicos necesarios para los procedimientos de instalación, uso y mantenimiento.
- Verificar que los controles estén correctamente implantados.
- Establecer indicadores que midan la implementación de los controles y si reduce el riesgo al nivel de aceptación.

Ilustración 21: Tratamiento del Riesgo en el Plan de SGSI

(Poveda, 2011)

SELECCIÓN DE CONTROLES

Los controles se seleccionarán e implementarán para minimizar en lo posible los riesgos detectados en el análisis de riesgos y que dañen los activos.

Veremos dos grandes grupos de controles:

- Los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos.
- Los organizativos que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

Usaremos controles de ambos tipos, ya que muchas medidas técnicas no pueden impedir que los usuarios de los sistemas cometan errores o dañen intencionadamente los activos y, al contrario, emitir muchas normas internas puede ser inútil si no hay una mínima seguridad técnica implantada.

Se pueden clasificar los controles como controles preventivos y correctivos. Los primeros son los que sirven para evitar incidentes de seguridad no deseados mientras que los segundos son aquellos que se pondrán en marcha ante la ocurrencia de fallos o incidentes de seguridad.

Se debe considerar los diferentes factores y restricciones en el momento de la selección de controles como costo de la implementación, mantenimiento del control, la disponibilidad, capacitación que se debe brindar a los colaboradores para desempeñar el control y su aplicabilidad por los riesgos que se han detectado.

No todos los controles se usaran, sin embargo hay algunos que son requisito de la norma NTP ISO-IEC 27001 tales como la Política de Seguridad o las Auditorías Internas.

IMPLEMENTACIÓN DE CONTROLES

Con los controles pertinentes, se definirá los procedimientos para su implantación. Los controles de tipo organizativo se prestan más a ser implantados mediante procedimientos; los de corte tecnológico pueden ser susceptibles de necesitar documentación. Debe analizarse la lista de controles seleccionados y establecer qué procedimientos necesitan ser desarrollados. Si la organización cuenta con procesos pequeños quizás varios controles puedan estar en un mismo procedimiento. No se recomienda, desarrollar un procedimiento para cada control. Una forma de gestionar de mejor manera los controles es documentarlos plenamente. También los procedimientos deben ser breves y concisos. No deben incluir demasiadas instrucciones ni particularidades de la tarea a realizar. Lo importante de este objetivo es que el procedimiento cualquiera pueda ejecutarla con un mínimo de rigor aun sin contar con formación o experiencia previa.

VERIFICACIÓN DE CONTROLES

Una vez puesto en marcha, debe verificar periódicamente que los controles implantados funcionan como se esperaba. Si no es así, deberán tomarse las acciones necesarias para corregir esa situación. Una herramienta fundamental del Plan SGSI es la verificación sobre la eficacia de los controles implantados. Para ello se debe establecer objetivos de rendimiento para los controles, marcar puntos de control y medición y registrar los

resultados de manera que se sepa si el control realmente cumple con la protección de los activos hasta el punto que la organización necesita.

DOCUMENTACIÓN DEL PLAN DE TRATAMENTO DE RIESGOS

La documentación de la gestión de riesgos se realiza mediante la Declaración de Aplicabilidad conocida también por sus siglas en inglés SOA -Statement Of Applicability-. Este documento, requerido por la Norma NTP/ISO-IEC 27001, es un resumen de las decisiones que se han tomado para tratar los riesgos analizados y debe hacer un match entre los controles del Anexo A de la Norma, con los deficiencias encontradas de la organización. Para cada uno de los controles identificados se debe reflejarse en este documento:

- Si está implantado actualmente en la organización, con una breve descripción de cómo se aplica.
- Si se va a implantar, es decir, si es uno de los controles escogidos para mitigar el riesgo, junto con las razones para haberlo seleccionado.
- Si no se va a implantar, entonces hay que exponer los motivos que han llevado a esta decisión. Las exclusiones deben justificarse adecuadamente.

Este documento constituye de alguna manera un registro de los resultados finales del Plan SGSI, ya que concreta de manera clara y directa en qué va a consistir el sistema de seguridad, detallando cada uno de los controles que se tiene la intención de aplicar de manera explícita.

Sólo insistir en que no es necesario seleccionar todos los objetivos ni todos los controles asociados a cada uno de los objetivos. Deben escogerse los objetivos y controles apropiados a las circunstancias, es decir, aquellos que se

considera que cubren los requisitos de seguridad de la organización y son viables.

CONTROLES PARA LAS ÁREAS DEL SIMTRAC Y COSAS – SARSAT ESTABLECIDOS EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008

Un punto de partida de la seguridad de la información es considerar las recomendaciones de las NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 en las mejores prácticas habituales para conseguir dicha seguridad; esto se visualiza en el anexo 2.

Relacionaremos las principales medidas de seguridad directamente con las áreas del SIMTRAC y del COSAS - SARSAT, los controles y su implementación, tomando como base la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 (Anexo 2.).

FORMACIÓN, TOMA DE CONCIENCIA Y COMPETENCIA

Como siguiente pasó en la fase de HACER; la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 establece que toda organización debe asegurar que su personal que tenga responsabilidades con el Plan SGSI debe ser competente para cumplir sus tareas asignadas. Para garantizar sus competencias la organización debe determinar las competencias necesarias de los colaboradores, realizar capacitaciones o contratar personal tercera con el fin de desarrollar formaciones, habilidades, experiencia y calificaciones. La organización debe asegurar que todos los colaboradores tomen conciencia de la pertinencia e importancia de sus actividades de seguridad de la información y su influencia en el cumplimiento de los objetivos del Plan SGSI - Anexo A.

OBJETIVOS DE CONTROL E INDICADORES

La Norma estipula que se deben incluir los objetivos de control y se debe establecer los indicadores de rendimiento para medir el cumplimiento de los objetivos.

Para proceder a construir el indicador se establecen las variables que lo conforman y la relación entre ellas para que se genere la información necesaria.

VERIFICAR

En esta fase una vez que está en marcha el Plan de SGSI es fundamental hacer un seguimiento de cómo funciona y cómo va evolucionando. En primera instancia revisar el Plan SGSI; medir la Eficiencia de los Controles establecidos y revisar los Riesgos Residuales para corregir las posibles desviaciones sobre lo planificado detectando oportunidades, lo cual tenemos que aprovecharlo.

Entrada:

- Plan SGSI.

Salida:

- Correcciones y mejoras del Plan de SGSI.

Ilustración 22: Proceso Verificar

FUENTE: Elaborado por los Autores

REVISIÓN DEL PLAN SGSI

Uno de los requisitos más importantes de la Norma NTP-ISO/IEC 27001:2008 es la revisión que la organización debe realizar con una cierta periodicidad, como mínimo anual, al Plan del Sistema de Gestión de Seguridad de la Información. Esta revisión tiene como objetivo asegurar que el Plan SGSI es en todo momento adecuado, apropiado y efectivo para los propósitos y contexto de la organización. Esta revisión nos ayuda a detectar los puntos débiles y discutir sobre cómo mejorarlos.

Entradas del Proceso

Existen diversas fuentes de cómo obtener datos e información útil para la Revisión del Plan de SGSI:

Toda tipo de auditoria, la auditoria interna y externas como la del cliente. Éstas aportan información sobre los puntos fuertes y débiles del Plan de SGSI y ofrece oportunidades de mejora.

La última versión o revisión anterior del Plan de SGSI es el punto de partida de dónde estaba el Plan de SGSI con respecto al presente. Esto proporciona información muy valiosa sobre qué se puede hacer para continuar mejorando y progresando.

Tener reuniones de los interesados a menudo, clientes, usuarios, proveedores, público, esto puede aportar algún comentario útil que serviría analizar y tomar alguna acción de mejora.

Las vulnerabilidades o amenazas que no se han tratado adecuadamente en análisis de riesgos anteriores. Es decir, si se han detectado nuevas amenazas o ha habido cambios que necesiten revisar o bien valorar si los riesgos que no se trataron por cualquier motivo antes, ahora necesitan tratamiento.

Hay que evaluar los objetivos. Uno de los principales objetivos de este punto es revisar si se han cumplidos los objetivos propuestos en un principio.

Salidas del Proceso

Mejora de eficiencia del Plan de SGSI, es decir, nos indica que hay que mejorar: si se va a implementar más controles, se va a mejorar los ya implementados, existen nuevos riesgos, etc.

Actualización de la evaluación de riesgos. Se tendrá que documentar los cambios.

Modificación de procedimientos y controles, esto quiere decir, mejorarlos o eliminarlo si es que ya no es útil en el Plan de SGSI.

MEDIR EFICIENCIA DE LOS CONTROLES

Para medir la eficiencia de los controles, es decir, si realmente está funcionando correctamente, para medir ello se debe de

implementar herramientas como cartas de control, planes de verificación del Plan de SGSI, balanced scorecard o cuadro de mando integral entre otros, que faciliten realizar el seguimiento del Plan de SGSI y determinar su cumplimiento de acuerdo a la NTP-ISO/IEC 27001:2008. -Ver Anexo C-

REVISAR RIESGOS RESIDUALES

A partir de la matriz ANÁLISIS MODAL DE FALLOS Y EFECTOS - AMFE - que se desarrollará en el apartado 3.1.3.3 del CAPÍTULO DE DESARROLLO DEL PROYECTO, se definirá la prioridad de los riesgos de acuerdo al IPR calculado en el análisis de la gravedad, frecuencia y detectabilidad de los riesgos presentes o potenciales en cada activo de información.

Estos son los riesgos que permanecen después de la planificación de la respuesta a los riesgos. Los riesgos residuales han sido aceptados para que se puedan crear los planes de contingencia y los planes alternativos. Deben ser documentados apropiadamente y revisados a lo largo del proyecto para ver si su clasificación ha cambiado.

En esta fase se tiene que tener en cuenta:

1. Identificar no conformidades del Plan de SGSI.
2. Realizar análisis de causa raíz.
3. Definir acciones correctivas y preventivas.
4. Identificar las mejoras potenciales del Plan de SGSI que se hayan propuesto en la fase anterior y ponerlas en marcha.
5. De ser necesario, obtener el visto bueno de la Dirección para la implementación de los cambios propuestos y aprobación de recursos necesarios.
6. Divulgar o comunicar las acciones y mejoras a todos los interesados.

7. Evaluar la efectividad del plan de mejora continua tomando como base los resultados obtenidos de las acciones implementadas y realizar planes de acción concretos para mejorar el Plan de SGSI.

ACTUAR

En esta fase se realizaran las acciones preventivas y acciones correctivas para la actualización del Plan de SGSI.

Entrada:

- Correcciones y mejoras del Plan de SGSI.

Salida:

- Aplicación de las nuevas mejoras.
- Retroalimentación.

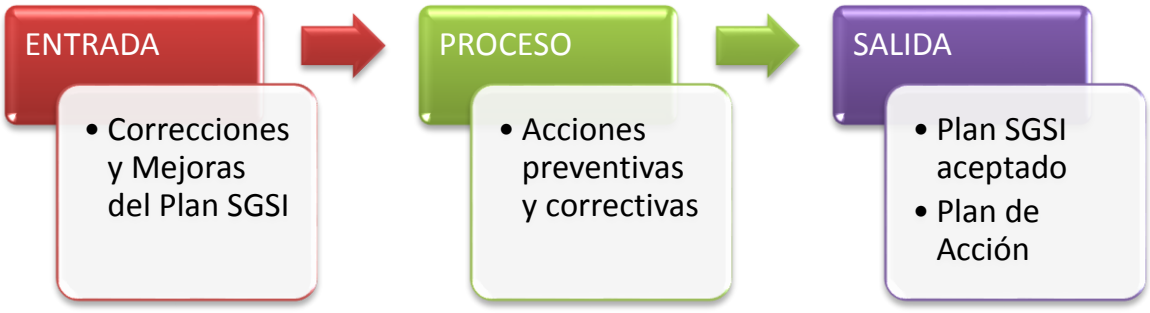

Ilustración 23: Proceso Actuar

FUENTE: Elaborado por los Autores

Es en esta fase es cuando deberemos analizar para luego implantar las medidas preventivas y correctivas consecuencia de las revisiones efectuadas, y mejorar así el rendimiento del Plan de SGSI. Las medidas correctivas comprenderán la selección de nuevos controles, la modificación de los existentes o la eliminación de los obsoletos.

Entradas del Proceso

1. Informes de no conformidades.
2. Informes de conclusiones y sugerencias después de implementar la revisión.
3. Propuestas de mejoras de otras áreas y unidades de negocios.

Salida del Proceso

Un Informe con el plan de mejoras, describiendo las conclusiones más relevantes surgidas de la etapa de revisión y especificando objetivos concretos, el impacto de los cambios y quienes estarían involucrados así como un plan tentativo para llevarlos a cabo.

Existen diversas herramientas que nos sirven a ayudar a establecer planes de acción efectivos al momento de resolver un problema dentro de una organización - Ver Anexo D -, se muestran algunas herramientas fáciles de aplicar en el sector de la Comandancia de Operaciones de Guardacostas.

ACCIONES PREVENTIVAS Y CORRECTIVAS

Cuando se producen no conformidades, es decir, cuando hay un incumplimiento de un requisito, se deben toman acciones encaminadas a resolver esa situación no deseada. Las acciones contempladas por la Norma NTP-ISO/IEC 27001:2008 se dividen en:

Acciones correctivas.

Acciones preventivas.

En el Anexo D, se muestran algunas herramientas fáciles de aplicar en el sector de la organización.

CAPÍTULO III: DESARROLLO DEL PROYECTO

3.1 PLANEAMIENTO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN USANDO LA NORMA TÉCNICA PERUANA -ISO/IEC 27001:2008

En este capítulo se desarrollara la metodología propuesta en sus tres etapas: Las entrada son la información requerida; para luego ser procesada bajo el ciclo PDCA y concluir en la salida obteniendo el Plan de SGSI.

ENTRADAS

Consolidado del Talento Humano

Esta entrada es un censo del Talento Humano que es dividida en 3 – tres – partes: Personal Oficial, Personal Subalterno y Personal de Marinería.

El Consolidado nos mostrara el total de personal y los principales campos característicos de las personas que laboran en la Comandancia de Operaciones Guardacostas en las áreas del SIMTRAC y del COSPAS SARSAT; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología para luego poder procesarla.

Personal Oficial

Las Entradas son requerimientos indispensables para el proceso a realizar como base para la metodología propuesta.

Esta tabla 18 – diez y ocho - nos mostrara el censo del personal Oficial que laboran en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología y luego poder procesarla.

Personal Oficial

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
11	Oficial	Guardacostas	Apellidos y nombres del personal Oficial	Número del Código de identidad	SIMTRAC / COSPAS SARSAT	Cargo que ejerce en el área de destaque

Tabla 18: Consolidado Personal Oficiales

Fuente: Elaborado por los Autores

Personal Subalterno

Las Entradas son requerimientos indispensables para el proceso a realizar como base para la metodología propuesta.

Esta tabla 19 – diez y nueve - nos mostrara el censo del personal Subalterno que laboran en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología y luego poder procesarla.

Personal Subalterno

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
78	Subalterno	Guardacostas	Apellidos y nombres del personal Subalterno	Número del Código de identidad	SIMTRAC / COSPAS SARSAT	Cargo que ejerce en el área de destaque

Tabla 19: Consolidado Personal Subalterno

Fuente: Elaborado por los Autores

Personal Marinería

Las Entradas son requerimientos indispensables para el proceso a realizar como base para la metodología propuesta.

Esta tabla 20 – veinte - nos mostrara el censo del personal de Marinería que laboran en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología y luego poder procesarla.

Personal de Marinería

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
6	Marinería	Guardacostas	Apellidos y nombres del personal de marinería	Número del Código de identidad	SIMTRAC / COSPAS SARSAT	Cargo que ejerce en el área de destaque

Tabla 20: Consolidado Personal Marinería

Fuente: Elaborado por los Autores

Los totales del personal de la Comandancia de Operaciones de Guardacostas se detallarán en el Anexo B

Consolidado de los Recursos Tecnológicos

Esta entrada de los Recursos Tecnológicos se dividida en 3 – tres – partes: Servidores SIMTRAC y COSPAS SARSAT; Estaciones de Trabajo SIMTRAC y COSPAS SARSAT y Equipos de Comunicación SIMTRAC y COSPAS SARSAT.

Servidores SIMTRAC y COSPAS SARSAT

El Consolidado nos mostrara el total de Equipos Servidores y los principales campos característicos de estos equipos que permiten las labores en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología para luego poder procesarla.

Servidores de las áreas del SIMTRAC y del COSPAS - SARSAT

Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
12	HP / Compatible	Velocidad del procesamiento	Especio de almacenamiento	Memoria física del recurso tecnológico	Sistema operativo del recurso tecnológico	Servicio que brinda el recurso tecnológico	Sistema o aplicación que se encuentra en el recurso tecnológico	Fecha de ingreso a la comandancia	Estado en que se encuentra el recurso tecnológico

Tabla 21: Consolidado Servidores SIMTRAC COSPAS-SARSAT

Fuente: Elaborado por los Autores

Estaciones de Trabajo SIMTRAC y COSPAS SARSAT

El Consolidado nos mostrara el total de Equipos de Estaciones de Trabajo y los principales campos característicos de estos equipos que permiten las labores en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología para luego poder procesarla.

Estaciones de trabajo de las áreas del SIMTRAC y del COSPAS - SARSAT

Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
16	HP / Compatible	Velocidad del procesamiento	Especio de almacenamiento	Memoria física del recurso tecnológico	Sistema operativo del recurso tecnológico	Servicio que brinda el recurso tecnológico	Sistema o aplicación que se encuentra en el recurso tecnológico	Fecha de ingreso a la comandancia	Estado en que se encuentra el recurso tecnológico

Tabla 22: Consolidado Estaciones de Trabajo SIMTRAC COSPAS-SARSAT

Fuente: Elaborado por los Autores

Equipos de Comunicación SIMTRAC y COSPAS SARSAT

El Consolidado nos mostrara el total de Equipos de Comunicaciones y los principales campos característicos de estos equipos que permiten las labores en la Comandancia de Operaciones Guardacostas; necesarios para el conocimiento de los requerimientos como entradas para nuestra metodología para luego poder procesarla.

Equipos de Comunicación de las áreas del SIMTRAC y del COSPAS SARSAT

Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
10	Varios	Velocidad del procesamiento	Especio de almacenamiento	Memoria física del recurso tecnológico	Sistema operativo del recurso tecnológico	Servicio que brinda el recurso tecnológico	Sistema o aplicación que se encuentra en el recurso tecnológico	Fecha de ingreso a la comandancia	Estado en que se encuentra el recurso tecnológico

Tabla 23: Consolidado Equipos de Comunicación SIMTRAC COSPAS-SARSAT

Fuente: Elaborado por los Autores

NOTA: Los totales de los recursos tecnológicos de la Comandancia de Operaciones de Guardacostas se detallarán en el Anexo B.

Consolidado de los Sistemas de Información

Las Entradas como requerimientos indispensables para el proceso a realizar como base para la metodología propuesta.

Software principal SIMTRAC y COSPAS SARSAT

Esta entrada de los Sistemas de Información es correspondiente a la cantidad de los principales sistemas o aplicaciones que se encuentran en Comandancia de Operaciones Guardacostas en las áreas del SIMTRAC y del COSPAS SARSAT.

Software principal de las áreas del SIMTRAC y del COSPAS SARSAT

Núm.	Tipo de sistema	Nombre	Proveedor	Versión	Responsable	Fecha Ingreso	Estado
15	Aplicativos / base de datos / web	Nombre del sistema de información	Proveedor del sistema de información de quien fue adquirido	Versión del sistema de información	Persona responsable del sistema de información	Fecha de adquisición del sistema de información	Estado en que se encuentra el sistema de información

Tabla 24: Consolidado Software Principal SIMTRAC COSPAS-SARSAT

Fuente: Elaborado por los Autores

NOTA: Los totales de los Sistemas de Información de la Comandancia de Operaciones de Guardacostas se detallarán en el Anexo B

PROCESOS

El Plan de SGSI se analizó en los puntos página 81; este Plan se desarrollará en base a la metodología vista en los puntos:

Fases del PDCA

Capítulo 3 – Página 124	Fases PDCA
Página 131	Planear
Página 148	Hacer
Página 179	Verificar
Página 187	Actuar

Tabla 25: Fase PDCA del Plan de SGSI

Fuente: Elaborado por los Autores

SALIDAS

El Plan de SGSI será la salida del proceso y se desarrollará en base a la metodología vista en los puntos:

Plan del Sistema de Gestión de Seguridad de la Información

Capítulo 3 – Artículo 3.1.2	HACER
Página 152	Controles para las áreas del SIMTRAC y COSAS – SARSAT establecidos en la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008

Tabla 26: Fase HACER del Plan de SGSI

Fuente: Elaborado por los Autores

PLANEAR

En la fase de Planear del desarrollo se realizara el alcance del Plan del SGSI, las políticas; también se implementan las herramientas para la identificación del riesgo, del impacto y se identificaran los riesgos, según el tipo de activo de información que se afectaría.

ALCANCE DEL PLAN SGSI

El alcance del Plan del SGSI abarcará:

Dentro de la Dirección General de Capitanías y Guardacostas – DICAPI – existe organizacionalmente la Comandancia de Operaciones

Guardacostas – COMOPERGUARD – donde se encuentra el Centro de Control de Misiones Guardacostas con sus departamentos de Información y Seguridad Acuática; e Información y Protección Acuática en estas se encuentran las divisiones de Información COSPAS SARSAT y Trafico Acuático SIMTRAC – Sistema de Información y Monitoreo de Trafico Acuático - respectivamente en donde se centrara esta tesis por ser las divisiones más vulnerables y de mayor riesgo en sus activos de información.

POLÍTICAS DEL PLAN SGSI

Se cumplirán con los objetivos mencionados en el apartado página xvi.

Objetivos Organizacionales:

- Salva guardar la vida humana en el mar.
- Evitar la depredación de la vio masa en el mar.
- Cuidar el medio ambiente.

Políticas del SGSI:

- Determinar un Alcance para el Plan de SGSI.
- Referirse a las NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008.
- Especificar Términos y Definiciones. Ver apartado 8.3.
- Administrar el Plan de SGSI.
- Responsabilizar a la Gerencia.
- Realizar Auditorías Internas del SGSI.
- Realizar Revisiones por Parte de la Gerencia del SGSI.
- Realizar las Mejoras Necesarias al SGSI.

- Mantener los Antecedentes.

  Se cumplirán con los objetivos de control mencionados en el anexo A.

Objetivos Específicos de Control:

A.5.1. Política de seguridad de la información

A.6.1 Organización interna

A.6.2 Seguridad del acceso a terceras partes

A.7.1 Responsabilidad por los activos

A.7.2 Clasificación de la información

A.8.1. Previo al empleo

A.8.2. Durante el empleo

A.8.3. Finalización o cambio de empleo

A.9.1. Áreas seguras

A.9.2. Seguridad de los equipos

A.10.1. Procedimientos y responsabilidades de operación

A.10.2. Gestión de entrega de servicios externos

A.10.3. Planificación y aceptación del sistema

A.10.4. Protección contra software malicioso

A.10.5. Gestión interna de respaldo y recuperación

A.10.6 Gestión de seguridad de redes

A.10.7. Utilización y seguridad de los medios de información

A.10.8. Intercambio de información

A.10.9. Servicios de comercio electrónico

A.10.10. Monitoreo

A.11.1. Requisitos de negocio para el control de accesos

A.11.2 Gestión de acceso de usuarios

A.11.3. Responsabilidades de los usuarios

A.11.4. Control de acceso a la red

A.11.5. Control de acceso al sistema operativo

A.11.6. Control de acceso a las aplicaciones e información

A.11.7. Informática móvil y teletrabajo

A.12.1. Requisitos de seguridad de los sistemas de información

A.12.2. Proceso correcto en aplicaciones

A.12.3. Controles criptográficos

A.12.4. Seguridad de los archivos del sistema

A.12.5. Seguridad en los procesos de desarrollo y soporte

A.12.6. Gestión de vulnerabilidades técnicas

A.13.1. Reportando eventos y debilidades en la seguridad de información

A.13.2. Gestión de los incidentes y mejoras en la seguridad de información

A.14.1. Aspectos de la gestión de continuidad del negocio en la seguridad de información

A.15.1. Cumplimiento de los requisitos legales

A.15.2. Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico

A.15.3. Consideraciones sobre la auditoría de sistemas

El tratamiento de los objetivos de control de la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 se vio detenidamente en el punto página 136 donde se determinaran las clausulas, objeticos de control y controles a utilizar para este trabajo.

IDENTIFICACIÓN DEL RIESGO

Realizado el inventario de activos de información relacionando cada proceso de la organización contemplado en el alcance del Plan SGSI –Ver Anexo B-.

En la tabla 27 – veinte y siete- grafica los riesgos contrastados con las clausulas, objetivos de control y controles de la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 numéricamente; permitiendo conocer cuáles de estas cláusulas, objetivos de control y controles apoyaran a minimizar los riesgos encontrados.

Riesgos Determinados

NÚM.	RIESGOS	NTP ISO/IEC 27001: 2008
1	NO HAY SEGURIDAD PARA LOS ACTIVOS	7.1.1; 7.1.2; 10.3.1
2	NO HAY ACUERDO DE CONFIDENCIALIDAD INTERNA	6.1.5
3	NO HAY UN RESPONSABLE DE LAS ÁREAS VULNERABLES	6.1.3; 6.1.5
4	NO EXISTEN DOCUMENTOS DE SEGURIDAD	6.1.3; 6.1.5
5	NO EXISTE UN PLAN DE CONTINUIDAD DE NEGOCIO	14.1.2
6	NO HAY SEGURIDAD EN LA RED	9.1.1; 10.6.1; 10.8.4
7	NO SE TOMAN EN CUENTA LAS POLÍTICAS DE ACCESO A LAS ÁREAS VULNERABLES	5.1.1; 11.1.1; 11.2.1
8	NO HAY UN CONTROL DE USUARIOS	5.1.1; 11.1.1; 11.2.1
9	FUGA DE INFORMACIÓN	12.5.4
10	NO ESTAN DELIMITADOS LOS ROLES DEL PERSONAL	5.1.1; 8.1.1
11	NO EXISTEN POLÍTICAS DE SEGURIDAD	5.1.1; 8.1.1

Tabla 27: Riesgo VS NTP ISO/IEC 27001: 2008

FUENTE: Elaborado por los Autores

En la tabla 28 – veinte y ocho - de Inventarios de Activos de Información se le ha adicionado el campo de los Riesgos para luego conocer el impacto que causa en ellos.

Inventario de Activos de Información

INVENTARIO DE ACTIVOS DE INFORMACIÓN								
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
Componentes del Servicio	Personal Destacado al Área	1; 2; 3; 8; 9; 10	Usuario	Jefe del Área	Pool de Operaciones			
	Instalaciones físicas	1; 3; 5; 6; 11	Organización	Jefe de la Comandancia	Coordenadas de la Organización			
	Sistemas Operativos	1; 5; 7; 8; 9; 11	Software	PDA	Oficinas			
	Estaciones de Trabajo	1; 3; 5; 6; 7; 9; 10; 11	Hardware	PDA	Oficinas y Pool de Operaciones			
	Servidores	1; 3; 5; 6; 7; 8; 11	Hardware	Administrador de Servidores	Salas de Servidores			
	Sistemas de Información Servidores	1; 2; 5; 6; 7; 8; 9; 11	Software	Administrador de Servidores	Salas de Servidores			

INVENTARIO DE ACTIVOS DE INFORMACIÓN								
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
	Imagen Organizacional	2; 4; 5; 9;	Organización	Relaciones Publicas	Área de Relaciones Publicas			
	Información de Embarcaciones	2; 4; 5; 9;	Información	Técnico a Cargo	Base de Datos			
	Informe de Operaciones	2; 4; 5; 9;	Información	Oficial a Cargo	Estación de Trabajo			
	Equipos de Comunicación	1; 3; 5; 6; 7; 9; 10; 11	Hardware y Red	Jefe de Electrónica	Área de Electrónica			

Tabla 28: Inventario De Activos De Información Vs Riesgos

FUENTE: Elaborado por los Autores

Leyenda de Confidencialidad, Integridad y Disponibilidad

C:	Confidencialidad
I:	Integridad
D:	Disponibilidad

Tabla 29: Leyenda Inventario de Activos de Información

FUENTE: Elaborado por los Autores

IDENTIFICACIÓN DEL IMPACTO

Al ser afectado un determinado activo de información, al alterar uno de sus componentes, el impacto de ese activo de información será mayor.

Estableciendo el comportamiento del activo de información, en el momento de decidir cuál de los 3 niveles aplica para cada categoría, de acuerdo al grupo interdisciplinario dentro de la discusión, se cuantifica de acuerdo a las opiniones brindadas, esto debe hacerse tomando activo por activo, evaluando los 3 requisitos mencionados en el punto página 119 antes de continuar con el siguiente.

Considerando las condiciones normales de operación, en las cuales se realiza básicamente consultas a los diferentes activos de información, el ingreso del personal a las áreas con un usuario y contraseña única, con acceso a la web por medio de navegadores con niveles bajos de seguridad; toda la información está en las aplicaciones y las base de datos estando con disponibilidad para los oficiales, esto es alimentado con la información llegada por los proveedores de servicios.

El desarrollo de la identificación del impacto se encuentra en la Tabla 30- treinta - Inventario de Activos de Información vs Riesgos e Impactos se muestra dicho inventario asociado a los diferentes riesgos con las priorizaciones de confidencialidad, integridad y disponibilidad.

Inventario de Activos de Información

INVENTARIO DE ACTIVOS DE INFORMACIÓN								
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
Componentes del Servicio	Personal Destacado al Área	1; 2; 3; 8; 9; 10	Usuario	Jefe del Área	Pool de Operaciones	Alta	Alta	Alta
	Instalaciones físicas	1; 3; 5; 6; 11	Organización	Jefe de la Comandancia	Coordenadas de la Organización	Alta	Alta	Alta
	Sistemas Operativos	1; 5; 7; 8; 9; 11	Software	PDA	Oficinas	Alta	Alta	Alta
	Estaciones de Trabajo	1; 3; 5; 6; 7; 9; 10; 11	Hardware	PDA	Oficinas y Pool de Operaciones	Alta	Media	Alta
	Servidores	1; 3; 5; 6; 7; 8; 11	Hardware	Administrador de Servidores	Salas de Servidores	Alta	Alta	Alta
	Sistemas de Información Servidores	1; 2; 5; 6; 7; 8; 9; 11	Software	Administrador de Servidores	Salas de Servidores	Alta	Alta	Alta
	Imagen Organizacional	2; 4; 5; 9;	Organización	Relaciones Publicas	Área de Relaciones Publicas	Alta	Alta	Media
	Información de Embarcaciones	2; 4; 5; 9;	Información	Técnico a Cargo	Base de Datos	Alta	Alta	Alta

INVENTARIO DE ACTIVOS DE INFORMACIÓN									
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
	Informe de Operaciones	2; 4; 5; 9;	Información	Oficial a Cargo	Estación de Trabajo	Alta	Alta	Alta
	Equipos de Comunicación	1; 3; 5; 6; 7; 9; 10; 11	Hardware y Red	Jefe de Electrónica	Área de Electrónica	Alta	Alta	Alta

Tabla 30: Inventario de Activos de Información vs Riesgos e Impactos

Fuente: (MINSA, 2012)

Leyenda de Confidencialidad, Integridad y Disponibilidad

C:	Confidencialidad
I:	Integridad
D:	Disponibilidad

Tabla 31: Leyenda Inventario de Activos de Información

Fuente: Elaborado por los Autores

ANÁLISIS Y EVALUACIÓN DEL RIESGO

Al estimar el riesgo usando la matriz de Análisis Modal de Fallos y Efectos AMFE; nos brindara un valor cuantitativo como resultado que no permita identificar el fallo potenciales, y elaborar planes de acción para combatir los riesgos, y facilitar acciones en prevención de riesgos - Bestratén, M. Orriols, R. Y Mata, C. Análisis modal de fallos y efectos AMFE. Instituto Nacional de Seguridad e Higiene en el trabajo. Notas Técnicas de Prevención. 679. P 1 – 8 - .

Los conceptos detallados para el uso de esta matriz se encuentran en el punto página 124.

En el caso de esta tesis, el análisis de riesgos se realiza por componente de servicio definiendo cada una de las actividades y luego los activos de información de cada actividad, como se observa en la matriz AMFE de la tabla 32 – treinta y dos - para el componente de servicio de elaboración de informes de resultados, en la cual se analiza cuáles son los riesgos, los efectos y las amenazas; sus niveles de Frecuencia, Gravedad y Detectabilidad con un nivel de Índice de Prioridad del Riesgo.

Matriz AMFE (Análisis Modal de sus Fallas y sus Efectos)

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)								
Activos de Información	**Código de Numeración**	**Modo de Fallo**	**Efecto**	**Causa**	**Frecuencia F**	**Gravedad G**	**Detectabilidad D**	**IPR**
Personal Destacado al Área	1.1	Falta de Recurso Humano	Área sin Personal	Retrasos en las búsquedas	2	3	3	18
	1.2	Falta de compromiso para el llenado de las bitácoras	Bitácora bacías	Desinformación para los superiores	3	4	1	12
	1.3	Falta de Capacitación Recurso Humano	Desinterés en el área	Mal manejo de los sistemas	4	3	2	24
	1.4	Divulgación de la Información Confidencial	Perdida de Confidencialidad	Descontento y falta de confianza del personal destacado	2	5	3	30
Instalaciones Físicas	2.1	Inadecuada Infraestructura de red	No escalable	No crecimiento de las áreas	5	5	2	50
	2.2	Inadecuada Infraestructura para Sala de Servidores	Difícil acceso	Deterioro de los servidores	5	5	1	25
Sistemas Operativos	3.1	SO sin Licencia	Detención del SO	No poder usar los sistemas	4	4	2	32
	3.2	Versiones pasadas de los SO	Poco soporte del fabricante	No funcionen las aplicaciones actuales	3	3	2	18

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)								
Activos de Información	**Código de Numeración**	**Modo de Fallo**	**Efecto**	**Causa**	**Frecuencia F**	**Gravedad G**	**Detectabilidad D**	**IPR**
	3.3	Perdida de la Información por falla de Servidor	Desinformación en las consultas	Mal manejo de las operaciones	5	5	2	50
	3.4	Sin Soporte para SO Libre	Desentendimiento de los SO libres	Sin solución a los posibles problemas	5	5	1	25
Estaciones de Trabajo	4.1	Estaciones de Trabajo Obsoletas	Incomodidad al trabajar	Respuesta inadecuadas a las consultas	3	4	1	12
	4.2	Estaciones de Trabajo sin homogeneidad	Tiempos de respuestas	Respuestas tardías en las operaciones	4	4	2	32
	4.3	Estaciones de trabajo sin mantenimiento regular	Menor rendimiento de la estación de trabajo	Deterioro de las estaciones de trabajo	3	3	2	18
Servidores	5.1	Lentitud en la Capacidad de Procesamiento	Aplicaciones detenidas	Procesador antiguo	5	5	2	50
	5.2	Poco Espacio de Almacenamiento	Consultas sin respuestas	Perdida de Información	5	5	2	50
	5.3	No se cuenta con un Mantenimiento de servidores	Aplicaciones y BD sin acceso	Mal funcionamiento de los servidores	4	4	2	32
Sistemas de Información Servidores	6.1	Versiones pasadas de los SO	Vulnerabilidad	Infiltración de virus, spam, otros	3	4	1	12

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)								
Activos de Información	**Código de Numeración**	**Modo de Fallo**	**Efecto**	**Causa**	**Frecuencia F**	**Gravedad G**	**Detectabilidad D**	**IPR**
	6.2	Sin Soporte para Sistema Servidor de Correo Libre	Desconocimiento de soluciones a los problemas de los servidores	Demoras en la solución de problemas	5	5	2	50
	6.3	Sin Soporte para Sistema Servidor de la Pagina Web Libre	Desconocimiento de soluciones a los problemas de los servidores	Demoras en la solución de problemas	5	5	3	75
	6.4	Falla en las Transacciones con la Base de Datos	Poco uso de las aplicaciones	Demora en las consultas a la Base de Datos / congelamiento de la aplicación	5	5	3	75
Imagen Organizacional	7.1	Pérdida de Status a nivel Organizacional	Mala imagen de la institución	Uso indebido de la imagen institucional; suplantación, fraude, otros	4	3	4	48
Información de Embarcaciones	8.1	Información Tardía de las Embarcaciones	Actuar con información pasada	Mal manejo de las operaciones guardacostas	4	4	4	64
	8.2	Datos Erróneos del Monitoreo de las Embarcaciones	Incertidumbre en las consultas	Mal manejo de los recursos guardacostas	3	5	4	60
Informe de Operaciones	9.1	Carencia de Automatización de las Bitácoras	Demora en la redacción de las bitácoras	Presentación tardía de los incidentes a los superiores	5	5	1	25

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)								
Activos de Información	Código de Numeración	Modo de Fallo	Efecto	Causa	Frecuencia F	Gravedad G	Detectabilidad D	IPR
Equipos de Comunicación	9.2	Datos Erróneos en las Bitácoras	Incertidumbre en la redacción	Desconfianza en la información de las bitácoras	4	4	3	48
	9.3	Perdidas de las Bitácoras	Incertidumbre de las acciones a tomar	Desconocimiento de lo ocurrido el día anterior y antes	2	4	4	32
	10.1	Equipos Obsoletos	Demora en las comunicaciones	Problemas con la comunicación	3	4	2	24
	10.2	Falta de Mantenimiento de los Equipos de Comunicación	Deterioro de los equipos de comunicación	Obsolescencia de los equipos de comunicación	5	4	2	40
	10.3	Líneas de Comunicación sin Protección	Líneas vulnerables	Infiltración de virus, spam, otros	4	5	3	60
	10.4	Arquitectura Inadecuada de la Red	Sin escalabilidad	Migración de todos los equipos de comunicación	4	5	2	40
	10.5	Conexiones de Red Publica sin Protección	Vulnerabilidad	Infiltración de virus, spam, otros	5	5	2	50

Tabla 32: Matriz AMFE

Fuente: (MINSA, 2012)

Índice de Prioridad del Riesgo

Índice de Prioridad del Riesgo	IPR

Tabla 33: Leyenda IPR

Fuente: (MINSA, 2012)

La tabla 32 - treinta y dos - mostrada anteriormente es analizada de acuerdo a los límites y criterios del Plan SGSI, el objetivo es comparar el resultado de la estimación del riesgo con los criterios y aceptación definidos; en ese momento se priorizan los riesgos que deben ser tratados y gestionados, de acuerdo al resultado de la matriz AMFE y al analizar el índice de prioridad del riesgo IPR.

La matriz AMFE nos permite evaluar la frecuencia, gravedad y defectibilidad de cada riesgo identificado. En este caso aplicado es conveniente dar prioridad a los IPR de 25 veinte y cinco – o superior con gravedad 5 -. Los riesgos con un IPR de 25 o mayor presentan una gravedad alta que perjudica a la organización y a la calidad del proceso; es por esta razón que se usara el criterio de IPR. Por ejemplo en las Instalaciones Físicas; la Inadecuada Infraestructura para Sala de Servidores, produce fallos en el servidor y la pérdida de confidencialidad son riesgos que pueden afectar a la adecuada operatividad de la comandancia, puede mermar la confianza de los usuarios, el incumplimiento en la entrega de información adecuada, aumenta el costos horas hombre al re consultar con los sistemas, lo que recae en la calidad de los procesos y servicios de la comandancia, con un considerable riesgo institucional.

Se encontraron 15 – quince – Modos de Fallos con Gravedad 5 – cinco – entre 25 – veinte y cinco – y 75 - setenta y cinco – de Índice de Prioridad de Riesgo; estos puntos serán los afrentados para la minimización de fallas.

HACER

En esta fase se ejecuta el Plan Estratégico determinado en la fase del PLANEAR que implica analizar y desarrollar los controles que permitan mitigar los riesgos encontrados en la fase antes mencionada.

PLAN DE TRATAMIENTO DEL RIESGO

Mitigar los Riesgos de:

- La seguridad para los activos
- Los acuerdo de confidencialidad interna
- Los responsables de las áreas vulnerables
- El plan de continuidad de negocio
- La seguridad en la red
- Las consideraciones de las políticas de acceso a las áreas vulnerables
- Los control de usuarios
- La fuga de información
- Las delimitación de los roles del personal
- Las políticas de seguridad

Asumir el Riesgo

- Documentos de seguridad

Transferir el Riesgo a un Tercero

Todos los riesgos deben ser asumidos por la COMANDANCIA y no transferidos a terceros por razones de seguridad interna.

Eliminar el Riesgo

Se considerara eliminar los riesgos de mayor gravedad o de mitigarlos lo menos posible.

MITIGACIÓN DEL RIESGO

En el desarrollo de la mitigación de los riesgos se seleccionaran los controles; no se implementarán controles nuevos hasta una nueva versión del Plan de SGSI; se realizaran verificaciones permanentes de los controles por medio de los indicadores implementados y se documentaran en el Plan de SGSI.

Selección de controles de la NORMA TÉCNICA PERUANA NTP ISO/IEC 27001: 2008

5.1.1 Documentos de política de seguridad de la información

6.1.3 Asignación de responsabilidades sobre seguridad de la información

6.1.5 Acuerdos de confidencialidad

7.1.1 Inventario de activos

7.1.2 Propiedad de los activos

8.1.1 Roles y responsabilidades

9.1.1 Seguridad física perimetral

10.3.1 Gestión de la capacidad

10.6.1 Controles de red

10.8.4 Seguridad del correo electrónico

11.1.1 Política de control de accesos

11.2.1 Registro de usuarios

12.5.4 Fuga de información

14.1.2 Continuidad del negocio y evaluación de riesgos

Indicadores identificados que mitigaran los riesgos.

- Activos vulnerados entre el total de activos
- Activos de información sin mecanismos de seguridad
- Activos de información con propietarios
- Personal comprometida con los acuerdos firmados
- Usuarios que cumplen con las políticas de seguridad de la información
- Procedimientos del Plan de SGSI Documentado
- Incidentes reportados
- Equipos de TI en la red
- Riesgos de la mensajería
- Control de visitantes
- Ingreso del personal
- Acceso de los usuarios
- Cumplimiento de niveles de seguridad para la información
- Funciones realizadas por el usuario
- Número de empleados que conocen las políticas de seguridad de la información entre el total de empleados

CONTROLES PARA LAS ÁREAS DEL SIMTRAC Y COSAS – SARSAT ESTABLECIDOS EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008

En este punto consideraremos las recomendaciones de las NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 en las mejores prácticas habituales para conseguir dicha seguridad; esto se visualiza en el Anexo 2; también relacionaremos las principales medidas de seguridad directamente con las áreas del SIMTRAC y del COSAS - SARSAT, los controles y su implementación, tomando como base la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 - Ver Anexo 2 -.

De la Recomendación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008:

Un punto de partida de la seguridad de la información es considerar las recomendaciones de las NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 en las mejores prácticas habituales para conseguir dicha seguridad.

- Controles esenciales para una Organización desde un punto de vista legislativa:

1. El control sobre los “Derechos de Propiedad Intelectual” que se encuentra en la cláusula “CUMPLIMIENTO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Dentro de los procesos y procedimientos establecidos se establecerá el cumplimiento de las restricciones legales, reguladoras y contractuales para el uso de material protegido por los derechos de la propiedad intelectual.

Protección de la propiedad intelectual:

- Se creara una política de derechos de autor del software definida por el área legal para estos productos.
- Se adquirirán solamente software de propietarios legales con licencias asegurando el derecho de autor.
- Concientizaremos a los usuarios sobre el derecho de autor en las adquisiciones dando a conocer las medidas de sanciones al violar estos derechos.
- Realizar registros del software para tener un control de la propiedad intelectual.
- Controlaremos la cantidad de usuarios que ingresen a los sistemas sin autorización.
- Controlaremos por medio de inventarios el software con licencias autorizados a utilizarse.
- Se efectuaran auditorias periódicas.
- Se controlaran el uso de software y de la información obtenida en las redes públicas.

2. El control sobre “Salvaguarda de los Registros de la Organización” que se encuentra en la cláusula “CUMPLIMIENTO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Se protegerán los registros de importancia en la comandancia por las posibles pérdidas, destrucción y falsificación.

- Se clasificaran los registros según sea el tipo; se guardaran los registros manteniendo su seguridad por el tiempo que se encuentren retenidos.
- Se mantendrá un control de los medios de almacenamiento por su deterioro en el tiempo según especificaciones del fabricante; incluyendo procedimientos para tener acceso a ellos.
- Se mantendrá un sistema que permita el almacenamiento y con la propiedad de poder recuperarse en el momento que se requieran.
- Crearemos guías sobre las retenciones, almacenamientos, tratamientos y eliminación de los registros para las personas responsables en la comandancia.
- Se confeccionara una agenda o calendario de la retención con periodos de caducidad de los registros.

3. El control sobre “Protección de los Datos y de la Privacidad de la Información Personal” que se encuentra en la cláusula “CUMPLIMIENTO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Se protegerán los datos y su privacidad de acuerdo a las legislaciones organizacionales.

- Crearemos una política de protección a los datos que se difundirá a todo el personal con el respectivo procedimiento a seguir.
- Se cumplirán las leyes de la protección de datos bajo una estructura de gestionable apropiada.

- Se designara un encargado para esta responsabilidad que ayude a entender y seguir los procedimientos de este servicio.

- Controles de mejores prácticas habituales para conseguir la seguridad de la información:

4. El control sobre “Documento de Política de Seguridad de la Información” que se encuentra en la cláusula “POLÍTICA DE SEGURIDAD” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Esta cláusula está desarrollada en el punto 3.1.2.3.2 Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008

5. El control sobre “Asignación de Responsabilidades sobre Seguridad de la Información” que se encuentra en la cláusula “ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Esta cláusula está desarrollada en el punto 3.1.2.3.2 Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008

6. El control sobre “Conocimiento, Educación y Entrenamiento de La Seguridad de Información” que se encuentra en la cláusula “SEGURIDAD EN RECURSOS HUMANOS” está recomendada por la

NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Brindaremos capacitaciones a los empleados; y si es necesario a los contratistas con los conocimientos y actualizaciones necesarias para la función de su trabajo.

Esto de la siguiente forma:

- Induciendo al empleado en los procesos necesarios para la designación de la seguridad de la información antes de conceder acceso a los sistemas de información o servicios.
- Los entrenamientos contemplaran los procesos de seguridad, responsabilidades legales y controles de la comandancia; así como el correcto uso de la información.

7. El control sobre “Validación de los Datos de Entrada” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Se validaran el ingreso de la información a los sistemas garantizando que sean correctos. Se consideraran:

- Que no se dupliquen las entradas detectando los errores de fuera de rango, caracteres inválidos, datos incompletos y datos no autorizados.
- Se verificara el contenido periódicamente de las claves para su validez e integridad.
- Verificaremos que los archivos físicos no tengan cambios no autorizados en sus ingresos de datos.

- Confeccionaremos procedimientos para los posibles errores de validación.
- Se otorgaran responsabilidades de los encargados en la entrada de datos.
- Todo lo efectuado se registrara y esto será un procedimiento de los datos de entrada.

8. El control sobre “Control del Proceso Interno” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Se integrara un sistema que nos permita monitorear los ingresos corruptos o con errores o por acciones negativas al sistema.

Aseguraremos con restricciones el riesgo de fallos al proceso; se considerara:

- Las funciones agregar y eliminar para modificaciones en los datos.
- Programas que aseguren la recuperación luego que se produzcan las fallas.
- Protegeremos la entrada de datos contra ataques usando corridas o desbordes de buffers.

En este punto se verificaran los accesos teniendo una documentación apropiada con lo siguiente:

- Un control de sesiones.
- Un control de tiempo de uso del sistema.
- Un control del perfil de ingreso con sus actividades.
- Un control que verifique que el sistema está operando adecuadamente.
- Se crearan registros de todas las actividades.

9. El control sobre “Integridad de Mensajes” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Asegurar la autenticidad e integridad de los mensajes con la creación de controles aceptados por la comandancia y que cumplan con las normativas de la misma.

La comandancia conviene en usar criptografías como medio adecuado para autenticación; esta será realizada por un área específica de la marina de guerra encargada de estos procedimientos.

10. El control sobre “Validación de los Datos de Salida” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

La validación de datos salientes se realizara por medio de encriptación de la VPN con el proveedor de servicio de datos externos; estas contienen:

- Veracidad de los datos para ser usados en el sistema.
- Un control que permita que asegure el correcto funcionamiento de todos los datos.
- Un registro de actividades y tareas para validar los datos de salida.

11. El control sobre “Control de las Vulnerabilidades Técnicas” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA

TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Mantener siempre informado de las vulnerabilidades del sistema; y evaluar a la comandancia sobre tales vulnerabilidades para tomar medidas apropiadas.

Se realizaran los inventarios técnico respectivo a fin de gestionar las vulnerabilidades; este inventario contemplara al proveedor de software, sus versiones y los responsables de estas aplicaciones en la comandancia.

Localizando las vulnerabilidades técnicas:

- Se definirán roles y responsabilidades en la gestión de vulnerabilidades así como su respectivo monitoreo de las mismas.
- Los recursos destinados para identificar las vulnerabilidades y su monitoreo serán actualizados de acuerdo a los cambios de inventarios.
- Verificaremos las vulnerabilidades con los riesgos asociados a ellos para posteriores acciones a tomar en cuenta.
- Siendo la vulnerabilidad alta las acciones a tomar serán de acuerdo a los controles de la gestión del cambio (ver 12.5.1).
- Si existen ecualizaciones se verificaran primero los riesgos de esta actualización; estos deberán ser evaluados antes de su instalación.
- Llevar un registro de ingresos para los procedimientos realizados.
- Los sistemas de mayor riesgo siempre serán tratados con prioridad.

12. El control sobre “Aprendiendo de los Incidentes en La Seguridad de Información” que se encuentra en la cláusula “GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Se utilizara una tarea que permita monitorear y cuantificar los costos de los incidentes en la seguridad de la información.

La información obtenida en la evaluación de los incidentes en la seguridad de la información se usara para visualizar los que se repiten o sean de gran impacto.

13. El control sobre “Recolección de Evidencia” que se encuentra en la cláusula “GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Los datos históricos servirán como evidencias que serán recolectadas, retenidas y presentadas según sean necesarias para implicancias legales correspondientes.

Existen procesos disciplinarios en la comandancia a los que se les integrara las evidencias necesarias para dicho propósito.

Usaremos:

- Evidencias que puedan ser usadas en las cortes militares y civiles; para esto los sistemas deben cumplir estándares para que la evidencia sea utilizada.
- De alta calidad y completa evidencia del acto en cuestión; debe ser confiable sin manipulación alguna durante el periodo de la evidencia.
- En documentos físicos; se tendrán registro de su hallazgo desde quien lo encontró, donde, cuando y un testigo del encuentro.
- En medios informáticos; se tomaran en cuenta las copias de seguridad e información de los discos duros. Se registraran todas las acciones realizadas a los medios o dispositivos de evidencia.

Los trabajos forenses solo se realizaran en la copia del material en evidencia. El material debe ser íntegro y protegido; las posibles copias requeridas serán supervisabas y registradas de cuando, donde, como y con qué herramienta fue realizado.

14. El control sobre “Incluyendo la Seguridad de Información en el proceso de Gestión de la Continuidad del Negocio” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Propondremos un proceso de gestión de desarrollo y mantenimiento para la continuidad del negocio que trate la seguridad de la información para dicha continuidad.

Consideraremos:

- Hacer entender los riesgos de la organización desde sus vulnerabilidades e impacto identificando y priorizando sus procesos críticos.
- Identificaremos los activos que estén en los procesos críticos del negocio.
- Sensibilizar sobre el impacto que causaría la interrupción del negocio.
- Aconsejaremos la adquisición de seguros que serán parte del proceso de continuidad de negocios.
- Implementaremos controles de prevención.
- Asegurar la seguridad del personal y la protección de las instalaciones y propiedad de la comandancia.
- Se formulara y documentara planes de continuidad de negocio a la par con la seguridad de la información.
- Incorporaremos la gestión de la continuidad del negocio en los procesos de la organización.

15. El control sobre “Continuidad del Negocio y Evaluación de Riesgos” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Esta cláusula está desarrollada en el punto 10.1.2.1.2 Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.

16. El control sobre “Redacción e Implantación de Planes de Continuidad que incluyen La Seguridad de Información” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Desarrollaremos planes de mantenimiento y recuperación de las operaciones del negocio asegurando la disponibilidad de la información en el tiempo necesario en una interrupción o falla de los procesos críticos.

Consideraremos:

- Los procedimientos de emergencia y acuerdos de responsabilidades.
- Aceptaremos ciertas perdidas de información y servicios que no comprometan a la comandancia.
- Evaluaremos escalas de tiempo para la recuperación y restauración de las operaciones por medio de procedimientos.
- Evaluaremos procedimientos operativos para la recuperación y restauración total.
- Documentar siempre los procedimientos acordados.

- Pruebas y mejoramiento de los planes acordados.

17. El control sobre “Marco de Planificación para La Continuidad del Negocio” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Crear una estructura de planes para la continuidad del negocio asegurando que los planes sean consistentes y nos permitan priorizar la seguridad, pruebas y mantenimiento.

El plan de continuidad de negocio estará limitado al alcance especificando claramente en que momentos se tomara acción de dicho plan incluyendo los procedimientos dentro de la gestión de cambios de la comandancia.

Determinando la envergadura de la comandancia se tendrán en cuenta uno o más planes con sus respectivos propietarios.

Se considera lo siguiente:

- Que los planes describan los procedimientos antes de dicha acción.
- Las acciones a tomar en caso de emergencias que amenacen a las actividades de la organización.
- Acciones necesarias de respaldo que permitan restablecer a la organización y volverla operativa en el tiempo requerido.
- Tareas requeridas que permitan terminar con la restauración y que las operaciones de la organización vuelvan a la normalidad.
- Los mantenimientos preventivos respectivos al plan realizando las pruebas necesarias para conocer su efectividad.
- Acciones de concientización de los procedimientos de la organización que aseguren su total entendimiento.

- Los responsables de las acciones críticas tendrán suplentes que permitan activar el plan en caso de pruebas, emergencia, respaldo y activación.

18. El control sobre “Prueba, Mantenimiento y Reevaluación de los Planes de Continuidad” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Implementación del Control:

Estos planes serán evaluados constantemente con el fin de actualizarlos y probar sus resultados.

Las pruebas consistirá en que los equipos de recuperación estarán atentos a sus responsabilidades para la continuidad de la organización y aseguramiento de la información conociendo sus roles dentro del plan.

La confección del plan de pruebas contendrá las fechas de estas mismas y la realización una por una.

Contemplaremos:

- Las pruebas en varios casos.
- Entrenamiento al equipo con simulaciones de los casos que podrían suceder.
- Las acciones para la recuperación de los sistemas de información.
- Las acciones a tomar para recuperación de la organización se al caso en un lugar diferente al actual.
- Que los proveedores de servicios cumplan los compromisos establecidos para la recuperación.

Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008:

Relacionaremos las principales medidas de seguridad directamente con las áreas del SIMTRAC y del COSAS - SARSAT, los controles y su implementación, tomando como base la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 - Ver Anexo 2 -.

1. El control sobre la “Documento de Política de Seguridad de La Información” que se encuentra en la cláusula “POLÍTICA DE SEGURIDAD” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No existen políticas de seguridad.

Implementación del Control:

Se iniciara con la concientización de las jefaturas de la comandancia comprometiéndolos a apoyar las distintas políticas que se implementaran en la seguridad de la información.

En principio se creara un documento de seguridad de la información que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Se definirá los objetivos de la seguridad de la información.
- Dentro de los objetivos de la jefatura es apoyar a los objetivos de la seguridad de la información.
- Un alcance que contendrá los objetivos de control, la evaluación de riesgos y la gestión de riesgos.
- Una breve explicación para los requisitos legislativos y contractuales; requisitos de formación en seguridad; gestión de la continuidad del

negocio y las consecuencias de las violaciones de la política de seguridad.

- Definiciones de las responsabilidades generales y específicas de la gestión de la seguridad de la información y de las incidencias de seguridad.
- Referencias de documentos que sustentarían la política.

2. El control sobre “Asignación de Responsabilidades sobre Seguridad de La Información” que se encuentra en la cláusula “ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay un responsable de las áreas vulnerables; no existen documentos de seguridad.

Implementación del Control:

Se consolidara las responsabilidades para la seguridad de la información esto en base a las políticas de seguridad para los activos creando procesos de seguridad claros; esto estará especificado en una guía que tendrá las ubicaciones, sistemas o servicios específicos; contendrá también la responsabilidad del proceso del plan de continuidad de negocio.

También contendrá:

- Identificación de los activos y procesos de seguridad por cada uno de los sistemas.
- Se nombrara al responsable del activo o procedimiento de seguridad documentando su responsabilidad.
- Se definirá y documentara los niveles de seguridad.

3. El control sobre “Acuerdos de Confidencialidad” que se encuentra en la cláusula “ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay acuerdos de confidencialidad internas.

Implementación del Control:

Los acuerdos de confidencialidad para la comandancia serán identificados y revisados continuamente anexando los requisitos indispensables para la protección de la información considerando los términos legales para este fin.

Consideraremos:

- La interpretación y clara definición de la información que será protegida.
- Acordar un tiempo de confidencialidad para la información o sin límite de tiempo.
- Las acciones necesarias al culmino de un acuerdo si es el caso.
- La responsabilidad y acciones a tomar para evitar acceso a la información no autorizada.
- Al propietario de la información; secretos de la comandancia y propiedad intelectual todo relacionado con la protección de la información.
- Los permisos de utilización de la información y los derechos y deberes de usarla.
- Procedimientos para las notificaciones del uso de información confidencial.
- Procedimientos para la destrucción de la información cuando esta sea cesada.
- Tomar acciones en caso no se cumpla este acuerdo.

4. El control sobre “Inventario de Activos” que se encuentra en la cláusula “CLASIFICACIÓN Y CONTROL DE ACTIVOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay seguridad para los activos.

Implementación del Control:

Serán identificados los activos de información con un inventario que será actualizado cada vez que se adquiera un activo.

El inventario estará descrito en un documento que incluirá toda la información que nos permita la recuperación de los mismos en caso de desastres; este debe discriminar entre los activos más importantes para que la organización sigua funcionando; aparte de los detalles de los activos como marca, modelo, entre otros; este debe contener a los propietarios de estos activos.

5. El control sobre “Propiedad de los Activos” que se encuentra en la cláusula “CLASIFICACIÓN Y CONTROL DE ACTIVOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay seguridad para los activos.

Implementación del Control:

No hay un área de sistemas designada en la comandancia; pero si un administrador de la red o responsable de los sistemas quien será el que tenga los procesos de información designados de la organización.

Se responsabilizara a los propietarios de los activos en las siguientes acciones:

- Que aseguren la información y los activos correspondientes clasificándolos apropiadamente.
- Definir y revisar cada cierto tiempo las restricciones de acceso considerando las políticas de control utilizadas.

6. El control sobre “Inclusión de la Seguridad en las Responsabilidades y Funciones Laborales” que se encuentra en la cláusula “SEGURIDAD EN RECURSOS HUMANOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No están delimitados los roles del personal.

Implementación del Control:

La comandancia tiene a bien elaborar los contratos por un área legal responsable; por lo tanto se inicializara con las funciones, responsabilidades y con un acuerdo de confidencialidad que también será documentada con los expedientes del contratado.

A los responsables de la seguridad se les comunicara de manera clara sus funciones durante su clasificación.

Las funciones de seguridad y responsabilidades contendrán:

- Implementadas y realizadas en coincidencia con las políticas de seguridad de la organización vistas en el punto 5.1.
- Deberán proteger los activos no autorizados de ser adulterados por alguna forma o razón.
- Tendrán procesos y actividades especiales para su ejecución.
- Al responsable asignado deberá tomar las acciones pertinentes según sea el caso.
- Serán reportados los incidentes que alteren la seguridad de la organización o que puedan ser un riesgo potencial.

7. El control sobre “Perímetro de Seguridad Física” que se encuentra en la cláusula “SEGURIDAD FÍSICA Y DEL ENTORNO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay seguridad en la red.

Implementación del Control:

Se realizara una nueva arquitectura de red con un cableado estructurado acorde a las nuevas tendencias tecnológicas; un nuevo data center de la misma manera y la seguridad requerida para dicho fin.

Pautas para el perimetraje de la seguridad física:

- Acorde con la evaluación de riesgos la seguridad estará definida; esto también en concordancia con los requisitos de seguridad del activo.
- En la construcción del edificio los muros de acceso deberán estar debidamente sólidos y los accesos contendrán equipos biométricos para los accesos a los ambientes que requieran la seguridad respectiva.
- Tendrá contemplado un área de recepción y control de acceso.
- Contemplara barreras de seguridad en todo el edificio evitando así entradas no autorizadas y contaminación del entorno.
- Tanto las salidas de emergencias y puertas de escape tendrán algún dispositivo de visualización o sonoro para saber dónde se encuentran en el momento de un incidente real; estos lugares serán evaluados y probados su resistencia en concordancia de los estándares requeridos para dicho fin.
- El área de procesamiento de información será separada físicamente para que no sean manipuladas por terceros.

8. El control sobre “Planificación de la Capacidad” que se encuentra en la cláusula “GESTIÓN DE COMUNICACIONES Y OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay seguridad para los activos.

Implementación del Control:

Por buenas practicas es recomendable no exceder del 20% de la capacidad máxima, por lo tanto los activos de información de la comandancia se tendrá que velar y monitorear que siempre tenga capacidad adecuada para su seguridad, lo cual la norma recomienda lo siguiente:

Se creará un documento de la capacidad de seguridad de la información que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Se deberá planificar los tiempos de llegada los recursos y sus costos, lo cual la gerencia tiene que monitorear la utilización de los recursos.
- La Gerencia deberá utilizar herramientas tecnológicas para determinar la tendencia de uso, relativamente al negocio.
- Los administradores deberán de analizar esta información y prever posibles amenazas sobre la seguridad de información y se deberá planificar el Plan de Acción respectivo.

9. El control sobre “Controles de Red” que se encuentra en la cláusula “GESTIÓN DE COMUNICACIONES Y OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay seguridad en la red.

Implementación del Control:

Las redes es una pieza fundamental para la seguridad de información en cualquier organización, lo cual la norma recomienda lo siguiente:

Se creará un documento de la seguridad de red que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- En la comandancia debe de separar la responsabilidad operativa y la operación operativa de las computadoras.
- La comandancia tiene que establecer responsabilidades para la administración de equipos remotos.
- La comandancia debe establecer procedimientos para proteger la confidencialidad e integridad de los datos que pasan a través de la red.
- La comandancia deberá contar con un registro y monitoreo de acciones de seguridad.
- La comandancia debe de realizar coordinaciones para verificar si se están aplicando los controles en toda la infraestructura de red.

10. El control sobre “Seguridad en la Mensajería Electrónica” que se encuentra en la cláusula “GESTIÓN DE COMUNICACIONES Y OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay seguridad en la red.

Implementación del Control:

Los correos electrónicos es una fuente de información que debe ser protegida, lo cual la norma recomienda lo siguiente:

Se creará un documento de la seguridad de red, respecto a la seguridad de correos electrónicos, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- La comandancia debe de establecer la protección de ingreso de correos.
- La comandancia debe establecer aquellas direcciones permitibles.
- La comandancia debe considerar las firmas digitales.
- La comandancia debe establecer una política para el personal autorizado que tenga correo para acceder desde wifi o acceso público de internet.

11. El control sobre “Política de Control de Accesos” que se encuentra en la cláusula “CONTROL DE ACCESOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No se toman en cuenta las políticas de acceso a las áreas vulnerables.

Implementación del Control:

Los accesos a cualquier fuente de información que deberá estar documentada, revisada y tiene que estar alineada a los requerimientos de seguridad y del negocio, lo cual la norma recomienda lo siguiente:

Se creará un documento de control de acceso, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- La comandancia debe identificar toda la información sobre el acceso a las aplicaciones con sus respectivos riesgos.
- La comandancia debe realizar políticas para la distribución de información y autorizaciones, lo cual debe tener coherencia entre control de accesos y clasificación de información.

- La comandancia debe establecer perfiles de acceso de usuario estandarizados.
- La comandancia debe tener la administración de acceso distribuido de la red con su rol de control respectivo.
- La comandancia debe de controlar el acceso a las áreas, solo para aquellas personas que se encuentre en el registro de usuario.
- La comandancia debe de generar periódicamente el monitoreo sobre el retiro de acceso a aquellas personas que ya no laboran o se desvinculen del área de sistemas.

12. El control sobre “Registro de Usuarios” que se encuentra en la cláusula “CONTROL DE ACCESOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No hay un control de usuarios.

Implementación del Control:

Un procedimiento adecuado de registro de usuario actualizando las altas y bajas de usuarios, garantiza un seguro acceso de los sistemas, lo cual la norma recomienda lo siguiente:

Se creará un documento de registro de usuario, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Implementar la utilización de un identificador único para cada usuario, con esta acción se vincularía a los usuarios con sus acciones.
- Realizar un control de comprobación de autorización de usuario.
- Se debe de entregar a los usuarios una relación de sus derechos de acceso.
- Se debe de cumplir la negación de acceso a menos que hayan completado los procedimientos de autorización.

- Realizar un mantenimiento del registro de autorización de acceso del servicio.
- Monitorear periódicamente la eliminación de identificadores y cuentas de usuario redundantes.
- Asegurar la no reasignación de usuarios con identificadores de usuarios dados de baja.

13. El control sobre “Fuga de Información” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: Fuga de información.

Implementación del Control:

La fuga de información debe de ser prevenida, lo cual la norma recomienda lo siguiente:

Se creará un documento de fuga de información, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Detectar todos los medios de salida de información como puerto usb, correos, carpetas compartidas, etc.
- Monitorear periódicamente las actividades del personal y del sistema, bajo las normas legales.
- Monitorear el uso de recursos en sistemas de cómputo.

14. El control sobre “Continuidad del Negocio y Evaluación de Riesgos” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” es obtenida por la NORMA TÉCNICA PERUANA NTP-

ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue.

Deficiencia: No existe un plan de continuidad de negocio.

Implementación del Control:

La continuidad del negocio es el punto más común y difícil que debe afrontar cualquier organización, identificar sus causas y darle pronta solución, lo cual la norma recomienda lo siguiente:

Se creará un documento de continuidad del negocio, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Identificar los eventos que puedan causar interrupciones en los procesos de negocio.
- Se debe de evaluar los riesgos para determinar su probabilidad e impacto de dichas interrupciones, debe incluir aspectos de seguridad de información, debe ser cuantificable y priorizar a los alineamientos de los objetivos de La Comandancia, incluyendo impacto de las interrupciones tiempos aceptables de la interrupción y prioridades de recuperación.
- Desarrollar un Plan Estratégico con un enfoque global de la continuidad del negocio a partir de la evaluación de riegos.
- Una vez aprobada el Plan Estratégico la jefatura de La Comandancia deberán respaldarla y desarrollar un Plan de Implementación de dicha estrategia.

FORMACIÓN, TOMA DE CONCIENCIA Y COMPETENCIA

La Comandancia de Operaciones Guardacostas implementará en su marco profesional para la capacitación de su personal Oficial; personal que estará encargado de dirigir las mejoras para la implementación del Plan de

SGSI y a su personal Subalterno quienes estarán a cargo de la parte operativa en las distintas áreas en donde será implementado el Plan de SGSI.

OBJETIVOS DE CONTROL E INDICADORES

Estos son los Objetivos de Control determinados que nos ayudaran a mitigar los riesgos encontrados.

A.5.1. Política de seguridad de la información

A.6.1 Organización interna

A.7.1 Responsabilidad por los activos

A.8.1. Previo al empleo

A.9.1. Áreas seguras

A.10.3. Planificación y aceptación del sistema

A.10.6 Gestión de seguridad de redes

A.10.8. Intercambio de información

A.11.1. Requisitos de negocio para el control de accesos

A.11.2 Gestión de acceso de usuarios

A.12.5. Seguridad en los procesos de desarrollo y soporte

A.14.1. Aspectos de la gestión de continuidad del negocio en la seguridad de información

Objetivos de Control de la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 asociadas a los indicadores de control.

Cláusula, Objetivos de Control y Controles asociados a los Indicadores

Núm.	NTP ISO/IEC 27001 / 2008	Indicadores
1	7.1.1; 7.1.2; 10.3.1	Activos vulnerados entre el total de activos
		Activos de información sin mecanismos de seguridad
		Activos de información con propietarios
2	6.1.5	Personal comprometida con los acuerdos firmados
3	6.1.3; 6.1.5	Usuarios que cumplen con las políticas de seguridad de la información
4	6.1.3; 6.1.5	Procedimientos del Plan de SGSI Documentado
5	14.1.2	Incidentes reportados
6	9.1.1; 10.6.1; 10.8.4	Equipos de TI en la red
		Riesgos de la mensajería
		Control de visitantes
7	5.1; 11.1.1; 11.2.1	Ingreso del personal
8	5.1; 11.1.1; 11.2.1	Acceso de los usuarios
9	12.5.4	Cumplimiento de niveles de seguridad para la información
10	5.1.1; 8.1.1	Funciones realizadas por el usuario
11	5.1.1; 8.1.1	Número de empleados que conocen las políticas de seguridad de la información entre el total de empleados

Tabla 34: NTP vs Indicadores

FUENTE: Elaborado por los autores

VERIFICAR

En esta fase verificaremos el Plan de SGSI; mediremos la eficiencia de los controles y revisaremos los riesgos residuales.

REVISIÓN DEL PLAN SGSI

En esta revisión del Plan de SGSI se comienza a revisar el Plan de SGSI, se revisa nuevamente las deficiencias encontradas en la Comandancia de Operaciones de Guardacostas y se verifica si cumple con los controles identificados para ellos en la 1ra versión del Plan de SGSI; esta revisión sirve para encontrar nuevas deficiencias y/o controles que se ajusten. En este caso no se encontraron más deficiencias por lo tanto son los mismos controles que satisfacen con los mismos. -Ver Tabla 35 -.

Chequeo de los Controles

Check List de los Controles		
Control	**Deficiencia en la Comandancia de Operaciones Guardacostas**	**Cumple**
Documento de política de seguridad de la información	No existen políticas de seguridad	☑
Asignación de responsabilidades sobre seguridad de la información	No hay un responsable de las áreas vulnerables	☑
Acuerdos de confidencialidad	No hay acuerdos de confidencialidad internas	☑
Inventario de activos	No hay seguridad para los activos	☑
Propiedad de los activos		☑
Planificación de la capacidad		☑
Inclusión de la seguridad en las responsabilidades y funciones laborales	No están delimitados los roles del personal	☑
Controles de red	No hay seguridad en la red	☑
Seguridad en la mensajería electrónica		☑
Perímetro de seguridad física		☑
Política de control de accesos	No se toman en cuenta las políticas de acceso a las áreas vulnerables.	☑
Registro de usuarios	No hay un control de usuarios	☑
Fuga de Información	Fuga de información	☑
Continuidad del negocio y evaluación de riesgos	No existe un plan de continuidad de negocio	☑

Tabla 35: Check List de Controles

Fuente: Elaborado por los Autores

MEDIR EFICIENCIA DE LOS CONTROLES

En el punto 2.2.1.3.2 nos permite escoger una herramienta que evaluará la eficiencia de los controles respecto a los riesgos encontrados; esto lo determinamos en la tabla 36 – treinta y seis -; esta tabla se tomará como plantilla y se encuentra en el Anexo C.

Plan de Verificaciones del Plan de Sistema de Gestión de Seguridad de la Información

PLAN DE VERIFICACIÓN DEL PLAN DE SGSI					
Riesgo a Controlar	Método de control			Objetivo de Control	Indicador
	Control Implementado	Registro	Responsable		
No existen políticas de seguridad	Documento de política de seguridad de la información	Registro de aprobación de políticas	PAREDES BLANCO, CESAR	Aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	Número de empleados que conocen las políticas de seguridad de la información entre el total de empleados
No hay un responsable de las áreas vulnerables	Asignación de responsabilidades sobre seguridad de la información	Registro de actividades y responsabilidades	PAREDES BLANCO, CESAR	Gestionar la seguridad de la información dentro de la organización.	Usuarios que cumplen con las políticas de seguridad de la información
No hay acuerdos de confidencialidad internas	Acuerdos de confidencialidad	Registro en documento firmado	PAREDES BLANCO, CESAR		Personal comprometida con los acuerdos firmados
No hay seguridad para los activos	Inventario de activos	Registro de inventarios de activos de información asignado propietario de los mismos	SANTA MARIA OLIVA ENRIQUE	Mantener una protección adecuada sobre los activos de la organización. Todos los activos deben ser considerados y tener un propietario asignado.	Activos vulnerados entre el total de activos
	Propiedad de los activos		SANTA MARIA OLIVA ENRIQUE		Activos de información sin mecanismos de seguridad
	Planificación de la capacidad		SANTA MARIA OLIVA ENRIQUE		Activos de información con propietarios

PLAN DE VERIFICACIÓN DEL PLAN DE SGSI					
Riesgo a Controlar	Método de control			Objetivo de Control	Indicador
	Control Implementado	Registro	Responsable		
No están delimitados los roles del personal	Inclusión de la seguridad en las responsabilidades y funciones laborales	Registro de roles del personal de T.I.	SEMINARIO SEMINARIO, LUIS	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y entiendan sus roles, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones.	Funciones realizadas por el usuario
No hay seguridad en la red	Controles de red	**Registro de configuración de la infraestructura de red, correos electrónicos**	SEMINARIO SEMINARIO, LUIS	Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.	Equipos de TI en la red
	Seguridad en la mensajería electrónica		SEMINARIO SEMINARIO, LUIS	Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones	Riesgos de la mensajería
	Perímetro de seguridad física		SEMINARIO SEMINARIO, LUIS	Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.	Control de visitantes
No se toman en cuenta las políticas de acceso a las áreas vulnerables	Política de control de accesos	Registro de políticas de acceso a los ambientes y aplicaciones	SEMINARIO SEMINARIO, LUIS	Controlar los accesos a la información.	Ingreso del personal
No hay un control de usuarios	Registro de usuarios	Registro de usuarios identificados en el AD	LUN PUN TORRES VICTOR	Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.	Acceso de los usuarios
Fuga de información	Fuga de Información	Registrar los niveles de seguridad a los documentos requeridos	LUN PUN TORRES VICTOR	Mantener la seguridad del software de aplicación y la información. Se deberían controlar	Nivel de Seguridad para los Documentos

PLAN DE VERIFICACIÓN DEL PLAN DE SGSI						
Riesgo a Controlar	Método de control			Objetivo de Control	Indicador	
	Control Implementado	Registro	Responsable			
		Registrar los bloqueo de puertos usb, no tener lectora DVD en las pc's	LUN PUN TORRES VICTOR	estrictamente los entornos del proyecto y de soporte.	Nivel de Seguridad para los Sistemas	
		Registrar los perfiles de usuarios	LUN PUN TORRES VICTOR		Nivel de seguridad para los usuarios	
No existe un plan de continuidad de negocio	Continuidad del negocio y evaluación de riesgos	Registro en documento de nuevos riesgos encontrados	LUN PUN TORRES VICTOR	Reaccionar a la interrupción de actividades de la organización y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.	Incidentes reportados	

Tabla 36: Plan De Verificación del Plan de SGSI

Fuente: Elaborado por los Autores

REVISAR RIESGOS RESIDUALES

Vamos a identificar aquellos riesgos que quedan después de haber aplicado el Plan de Contingencia a los Riesgos. En la matriz AMFE desarrollado en el punto página 162 nos permite contar con los riesgos identificados. En este caso solo se revisará los riesgos con prioridad de IPR de 25 o superior, porque presentan una gravedad alta que perjudica a la organización y a la calidad del proceso.

Nuestros riesgos residuales serán considerados aquellos de Gravedad con nivel 5, 4 y 3; los riesgos de Gravedad de nivel 2 y 1 serán riesgos considerados aceptables para la COMANDANCIA.

Matriz AMFE Riesgos Residuales (Análisis Modal de sus Fallas y sus Efectos)

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)										
Activos de Información	RIESGOS	Modo de Fallo	Frecuencia F		Gravedad G		Detectabilidad D		IPR	
			Antes	Después	Antes	Después	Antes	Después	Antes	Después
Personal Destacado al Área	1; 2; 3; 8; 9; 10	Divulgación de la Información Confidencial	2	1	5	3	3	2	30	6
Instalaciones Físicas	1; 3; 5; 6; 11	Inadecuada Infraestructura de red	5	3	5	3	2	2	50	18
		Inadecuada Infraestructura para Sala de Servidores	5	2	5	2	1	1	25	4
Sistemas Operativos	1; 5; 7; 8; 9; 11	Perdida de la Información por falla de Servidor	5	3	5	2	2	2	50	12
		Sin Soporte para SO Libre	5	5	5	4	1	1	25	20
Servidores	1; 3; 5; 6; 7; 8; 11	Lentitud en la Capacidad de Procesamiento	5	3	5	3	2	2	50	18
		Poco Espacio de Almacenamiento	5	4	5	2	2	2	50	16
Sistemas de Información Servidores	1; 2; 5; 6; 7; 8; 9; 11	Sin Soporte para Sistema Servidor de Correo Libre	5	3	5	3	2	2	50	18

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)												
Activos de Información	RIESGOS	Modo de Fallo	Frecuencia F		Gravedad G		Detectabilidad D		IPR	
			Antes	Después	Antes	Después	Antes	Después	Antes	Después
		Sin Soporte para Sistema Servidor de la Pagina Web Libre	5	3	5	3	3	2	75	18
		Falla en las Transacciones con la Base de Datos	5	3	5	2	3	2	75	12
Información de Embarcaciones	2; 4; 5; 9	Datos Erróneos del Monitoreo de las Embarcaciones	3	3	5	2	4	3	60	18
Informe de Operaciones	2; 4; 5; 9	Carencia de Automatización de las Bitácoras	5	3	5	2	1	1	25	6
Equipos de Comunicación	1; 3; 5; 6; 7; 9; 10; 11	Líneas de Comunicación sin Protección	4	2	5	2	3	2	60	8
		Arquitectura Inadecuada de la Red	4	4	5	2	2	2	40	16
		Conexiones de Red Publica sin Protección	5	3	5	2	2	1	50	6

Tabla 37: Matriz AMFE Riesgos Residuales (Análisis Modal De Sus Fallas Y Sus Efectos)

Fuente: Elaborado por los Autores

ACTUAR

Es en esta fase implantaremos las medidas preventivas y correctivas de las revisiones efectuadas y mejorar así el rendimiento del Plan de SGSI. Las medidas correctivas comprenden la selección de nuevos controles, la modificación de los existentes o la eliminación de los obsoletos.

Entradas del Proceso y Salida del Proceso

Utilizaremos la herramientas de las “5 ¿POR QUÉ?” para establecer los planes de acción efectivos al momento de resolver un problema dentro de la Comandancia de Operaciones Guardacostas; en el Anexo D, podremos visualizar esta herramienta.

ACCIONES PREVENTIVAS Y CORRECTIVAS

Encontrado algún incumplimiento de un requisito, se deben toman acciones para resolver esa situación no deseada. La Norma NTP-ISO/IEC 27001:2008 divide en dos tipos de acciones a tomar: Acciones correctivas y Acciones preventivas.

En el Anexo D, se muestra la herramienta que se usó en la Comandancia de Operaciones de Guardacostas para estas acciones.

Las tablas 38 – treinta y ocho – y 39 – treinta y nueve -; están desarrolladas bajo la metodología de los “5 ¿POR QUÉ?”; esta herramienta es utilizada para actuar en el incumplimiento de un requisito y se separa en dos tipos de planes Preventivo y Correctivo.

En el Anexo D utilizaremos la plantilla de la metodología “5 ¿POR QUÉ?”.

Acciones Preventivas.

PLAN DE ACIONES PREVENTIVA - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
No existen políticas de seguridad de información	1- No se tiene claro la importancia de seguridad de información en las áreas SIMTRAC Y COMPAS SARSAT 2- No hay registro histórico de políticas de seguridad de información. 3- El personal trabaja por experiencia, sin alinearse a normas. 4- En la Comandancia se trabaja por "obligaciones". 5- En la Comandancia trabaja por órdenes jerárquico.	- Ofrecer capacitación sobre políticas de seguridad a todo el personal de las áreas SIMTRAC Y COMPAS SARSAT. - Ofrecer cursos de seguridad de información a los jefes de área para que lo comparta con su equipo de trabajo. - Visitar a entidades del estado que cuenten con políticas de seguridad de información bajo NTP-ISO/IEC 27001:2008 para ver la importancia.
No hay un responsable de las áreas vulnerables	1- No hay un organigrama de personal asociado a sus responsabilidades de seguridad de información. 2- No se tiene conocimiento a quien reportar incidencias y clasificarlas. 3- Hay mucha rotación de personal en las áreas SIMTRAC Y COMPAS SARSAT. 4- No hay delegación de personal sobre activos de información vulnerables. 5- Los jefe de área no quieren hacerse responsables sobre una incidencia mayor o desastre.	- Desarrollar matriz RACI para el personal de sistemas en las áreas SIMTRAC Y COMPAS SARSAT. - Capacitar al personal de sistemas en las áreas SIMTRAC Y COMPAS SARSAT, sobre riesgos informáticos. - Entregar un manual de clasificación de riesgos de las áreas de SIMTRAC Y COMPAS SARSAT.
No hay acuerdos de confidencialidad internas	1- No existen los acuerdos para la seguridad de información. 2- El personal Oficial encargado de las áreas no se responsabiliza de la seguridad de los activos de información. 3- Poco interés en la información confidencial asignada a los usuarios. 4- Se comparte la información sin ningún medio de confidencialidad. 5- Los acuerdos de confidencialidad con terceros no se	- Elaborar documentación para las políticas de confidencialidad. - Logran el compromiso de confidencialidad.

PLAN DE ACIONES PREVENTIVA - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
	les hace un seguimiento.	
No hay seguridad para los activos de información	1- No hay un control de inventario de activos de información. 2- No existen responsabilidad asignada de los activos de información. 3- La adquisición de un activo de información no está evaluado y no se encuentra en los inventarios. 4- El dado de baja de un activo de información es interno no llega a su destino de desuso. 5- La compra de un activo de información es adquirida por necesidad propia-	- Realizar documentación de inventarios de activos de información. - Las responsabilidades deberían ser consideradas bajo una matriz RACI. - Tener un registro que controle los activos de información que son dados de baja. - Llevar un registro de las compras de activos de información.
No están delimitados los roles del personal	1- Las funciones internas del personal no contemplan la seguridad de los activos de información. 2- El personal se limita a sus funciones internas. 3- Las jefaturas no promueven la seguridad de los activos de información. 4- EL personal no transmite sus conocimientos al delegar funciones en sus traslados de áreas. 5- La información de sus trabajos no es tratada con la seguridad requerida de acuerdo a sus funciones.	- Dentro de las funciones del personal contemplar la seguridad de los activos de información. - Los roles deberían ser consideradas bajo una matriz RACI alineada a actividades. - Las jefaturas deben concientizar al personal sobre la seguridad de la información.
No hay seguridad en la red	1- Los dispositivos de red no tienen una normativa de seguridad de la información. 2- No hay un inventario de dispositivita de red. 3- No hay homogeneidad en los dispositivos de red. 4- El cableado estructurado no está normalizado. 5- No hay un Firewall que separe la parte privada de la organización de la pública.	- Homogenizar los dispositivos de red. - Contar con uno o más Firewall que brinden mayor seguridad a la red. - Estandarizar el cableado estructurado. - Contar con un registro del inventario de los equipos de red.

PLAN DE ACIONES PREVENTIVA - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
No se toman en cuenta las políticas de acceso a las áreas vulnerables	1- No hay interés por parte del personal sobre las políticas de acceso a las áreas vulnerables. 2- No hay un repositorio de datos para la documentación que permita el acceso a los usuarios por perfiles. 3- En las áreas no existe seguridad física por lo que se encuentran vulnerables. 4- No hay un registro de control de acceso al data center. 5- Existe confianza excesiva con los proveedores.	- Concientizar al personal sobre el uso de las políticas de acceso a las áreas vulnerables. - Crear repositorios de datos para la información vulnerable. - Llevar un registro del acceso al data center y otro a las áreas vulnerables. - Limitar el acceso a personal ajeno a las áreas vulnerables.
No hay un control de usuarios	1- Los sistemas carecen de un control de usuarios por perfiles de seguridad. 2- La asignación de acceso a los sistemas no tiene un registro. 3- En la arquitectura de los servidores no hay un dominio que administre a los usuarios. 4- Los usuarios permiten el acceso al área a personal ajeno. 5- Los usuarios no tienen conocimiento de sus funciones asignadas.	- Crear controles de acceso para los usuarios. - Crear un dominio para la red. - Capacitar al personal sobre sus funciones asignadas.
Fuga de información	1- El personal de las áreas comparten sus usuarios y contraseñas. 2- No usan los correos institucionales. 3- El personal divulga la información confidencial. 4- EL tratamiento de la información no está catalogada por niveles de seguridad. 5- Los equipos estaciones de trabajo son usados por diversos usuarios.	- Concientizar al personal que su usuario y contraseña es única e intransferible. - Concientizar sobre el uso de los correos institucionales. - Crear un catálogo de niveles de seguridad para el tratamiento de la información.

PLAN DE ACIONES PREVENTIVA - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
No existe un plan de continuidad de negocio	1- Poca importancia de la organización. 2- No tienen plan de contingencia para los activos de información. 3- Las jefatura no se responsabilizan de los activos de información. 4- No hay personal asignado a los activos de información responsable de su bienestar. 5- No hay asesoramiento para un plan de continuidad de negocio.	- Difundir la Misión y Visión dela comandancia al personal delas áreas. - Elaborar un plan de contingencia para los activos de información. - Concientizar a las jefaturas sobre la responsabilidad que deben tener sobre los activos de información.

Tabla 38: Plan de Acciones Preventivas

Fuente: Elaborado por los Autores

Después de identificar 5 posibles causas para cada riesgo, se pudo analizar todas las causas, analizarlas y desarrollas, lo cual nos da una lista de Acciones Preventivas, esto es para adelantarnos al suceso de los riesgos para mitigar el riesgo.

PLAN DE ACIONES CORRECTIVAS - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
No existen políticas de seguridad	1- No se tiene claro la importancia de seguridad de información en las áreas SIMTRAC Y COMPAS SARSAT 2- No hay registro histórico de políticas de seguridad de información. 3- El personal trabaja por experiencia, sin alinearse a normas. 4- En la Comandancia se trabaja por "obligaciones". 5- En la Comandancia trabaja por órdenes jerárquico.	- Asignar a la urgencia presentada una política de seguridad inmediata. - Registrar en ese momento el incidente ocurrido.
No hay un responsable de las áreas vulnerables	1- No hay un organigrama de personal asociado a sus responsabilidades de seguridad de información. 2- No se tiene conocimiento a quien reportar incidencias y clasificarlas. 3- Hay mucha rotación de personal en las áreas SIMTRAC Y COMPAS SARSAT. 4- No hay delegación de personal sobre activos de información vulnerables. 5- Los jefe de área no quieren hacerse responsables sobre una incidencia mayor o desastre.	- Responsabilizar al personal en el momento del incidente. - En el momento del incidente se prioriza las áreas vulnerables.
No hay acuerdos de confidencialidad internas	1- No existen los acuerdos para la seguridad de información. 2- El personal Oficial encargado de las áreas no se responsabiliza de la seguridad de los activos de información. 3- Poco interés en la información confidencial asignada a los usuarios. 4- Se comparte la información sin ningún medio de confidencialidad. 5- Los acuerdos de confidencialidad con terceros no se les hace un seguimiento.	- Realizar una investigación para realizar las sanciones correspondientes. - Responsabilizar a los jefes de área cuando ocurre un incidente.
No hay seguridad para los activos de información	1- No hay un control de inventario de activos de información. 2- No existen responsabilidad asignada de los activos de información.	- Listar los activos de información vulnerados en el incidente. - Responsabilizar al personal de los activos de

PLAN DE ACIONES CORRECTIVAS - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
	3- La adquisición de un activo de información no está evaluado y no se encuentra en los inventarios. 4- El dado de baja de un activo de información es interno no llega a su destino de desuso. 5- La compra de un activo de información es adquirida por necesidad propia	información en el momento del incidente.
No están delimitados los roles del personal	1- Las funciones internas del personal no contemplan la seguridad de los activos de información. 2- El personal se limita a sus funciones internas. 3- Las jefaturas no promueven la seguridad de los activos de información. 4- EL personal no transmite sus conocimientos al delegar funciones en sus traslados de áreas. 5- La información de sus trabajos no es tratada con la seguridad requerida de acuerdo a sus funciones.	- Asignar tareas o roles al personal que contemplen la seguridad de los activos de información en el momento del incidente. - Concientizar al personal que transmita el total de los conocimientos necesario en el momento de cambio de personal.
No hay seguridad en la red	1- Los dispositivos de red no tienen una normativa de seguridad de la información. 2- No hay un inventario de dispositivita de red. 3- No hay homogeneidad en los dispositivos de red. 4- El cableado estructurado no está normalizado. 5- No hay un Firewall que separe la parte privada de la organización de la pública.	- Aislar la red pública de la red privada. - Listar los dispositivos de red en el momento del incidente. - Utilizar los Firewall secundarios de los sistemas operativos en el momento del incidente.
No se toman en cuenta las políticas de acceso a las áreas vulnerables	1- No hay interés por parte del personal sobre las políticas de acceso a las áreas vulnerables. 2- No hay un repositorio de datos para la documentación que permita el acceso a los usuarios por perfiles. 3- En las áreas no existe seguridad física por lo que se encuentran vulnerables. 4- No hay un registro de control de acceso al data center. 5- Existe confianza excesiva con los proveedores.	- Asignar responsabilidad de acceso a las áreas vulnerables en el momento del incidente. - Listar digitalmente o físicamente la documentación vulnerable. - Listar el acceso al data center. - Limitar acceso a las áreas en el momento del incidente.
No hay un control de usuarios	1- Los sistemas carecen de un control de usuarios por perfiles de seguridad. 2- La asignación de acceso a los sistemas no tiene un registro.	- Listar al personal en el momento del incidente. - Limitar el acceso a los sistemas vulnerables. - Asignar las funciones necesarias en el momento

PLAN DE ACIONES CORRECTIVAS - 5 ¿POR QUÉ?		
Riesgo a Controlar	**¿POR QUÉ?**	**Acciones**
	3- En la arquitectura de los servidores no hay un dominio que administre a los usuarios. 4- Los usuarios permiten el acceso al área a personal ajeno. 5- Los usuarios no tienen conocimiento de sus funciones asignadas.	del incidente.
Fuga de información	1- El personal de las áreas comparten sus usuarios y contraseñas. 2- No usan los correos institucionales. 3- El personal divulga la información confidencial. 4- EL tratamiento de la información no está catalogada por niveles de seguridad. 5- Los equipos estaciones de trabajo son usados por diversos usuarios.	- Listar al personal en el momento del incidente. - Limitar el acceso a los sistemas vulnerables. - Dar niveles a la información vulnerable en el momento del incidente. - Limitar el acceso a las estaciones de trabajo sensibles a la información.
No existe un plan de continuidad de negocio	1- Poca importancia de la organización. 2- No tienen plan de contingencia para los activos de información. 3- Las jefatura no se responsabilizan de los activos de información. 4- No hay personal asignado a los activos de información responsable de su bienestar. 5- No hay asesoramiento para un plan de continuidad de negocio.	- Listar tareas y actividades para continuar con las operaciones cotidianas. - Responsabilizar a las jefaturas de los activos de información vulnerables.

Tabla 39: Plan De Acciones Correctivas

Fuente: Elaborado por los Autores

Después de identificar 5 posibles causas para cada riesgo, se pudo analizar todas las causas, analizarlas y desarrollas, lo cual nos da una lista de Acciones Correctivas, para corregir en el instante que aparezcan para eliminar la causa raíz del riesgo.

CAPÍTULO IV: PRUEBAS Y RESULTADOS

4.1 ANÁLISIS SITUACIONAL DE LOS ACTIVOS DE INFORMACIÓN

Las siguientes ilustraciones muestran el análisis situacional del inventario de los activos de información al 100% de las áreas del SIMTRAC y del COSPAS SARSAT para el Plan del SGSI.

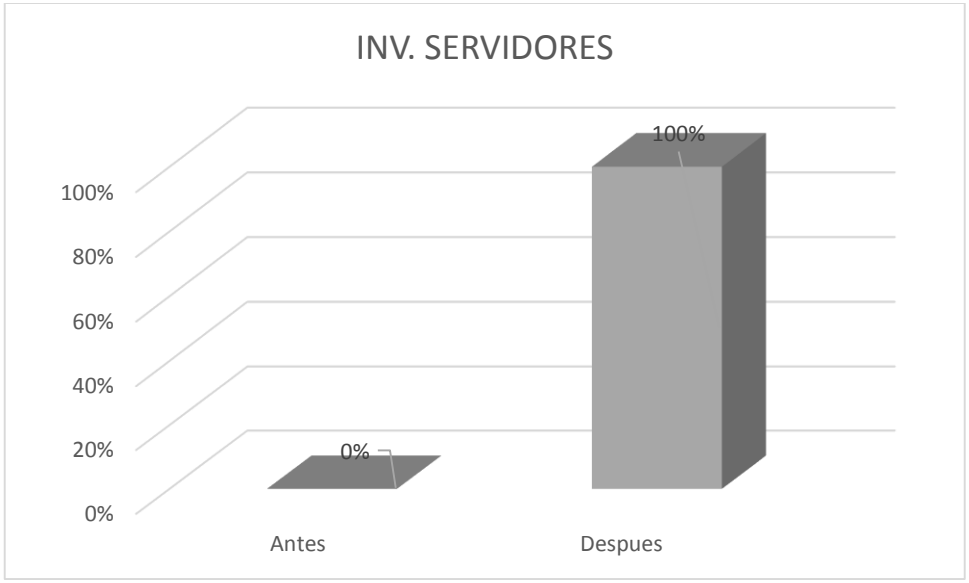

Ilustración 24: Inventario de Servidores

FUENTE: Elaborado por los Autores

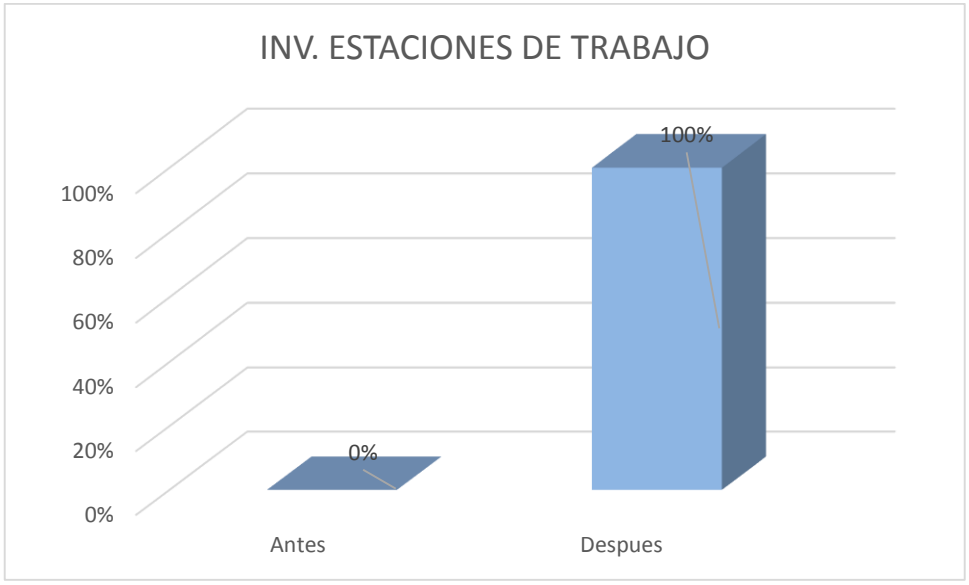

Ilustración 25: Inventario de Estaciones de Trabajo

FUENTE: Elaborado por los Autores

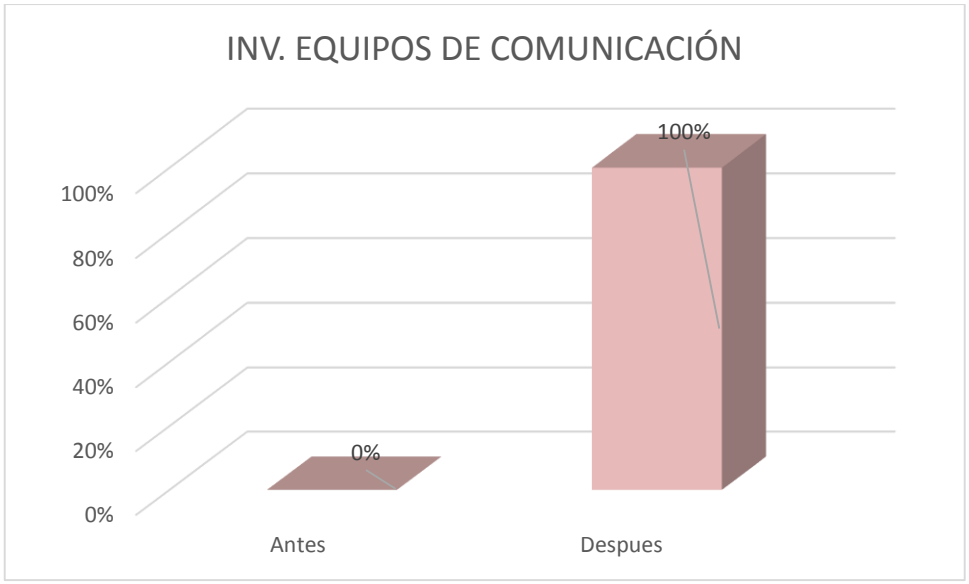

Ilustración 26: Inventario de Equipos de Comunicación

FUENTE: Elaborado por los Autores

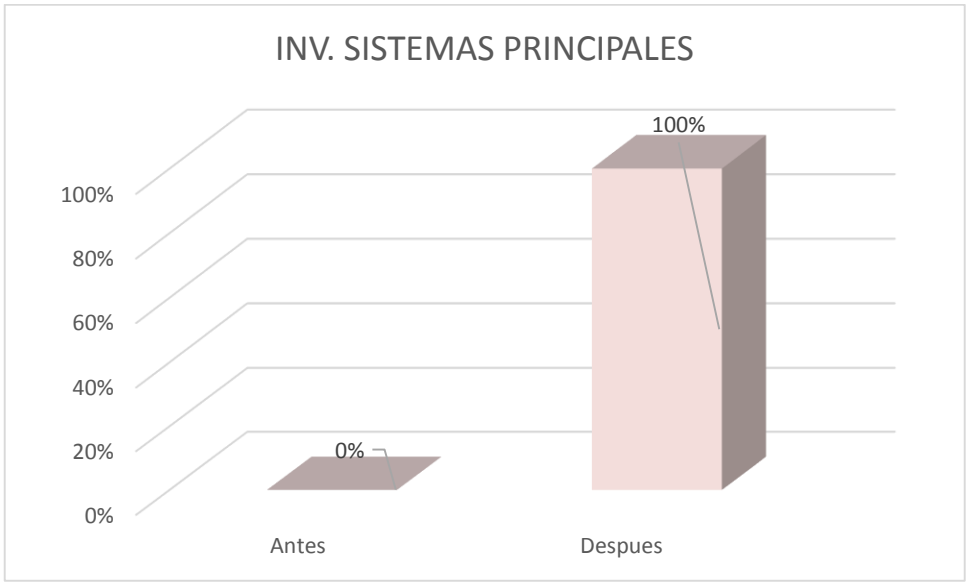

Ilustración 27: Inventario de Sistemas Principales

FUENTE: Elaborado por los Autores

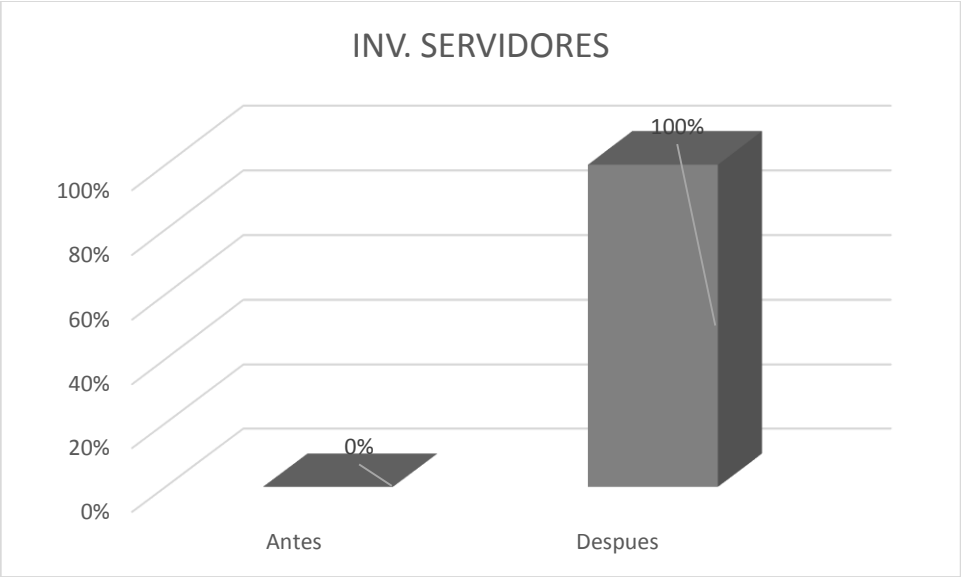

Ilustración 28: Inventario de Servidores

FUENTE: Elaborado por los Autores

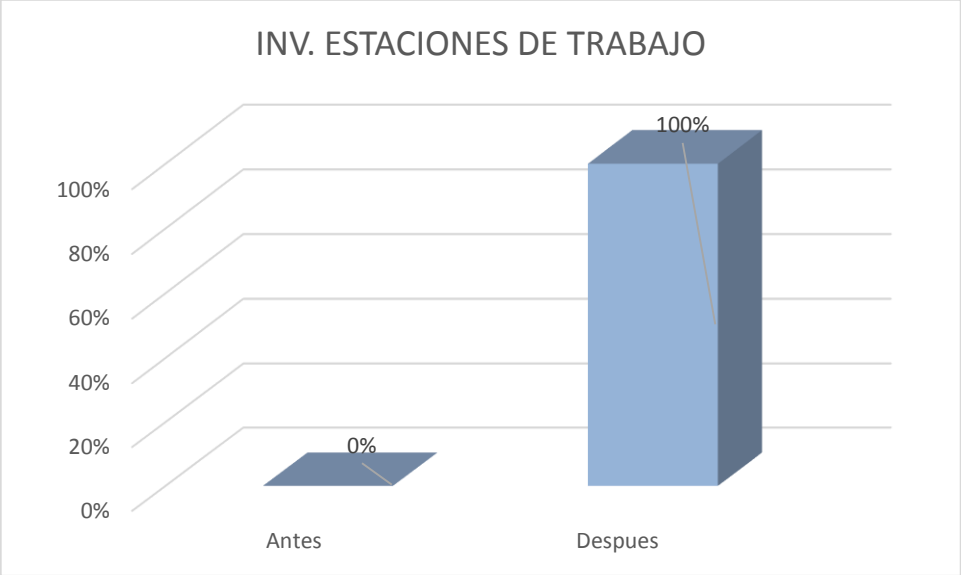

Ilustración 29: Inventario de Estaciones de Trabajo

FUENTE: Elaborado por los Autores

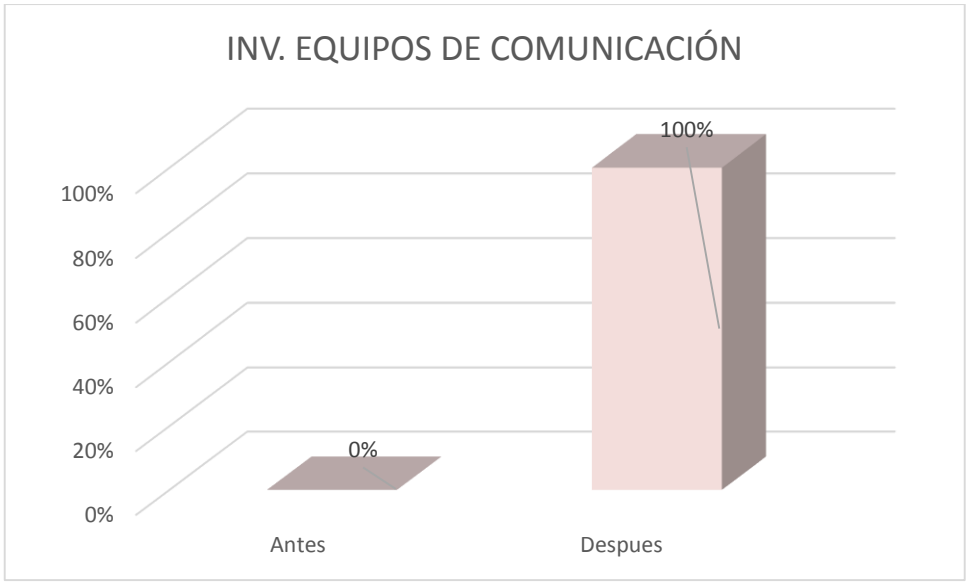

Ilustración 30: Inventario de Equipos de Comunicación

FUENTE: Elaborado por los Autores

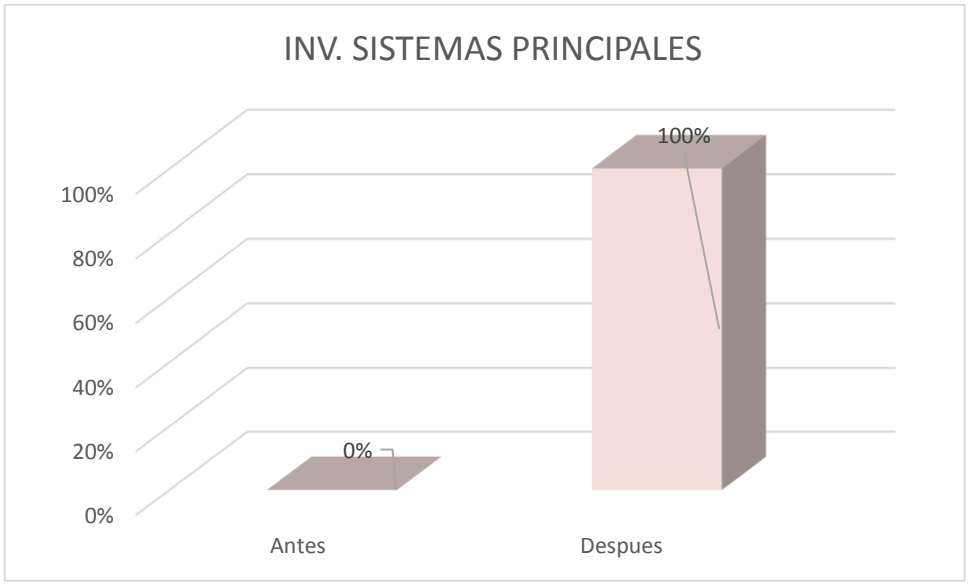

Ilustración 31: Inventario de Sistemas Principales

FUENTE: Elaborado por los Autores

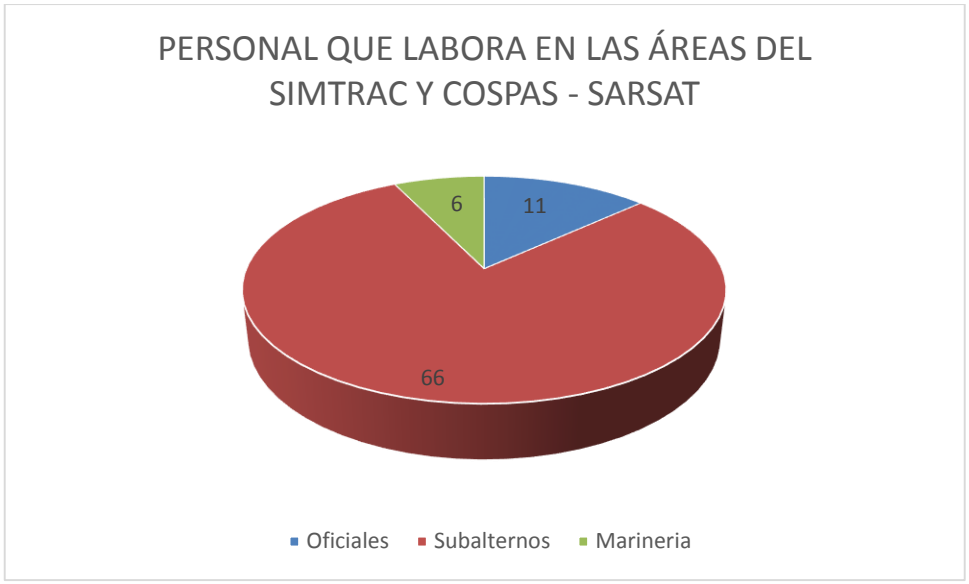

Ilustración 32: Personal de las Áreas SIMTRA y COSPAS SARSAT

FUENTE: Elaborado por los Autores

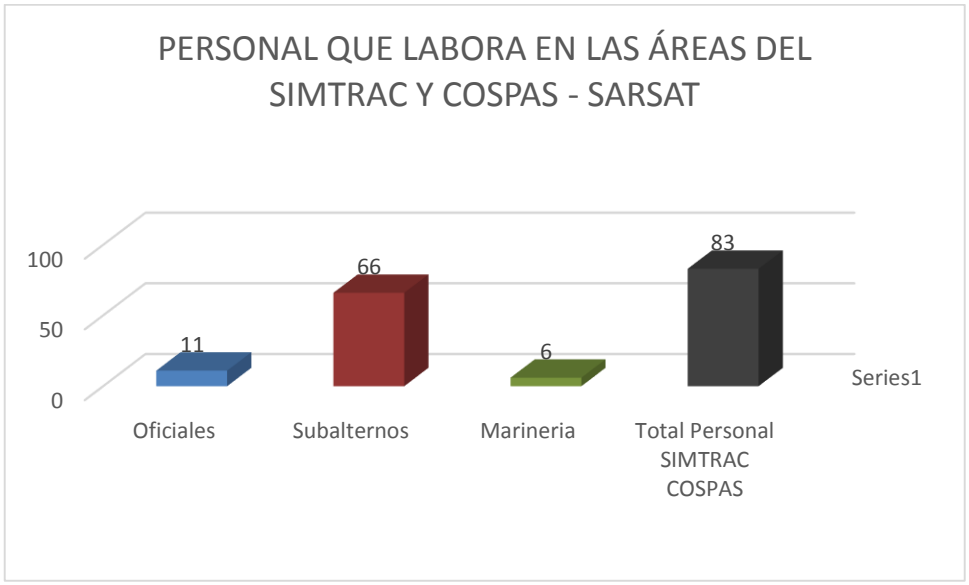

Ilustración 33: Total de Personal de las Áreas SIMTRA y COSPAS SARSAT

FUENTE: Elaborado por los Autores

4.2 ANÁLISIS DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN.

Teniendo el Análisis de Situacional se logró identificar los riesgos de los activos de información y asociarlos a algunas de las clausulas, objetivos de control y controles de la NTP mostrados en la tabla 40.

Luego se realizó el análisis de riesgo identificando la confidencialidad, integridad y disponibilidad al 100%; mostrando así el impacto de los riesgos en las áreas del SIMTRAC y del COSPAS SARSAT en la tabla 41 – cuarenta y uno - y en la ilustración 34 – treinta y cuatro-.

Identificación De Los Riesgos Vs NTP-ISO/IEC 27001:2008

NÚM.	RIESGOS	NTP ISO/IEC 27001:2008
1	NO HAY SEGURIDAD PARA LOS ACTIVOS	7.1.1; 7.1.2; 10.3.1
2	NO HAY ACUERDO DE CONFIDENCIALIDAD INTERNA	6.1.5
3	NO HAY UN RESPONSABLE DE LAS ÁREAS VULNERABLES	6.1.3; 6.1.5
4	NO EXISTEN DOCUMENTOS DE SEGURIDAD	6.1.3; 6.1.5
5	NO EXISTE UN PLAN DE CONTINUIDAD DE NEGOCIO	14.1.2
6	NO HAY SEGURIDAD EN LA RED	9.1.1; 10.6.1; 10.8.4
7	NO SE TOMAN EN CUENTA LAS POLÍTICAS DE ACCESO A LAS ÁREAS VULNERABLES	5.1; 11.1.1; 11.2.1
8	NO HAY UN CONTROL DE USUARIOS	5.1; 11.1.1; 11.2.1

NÚM.	RIESGOS	NTP ISO/IEC 27001:2008
9	FUGA DE INFORMACIÓN	12.5.4
10	NO ESTAN DELIMITADOS LOS ROLES DEL PERSONAL	5.1.1; 8.1.1
11	NO EXISTEN POLÍTICAS DE SEGURIDAD	5.1.1; 8.1.1

Tabla 40: RIESGOS VS NTP/IEC 27001:2008

FUENTE: Elaborado por los Autores

Identificación del Impacto

INVENTARIO DE ACTIVOS DE INFORMACIÓN								
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D
Componentes del Servicio	Personal Destacado al Área	1; 2; 3; 8; 9; 10	Usuario	Jefe del Área	Pool de Operaciones	Alta	Alta	Alta
	Instalaciones físicas	1; 3; 5; 6; 11	Organización	Jefe de la Comandancia	Coordenadas de la Organización	Alta	Alta	Alta
	Sistemas Operativos	1; 5; 7; 8; 9; 11	Software	PDA	Oficinas	Alta	Alta	Alta
	Estaciones de Trabajo	1; 3; 5; 6; 7; 9; 10; 11	Hardware	PDA	Oficinas y Pool de Operaciones	Alta	Media	Alta
	Servidores	1; 3; 5; 6; 7; 8; 11	Hardware	Administrador de Servidores	Salas de Servidores	Alta	Alta	Alta
	Sistemas de Información Servidores	1; 2; 5; 6; 7; 8; 9; 11	Software	Administrador de Servidores	Salas de Servidores	Alta	Alta	Alta
	Imagen Organizacional	2; 4; 5; 9	Organización	Relaciones Publicas	Área de Relaciones Publicas	Alta	Alta	Media
	Información de Embarcaciones	2; 4; 5; 9	Información	Técnico a Cargo	Base de Datos	Alta	Alta	Alta

INVENTARIO DE ACTIVOS DE INFORMACIÓN									
COMPONETES DEL SERVICIO	IDENTIFICACIÓN DE ACTIVO	RIESGOS	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D	
	Informe de Operaciones	2; 4; 5; 9	Información	Oficial a Cargo	Estación de Trabajo	Alta	Alta	Alta	
	Equipos de Comunicación	1; 3; 5; 6; 7; 9; 10; 11	Hardware y Red	Jefe de Electrónica	Área de Electrónica	Alta	Alta	Alta	
					TOTAL	100	99	99	

Tabla 41: Identificación del Impacto

FUENTE: Elaborado por los Autores

Leyenda

C:	Confidencialidad
I:	Integridad
D:	Disponibilidad

Tabla 42: Leyenda Inventario de Activos de Información

Fuente: Elaborado por los Autores

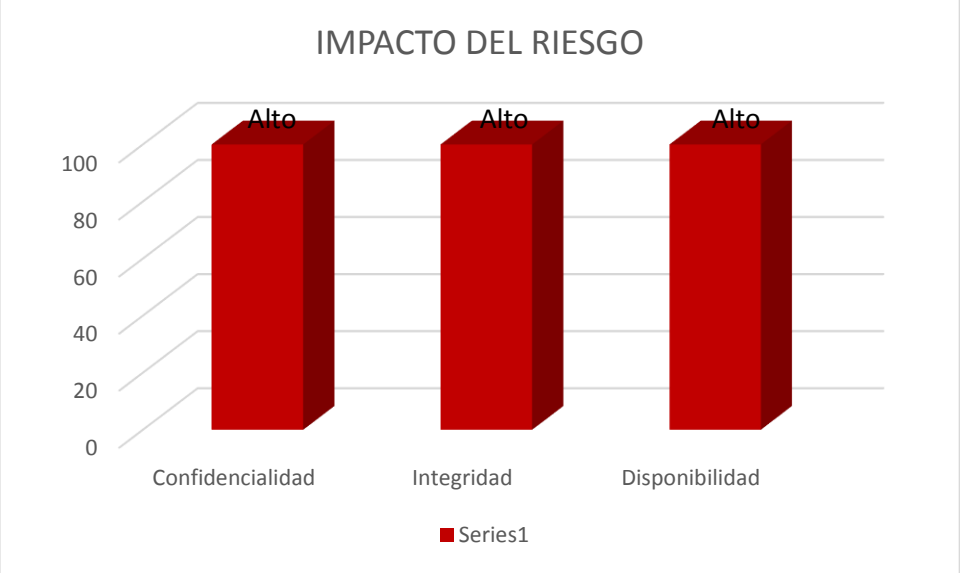

Ilustración 34: Impacto del Riesgo

FUENTE: Elaborado por los Autores

4.3 EVALUACIÓN SELECTIVA DE LOS ACTIVOS DE INFORMACIÓN.

Teniendo el análisis de riesgos se logró identificar los activos de información de mayor vulnerabilidad mostrado en la tabla 41 – cuarenta y uno -; para identificar estos activos se utilizó el campo de la Gravedad con el nivel 5 – cinco – el más alto.

En la tabla 43 – cuarenta y tres – se muestra un total de 31 – treinta y uno - activos de información, de los cuales 15 – quince - de ellos con una gravedad nivel 5 – cinco -; lo que determina un 48% del total de activos vulnerables.

Análisis y Evaluación del Riesgo

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)						
Activos de Información	**Código de Numeración**	**Modo de Fallo**	**Frecuencia F**	**Gravedad G**	**Detectabilidad D**	**IPR**
Personal Destacado al Área	1.1	Falta de Recurso Humano	2	3	3	18
	1.2	Falta de compromiso para el llenado de las bitácoras	3	4	1	12
	1.3	Falta de Capacitación Recurso Humano	4	3	2	24
	1.4	Divulgación de la Información Confidencial	2	5	3	30
Instalaciones Físicas	2.1	Inadecuada Infraestructura de red	5	5	2	50
	2.2	Inadecuada Infraestructura para Sala de Servidores	5	5	1	25
Sistemas Operativos	3.1	SO sin Licencia	4	4	2	32
	3.2	Versiones pasadas de los SO	3	3	2	18
	3.3	Pérdida de la Información por falla de Servidor	5	5	2	50
	3.4	Sin Soporte para SO Libre	5	5	1	25

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)						
Activos de Información	**Código de Numeración**	**Modo de Fallo**	**Frecuencia F**	**Gravedad G**	**Detectabilidad D**	**IPR**
Estaciones de Trabajo	4.1	Estaciones de Trabajo Obsoletas	3	4	1	12
	4.2	Estaciones de Trabajo sin homogeneidad	4	4	2	32
	4.3	Estaciones de trabajo sin mantenimiento regular	3	3	2	18
Servidores	5.1	Lentitud en la Capacidad de Procesamiento	5	5	2	50
	5.2	Poco Espacio de Almacenamiento	5	5	2	50
	5.3	No se cuenta con un Mantenimiento de servidores	4	4	2	32
Sistemas de Información Servidores	6.1	Versiones pasadas de los SO	3	4	1	12
	6.2	Sin Soporte para Sistema Servidor de Correo Libre	5	5	2	50
	6.3	Sin Soporte para Sistema Servidor de la Pagina Web Libre	5	5	3	75
	6.4	Falla en las Transacciones con la Base de Datos	5	5	3	75

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)						
Activos de Información	**Código de Numeración**	**Modo de Fallo**	**Frecuencia F**	**Gravedad G**	**Detectabilidad D**	**IPR**
Imagen Organizacional	7.1	Pérdida de Status a nivel Organizacional	4	3	4	48
Información de Embarcaciones	8.1	Información Tardía de las Embarcaciones	4	4	4	64
	8.2	Datos Erróneos del Monitoreo de las Embarcaciones	3	5	4	60
Informe de Operaciones	9.1	Carencia de Automatización de las Bitácoras	5	5	1	25
	9.2	Datos Erróneos en las Bitácoras	4	4	3	48
	9.3	Pérdidas de las Bitácoras	2	4	4	32
Equipos de Comunicación	10.1	Equipos Obsoletos	3	4	2	24
	10.2	Falta de Mantenimiento de los Equipos de Comunicación	5	4	2	40
	10.3	Líneas de Comunicación sin Protección	4	5	3	60
	10.4	Arquitectura Inadecuada de la Red	4	5	2	40
	10.5	Conexiones de Red Pública sin Protección	5	5	2	50

Tabla 43: Matriz AMFE (Análisis Modal De Sus Fallas Y Sus Efectos)

FUENTE: Elaborado por los Autores

Ilustración 35: Existencia de 31 Modo de Fallos

FUENTE: Elaborado por los Autores

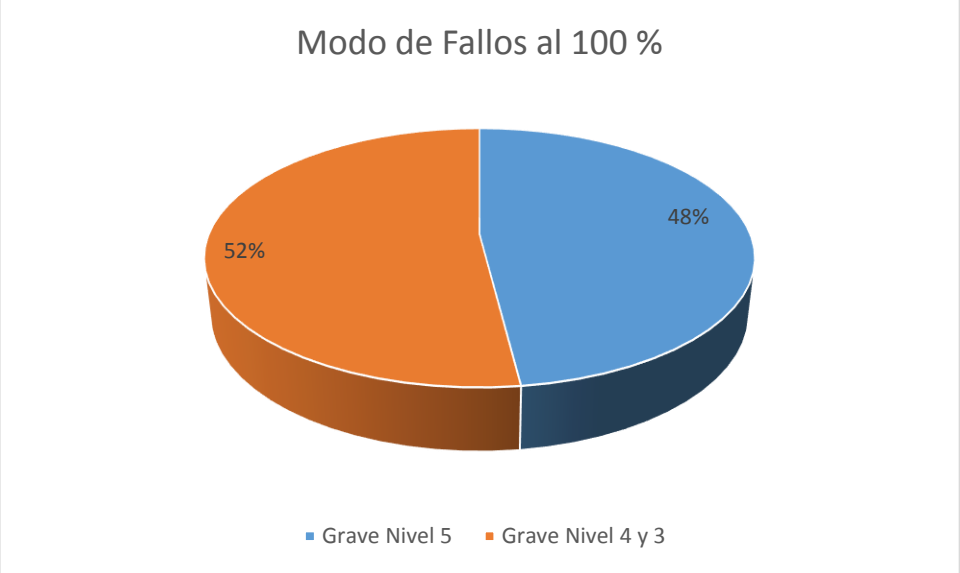

Ilustración 36: Modo de Fallos al 100%

FUENTE: Elaborado por los Autores

4.4 ANÁLISIS COMPARATIVO.

Con la evaluación selectiva se identificó los riesgos que se asociaran a la norma que ayudaran a minimizar los riesgos; para esto se utilizara un 24% de controles de la norma entre las recomendaciones y el análisis que se realizó de los riesgos.

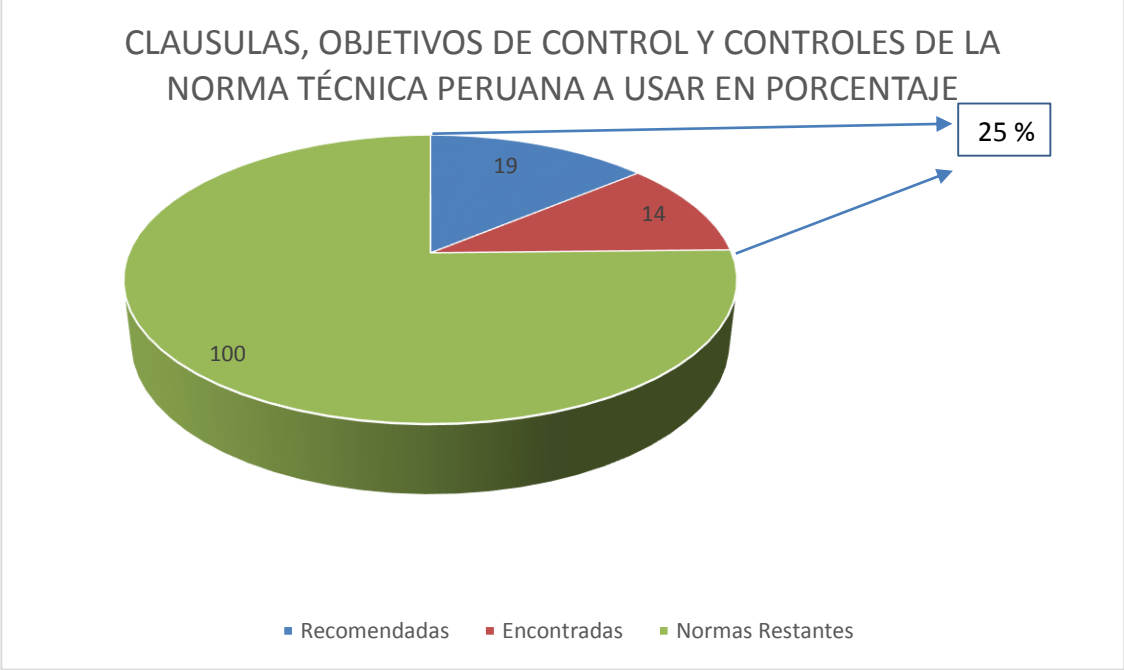

Ilustración 37: Cláusulas, Objetivos de Control y Controles de la Norma Técnica Peruana a usar, en porcentaje

FUENTE: Elaborado por los Autores

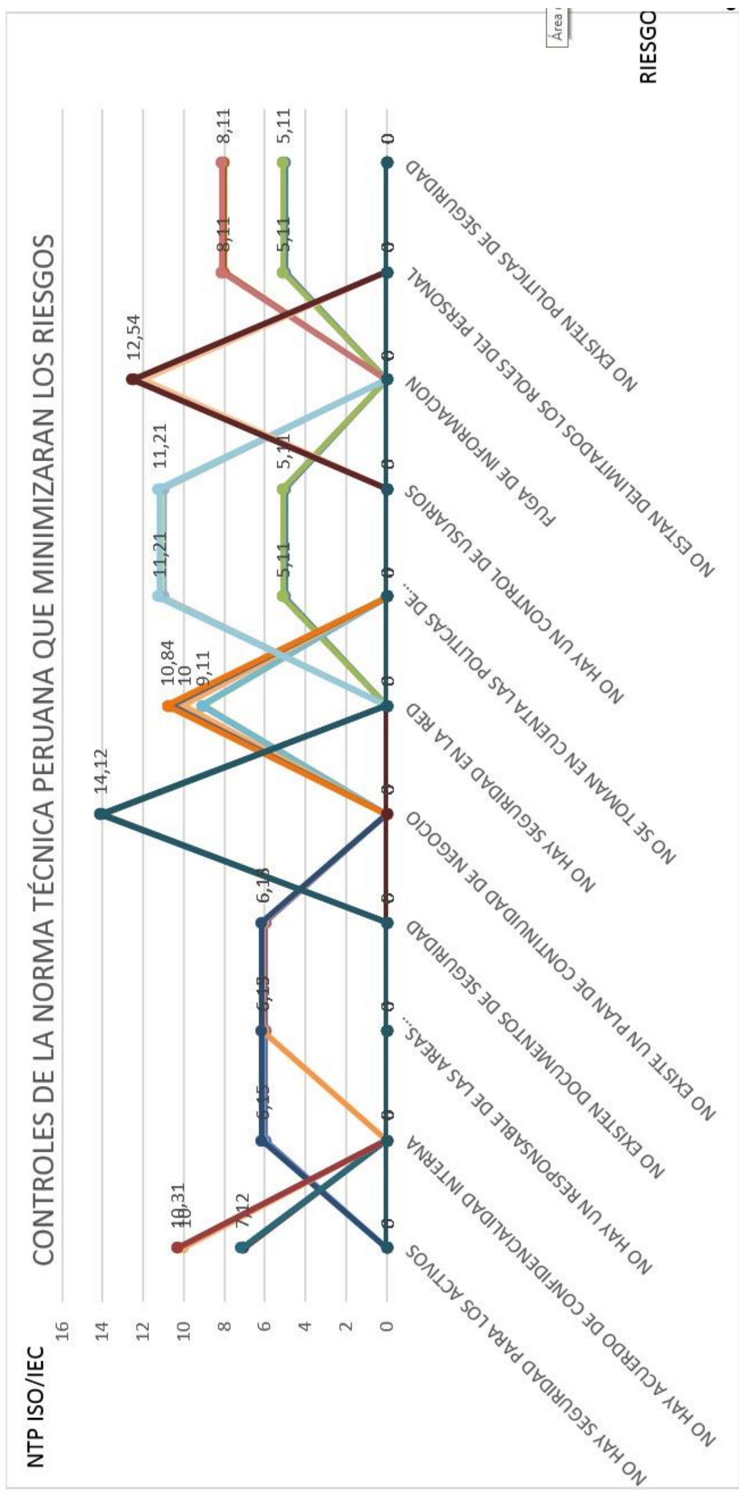

Ilustración 38: Controles de la Norma Técnica Peruana que minimizaran los riesgos

FUENTE: Elaborado por los Autores

4.5 MITIGACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN.

Luego de implantar los controles y de asociarlos a los riesgos de nivel 5 de gravedad se logró que el IPR – Índice de Probabilidad de Riesgos - se redujera en un 73%.

Matriz AMFE (Análisis Modal de sus Fallas y sus Efectos)

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)										
Activos de Información	RIESGOS	Modo de Fallo	Frecuencia F		Gravedad G		Detectabilidad D		IPR	
			Antes	Después	Antes	Después	Antes	Después	Antes	Después
Personal Destacado al Área	1; 2; 3; 8; 9; 10	Divulgación de la Información Confidencial	2	1	5	3	3	2	30	6
Instalaciones Físicas	1; 3; 5; 6; 11	Inadecuada Infraestructura de red	5	3	5	3	2	2	50	18
		Inadecuada Infraestructura para Sala de Servidores	5	2	5	2	1	1	25	4
Sistemas Operativos	1; 5; 7; 8; 9; 11	Perdida de la Información por falla de Servidor	5	3	5	2	2	2	50	12
		Sin Soporte para SO Libre	5	5	5	4	1	1	25	20
Servidores	1; 3; 5; 6; 7; 8; 11	Lentitud en la Capacidad de Procesamiento	5	3	5	3	2	2	50	18
		Poco Espacio de Almacenamiento	5	4	5	2	2	2	50	16
Sistemas de Información Servidores	1; 2; 5; 6; 7; 8; 9; 11	Sin Soporte para Sistema Servidor de Correo Libre	5	3	5	3	2	2	50	18

MATRIZ AMFE (ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS)													
Activos de Información	RIESGOS	Modo de Fallo	Frecuencia F		Gravedad G		Detectabilidad D		IPR				
			Antes	Después	Antes	Después	Antes	Después	Antes	Después			
		Sin Soporte para Sistema Servidor de la Pagina Web Libre	5	3	5	3	3	2	75	18			
		Falla en las Transacciones con la Base de Datos	5	3	5	2	3	2	75	12			
Información de Embarcaciones	2; 4; 5; 9	Datos Erróneos del Monitoreo de las Embarcaciones	3	3	5	2	4	3	60	18			
Informe de Operaciones	2; 4; 5; 9	Carencia de Automatización de las Bitácoras	5	3	5	2	1	1	25	6			
Equipos de Comunicación	1; 3; 5; 6; 7; 9; 10; 11	Líneas de Comunicación sin Protección	4	2	5	2	3	2	60	8			
		Arquitectura Inadecuada de la Red	4	4	5	2	2	2	40	16			
		Conexiones de Red Publica sin Protección	5	3	5	2	2	1	50	6			
		Totales	68	45	75	37	33	27	715	196			

Tabla 44: Matriz AMFE (Análisis Modal de sus Fallas y sus Efectos) Antes y Después

FUENTE: Elaborado por los Autores

Índice de Prioridad de Riesgos Antes y Después

Activos de Información	Modo de Fallo	IPR	
		Antes	Después
Personal Destacado al Área	Divulgación de la Información Confidencial	30	6
Instalaciones Físicas	Inadecuada Infraestructura de red	50	18
	Inadecuada Infraestructura para Sala de Servidores	25	4
Sistemas Operativos	Pérdida de la Información por falla de Servidor	50	12
	Sin Soporte para SO Libre	25	20
Servidores	Lentitud en la Capacidad de Procesamiento	50	18
	Poco Espacio de Almacenamiento	50	16
Sistemas de Información Servidores	Sin Soporte para Sistema Servidor de Correo Libre	50	18
	Sin Soporte para Sistema Servidor de la Pagina Web Libre	75	18
	Falla en las Transacciones con la Base de Datos	75	12
Información de Embarcaciones	Datos Erróneos del Monitoreo de las Embarcaciones	60	18
Informe de Operaciones	Carencia de Automatización de las Bitácoras	25	6
Equipos de Comunicación	Líneas de Comunicación sin Protección	60	8
	Arquitectura Inadecuada de la Red	40	16

Activos de Información	Modo de Fallo	IPR	
		Antes	Después
	Conexiones de Red Pública sin Protección	50	6
	Total	715	196

Tabla 45: Minimización de los Riesgos IPR

FUENTE: Elaborado por los Autores

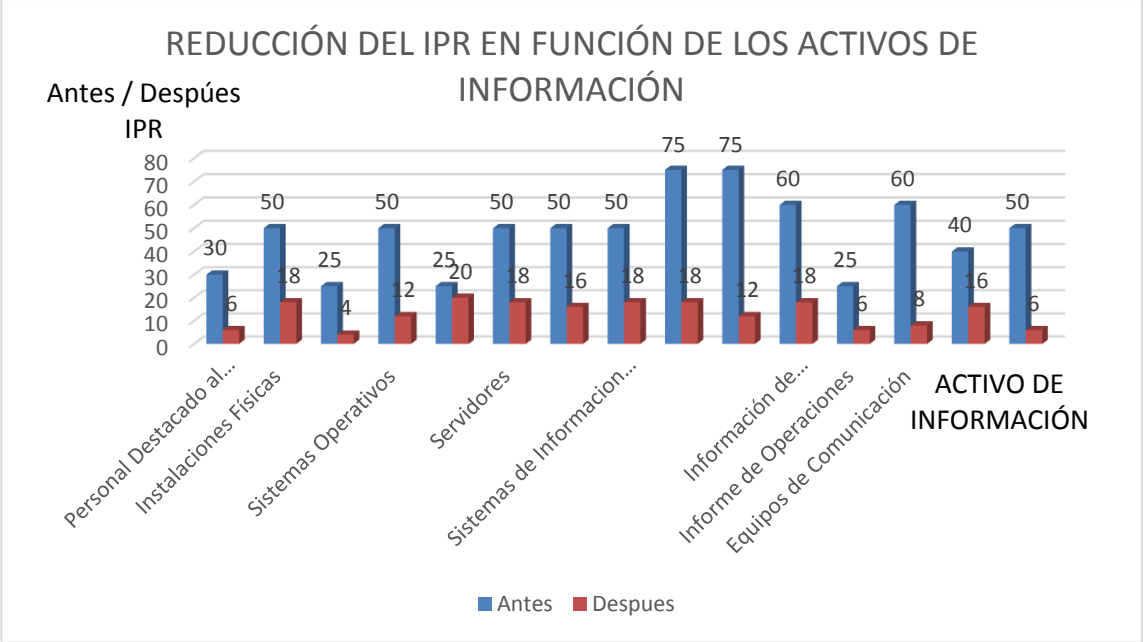

Ilustración 39: Reducción del IPR en función de los Activos de Información

FUENTE: Elaborado por los Autores

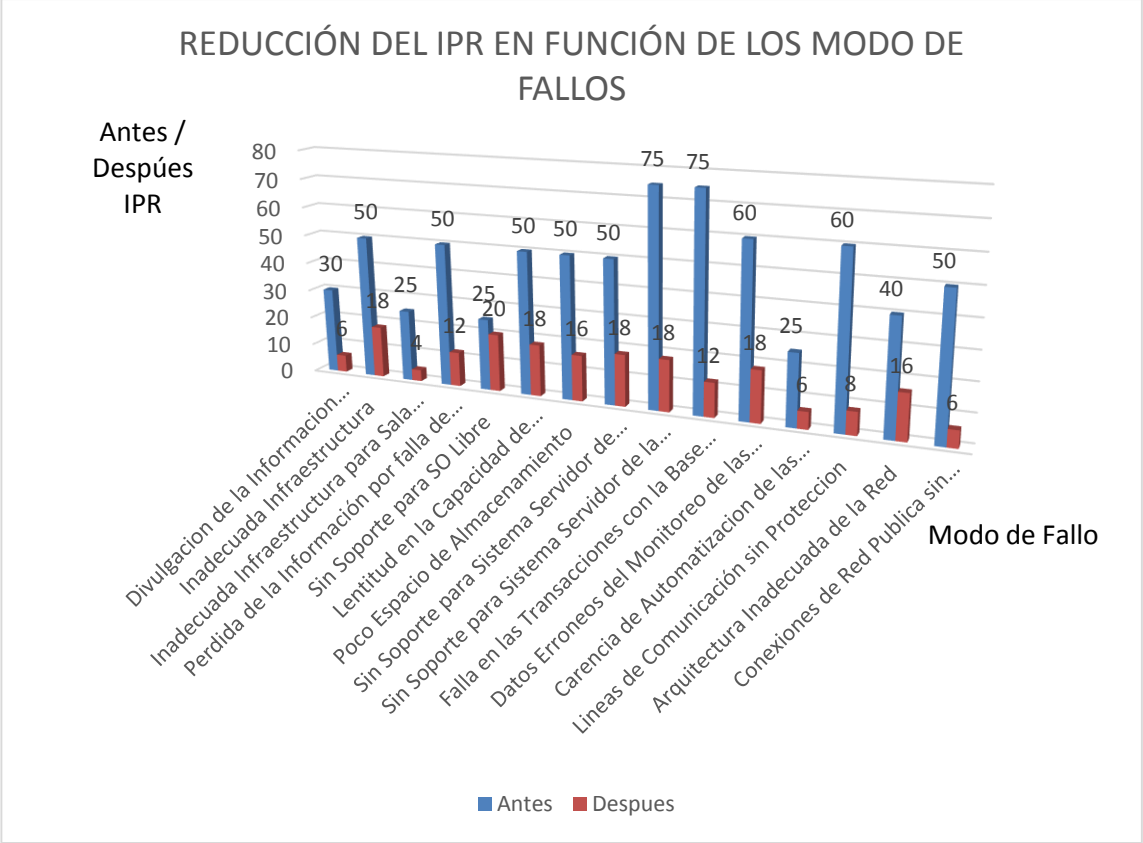

Ilustración 40: Reducción del IPR en Función del Modo de Fallo

FUENTE: Elaborado por los Autores

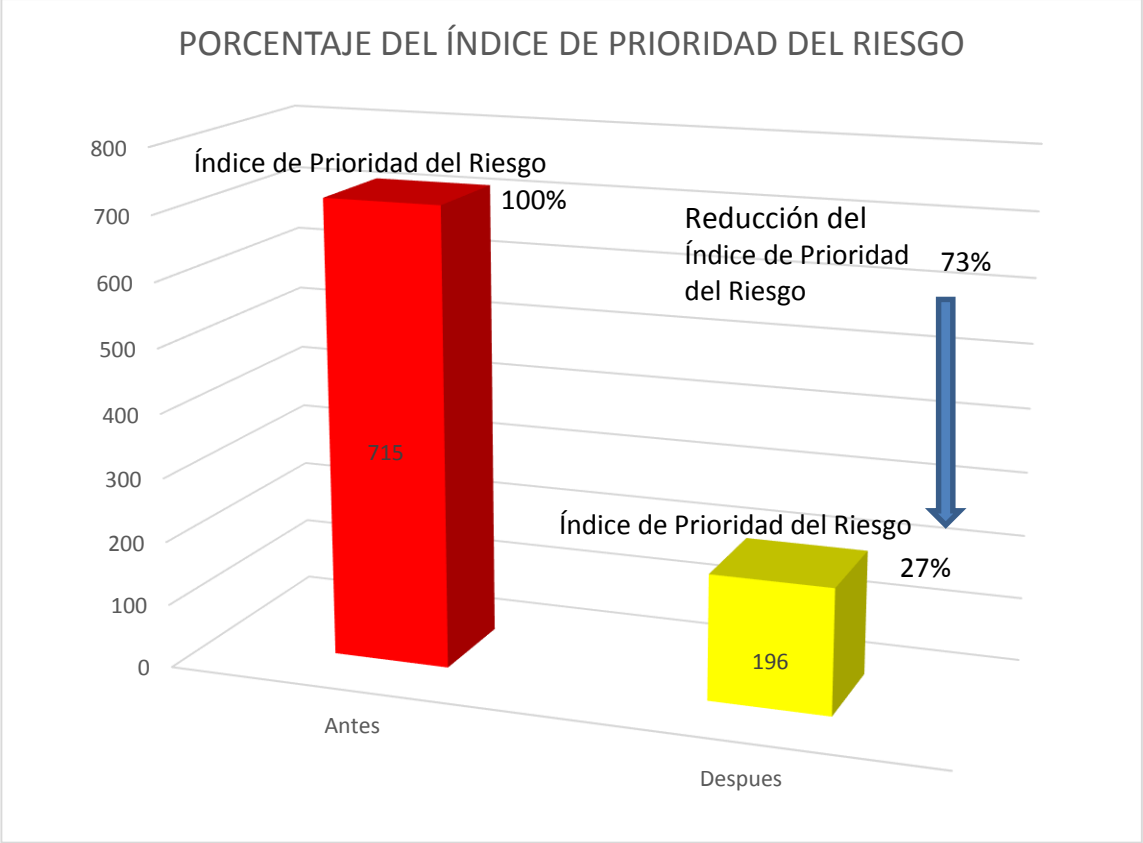

Ilustración 41: Porcentaje del Índice de Prioridad del Riesgo

FUENTE: Elaborado por los Autores

4.6 SENSIBILIZACIÓN Y COMPROMISO DEL PERSONAL DE LA COMANDANCIA.

Bajo el Plan de Verificación del Plan de SGSI en la tabla 46 – cuarenta seis- se obtuvo un 80% de compromiso de los Oficiales, Subalternos y Personal de Marinería y de igual forma se obtuvo un 80% de sensibilización del personal.

Ilustración 42: Logro Oficiales Responsables

FUENTE: Elaborado por los Autores

Plan de Verificación del Plan de Sistema de Gestión de Seguridad de la Información

PLAN DE VERIFICACIÓN DEL PLAN DE SGSI					
Riesgo a Controlar	Objetivo de Control	Responsable	Indicador Formula	Meta	Logro
No existen políticas de seguridad	Aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.	PAREDES BLANCO, CESAR	núm. personal que conoce las políticas S.I. / total de personal de las áreas	80	70
No hay un responsable de las áreas vulnerables	Gestionar la seguridad de la información dentro de la organización.	PAREDES BLANCO, CESAR	núm. usuarios que cumplen las políticas S.I. / total de usuarios de las áreas	100	70
No hay acuerdos de confidencialidad internas		PAREDES BLANCO, CESAR	núm. personal que firma acuerdos / total de acuerdos	100	80
No hay seguridad para los activos	Mantener una protección adecuada sobre los activos de la organización. Todos los activos deben ser considerados y tener un propietario asignado.	SANTA ENRIQUE MARIA OLIVA	núm. de activos vulnerables / total de activos	100	100
		SANTA ENRIQUE MARIA OLIVA	núm. de activos sin seguridad / total de activos	100	100
		SANTA ENRIQUE MARIA OLIVA	núm. de activos con propietarios / total de activos	100	70
No están delimitados los roles del personal	Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y entiendan sus roles, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones.	SEMINARIO SEMINARIO, LUIS	funciones realizadas por el usuario / total de usuarios	100	80
No hay seguridad en la red	Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.	SEMINARIO SEMINARIO, LUIS	equipos de TI autorizados / equipos de TI no autorizados	100	80
	Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones	SEMINARIO SEMINARIO, LUIS	mensajería spam actual / total de spam	100	60

PLAN DE VERIFICACIÓN DEL PLAN DE SGSI					
Riesgo a Controlar	Objetivo de Control	Responsable	Indicador Formula	Meta	Logro
	Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.	SEMINARIO SEMINARIO, LUIS	núm. de visitantes no autorizados / total de visitantes	100	70
No se toman en cuenta las políticas de acceso a las áreas vulnerables	Controlar los accesos a la información.	SEMINARIO SEMINARIO, LUIS	núm. de ingreso del personal autorizado / el total de personas ingresantes	100	100
No hay un control de usuarios	Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.	LUN PUN TORRES VICTOR	acceso usuario en su guardia / tiempo total de acceso por día	100	100
Fuga de información	Mantener la seguridad del software de aplicación y la información. Se deberían controlar estrictamente los entornos del proyecto y de soporte.	LUN PUN TORRES VICTOR	nivel de seguridad usado / núm. total de información	100	100
No existe un plan de continuidad de negocio	Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.	LUN PUN TORRES VICTOR	núm. de incidentes / núm. total de incidentes	100	50
			TOTAL	1380	1130
			Porcentajes	100%	80%

Tabla 46: Plan de Verificación del Plan de SGSI

FUENTE: Elaborado por los Autores

CAPÍTULO V: DISCUSIÓN Y APLICACIONES

5.1 ANÁLISIS SITUACIONAL DE LOS ACTIVOS DE INFORMACIÓN

En el apartado 4.1 se visualiza en las ilustraciones el Análisis Situacional de los activos de información de las áreas COSPAS SARSAT y del SIMTRAC en la Comandancia de Operaciones Guardacostas; mostrándonos un inventario de los equipos de TI y un censo del personal oficial, subalterno y de marinería que labora en la Comandancia como entrada para el Plan de SGSI.

Como se muestra anteriormente no se tenía un inventario de TI ni un censo del personal orientado para la seguridad de la información.

En este trabajo se logró obtener el inventario de TI al 100% con el censo del personal que labora en las áreas antes mencionadas también al 100%.

5.2 ANÁLISIS DE RIESGO DE LOS ACTIVOS DE INFORMACIÓN

Realizado el análisis situacional en base al inventario y censo respectivo se logró conocer e identificar los riesgos; estos a su vez contrastando con las clausulas, objetivos de control y controles de la NTP-ISO/IEC 2700:2008 permitió que dichos estándares ayudaran a minimizar estos riesgos.

Valorizando cualitativamente la confidencialidad, integridad y disponibilidad de los activos de información en valor bajo, valor medio y valor alto; logramos obtener al 100% el impacto de los riesgos sobre los activos de información.

5.3 EVALUACIÓN SELECTIVA DE LOS ACTIVOS DE INFORMACIÓN

Con el análisis de riesgo anteriormente obtenido al 100% se logró valorizar cuantitativamente utilizando la herramienta AMFE las frecuencias con que ocurren los fallos de determinado riesgo; la gravedad del riesgo y la detectabilidad de ese fallo del riesgo; obteniendo una Evaluación Selectiva; con esto se determina un 48% del total de activos que son vulnerables.

5.4 ANÁLISIS COMPARATIVO

Con la evaluación selectiva de los activos de información con mayor riesgo se realizó el análisis comparativo entre dichos riesgos y las clausulas, objetivos de control y controles de la NTP-ISO/IEC 27001:2008 que ayudarán a la mitigación de estos riesgos.

En este análisis comparativo nos referimos a la utilización de un 38% de la NTP-ISO/IEC 27001:2008 con el fin de estandarizar y normalizar los riesgos de tal forma que nos permita minimizar los riesgos encontrados.

La ilustración 37 – treinta y siete – nos permite visualizar que clausulas, objetivos de control y controles se asocian a los riesgos para mitigarlos.

5.5 MITIGACIÓN DE RIESGOS DE LOS ACTIVOS DE INFORMACIÓN

En el apartado 11.5 se visualiza a los activos de información con sus riesgos asociados y cuantificados en 715 – setecientos quince – que significa el 100% del índice de prioridad de riesgos; posteriormente luego de implantar este trabajo se logró reducir estos riesgos a una cuantificación de 196 – ciento noventa y seis – que nos refiere un 27%; esto significa que se logró reducir los riesgos en un 73%.

5.6 SENSIBILIZACIÓN Y COMPROMISO DEL PERSONAL DE LA COMANDANCIA

Con la verificación del Plan de SGSI visualizamos que los indicadores lograron un 80% del total de las metas; esto significa que los oficiales responsables de cada área y de los riesgos a controlar se comprometieron en alcanzar la mitigación de estos riesgos ayudados de su personal subalterno; lo que nos hace suponer que hubo una sensibilización adecuada.

CONCLUSIONES

1. Se realizó al 100% el Análisis Situacional de los activos de información en las áreas COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas permitiendo conocer con que equipos de TI cuenta la comandancia.
2. Se realizó al 100% el Análisis de Riesgos de los activos de información focalizados en el Análisis Situacional, en las áreas COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas, mostrando así el impacto de los riesgos en dichas áreas.
3. De acuerdo a una Evaluación Selectiva de los activos de información se encontraron 48% de activos de información vulnerables.
4. Al realizar el Análisis Comparativo entre la Evaluación Selectiva y la NTP-ISO/IEC 27001:2008 se logra utilizar un 25% de controles de la NTP-ISO/IEC 27001:2008 para la elaboración del Plan de SGSI para la Comandancia de Operaciones Guardacostas.
5. En el análisis y diseño del Plan de SGSI se demostró que se minimizaron los riesgos, amenazas y vulnerabilidades en un 73% de los activos de información.
6. Se logró el compromiso de la plana superior de la comandancia y sensibilización del personal en un 80% en la Comandancia de Operaciones Guardacostas.

Se diseñó un plan de sistema de gestión de seguridad de la información para las áreas COSPAS-SARSAT y SIMTRAC de la Comandancia de Operaciones Guardacostas -COMOPERGUARD- basada en la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.– ver Anexo E -.

RECOMENDACIONES

1. Se considera importante, que tomando como base inicial esta Tesis, se establezcan y desarrollen para la Comandancia de Operaciones Guardacostas, los siguientes aspectos:

   Implantar el Plan de Sistema de Gestión de Seguridad de Información elaborado en esta tesis para dicha Comandancia, como una primera etapa y alternativa mientras la organización militar se prepara para llegar a la certificación internacional.

   Desarrollar la planificación y las actividades necesarias para obtener la certificación internacional ISO 27001 para la Comandancia.

2. Se sugiere la publicación y difusión de esta tesis, a toda la Comandancia de Operaciones Guardacostas, para que pueda ser utilizado en beneficio del mejoramiento de la seguridad de información, que es el objetivo principal de esta tesis.

3. Se sugiere incorporar a la estructura organizacional de la Comandancia de Operaciones Guardacostas, un departamento que trabaje de manera proactiva y reactiva en Sistemas de Gestión de Seguridad de Información.

4. Sugerimos usar esta tesis basada en nuestra investigación de la NTP-ISO/IEC 27001:2008 que con sus controles dará seguridad a los activos de información en cualquier organización y que nos servirá como base para futuros planes de seguridad.

FUENTES DE INFORMACIÓN

BIBLIOGRAFÍA

Alexander, A. G. (10 de 12 de 2006). Análisis del Riesgo y el Sistema de Gestión de Seguridad de Información: El Enfoque ISO 27001:2005.

Areitio, J. (2008). *Seguridad de la Información.* España: Learning Paraninfo S.A.

Bestratén M. Orriols, R. Y. (2010). *Análisis modal de fallos y efectos AMFE.* Madrid: Bestratén Belloví.

Boonen, B. y. (2007). *IT Governance based on CobiT 4.1 - A Management Guide.* USA: Van Haren.

commoncriteria. (2013). *commoncriteria*. Obtenido de http://www.commoncriteria.org/

Daltabuit, E. (2007). *Seguridad de Información.* Mexico: Editorial Limusa.

De Jong, A. (2007). *Foundations of IT Service Management Based on ITIL.* USA: Van Haren Publishing.

Díaz, L. J., Harari, C. V., & Venosa, L. P. (8 de 4 de 2003). Auditoría de Seguridad de Organizaciones, fortalezas y debilidades de la Norma ISO 17799.

ESAN. (20 de 04 de 2013). Control de Calidad, Limites de control. *Diplomado Six Sigma*. Lima, Peú.

ESPAÑOL, I. E. (2012). *ISO.* Obtenido de http://www.iso27000.es

García, C. J. (20 de 11 de 2013). METODOLOGÍA PARA ALINEAR LA ISO 27001 AL MODELO OPERATIVO DE UNA ENTIDAD ASEGURADORA: caso de estudio.

Getion-calidad. (2009). *ISO 27002:2005*. Obtenido de (Anterior ISO 17799:2005): http://www.gestion-calidad.com/iso-27002.html

Gómez Vieites, Á. (2006). *Enciclopedia de la Seguridad Informática.* Madrid, España: RA-MA EDITORIA.

Indecopi. (2014). *Inicio*. Obtenido de Indecopi: www.indecopi.gob.pe

Institute, I. G. (2010). *Leading the IT Governance Community.* Obtenido de http://www.itgi.org/

IRAM. (2014). *Instituo Argentino de Normalización y Certificación*. Obtenido de http://www.iram.org.ar/

ISO. (2012). Obtenido de http://www.iso27000.es

ISO. (2012). *ISO 27000 ESPAÑOL.* Obtenido de http://www.iso27000.es/sgsi_implantar.html#seccion1

ISO. (2012). *ISO, ESPAÑOL.* Obtenido de http://www.iso27000.es

ISO. (2014). *The International Organization for Standardization*. Obtenido de http://www.iso.org/iso/home.htm?=

ITGRC. (23 de 03 de 2012). *IT – Governance, Risk & Compliance.* Obtenido de www.francoitgrc.wordpress.com/page/2/

Jocelyne, N. (15 de Octubre de 2013). *Procedimientos para la auditoría física y medio ambiental de un Data.* Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/4978/NOGUEIRA_JOCELYNE_PROCEDIMIENTOS_AUDITORIA_FISICA_MEDIO_AMBIENTAL_DATA_CENTER_CLASIFICACION_ESTANDAR_INTERNACIONAL_TIER.pdf?sequence=1

LCE. (2009). *LCE.* Obtenido de http://intranet2.minem.gob.pe/web/archivos/dge/publicaciones/compendio/dl25844.pdf

Mantilla, A. (07 de 2009). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA COOPERATIVAS DE AHORRO Y CRÉDITO EN BASE A LA NORMA ISO 27001. Quito, Ecuador: Tesis.

Marina, A. d. (16 de 10 de 2013). Planeamiento Estratégico. *Planeamiento Estratégico*. Callao, Peru: Documento Oficial.

Merino Bada, C. (2011). *Implementación SGSI según ISO 27001.* Madris: Fundación Confemetal.

MINSA. (2012). *ANÁLISIS MODAL DE SUS FALLAS Y SUS EFECTOS AMFE.* Obtenido de http://www.minsa.gob.pe/dgsp/observatorio/documentos/herramientas/AMFE.pdf

Moreno, F. (2009). *La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC* (Cuarta edición ed.). Bogota: Puerto ColombiaA.A. .

Moyano Fuentes, J. (2010). *Gestión de la calidad en las empresas tecnologicas de TQM a ITIL.* Madrid, España: StarBook.

Netec. (15 de 07 de 2014). Taller de Ceritifación ITIL Foundation. *ITIL Foundation v3*. Lima, Perú.

Poveda, J. M. (2011). *Gestión y tratamiento de los riesgos.* Obtenido de Modulo 9: http://jmpovedar.files.wordpress.com/2011/03/mc3b3dulo-9.pdf

PriteshGupta. (2012). *El portal de ISO 27001 en Español*. Obtenido de www.iso27000.es

Sans, M. C. (14 de 12 de 1998). Las normas ISO. *Biblio 3W. Revista Bibliográfica de Geografía y Ciencias Sociales Universidad de Barcelona*, Nº 129.

Santa María, F. (30 de Octubre de 2012). *BUENAS PRÁCTICAS PARA AUDITAR REDES INALÁMBRICAS APLICADAS A LAS EMPRESAS DEL RUBRO HOTELERO DE LA CIUDAD DE CHICLAYO.* Obtenido de http://tesis.usat.edu.pe/jspui/bitstream/123456789/105/1/TL_SantaMaria_Becerra_Franck.pdf

Scherkenbach, W. (1994). *La Ruta Deming, hacia la mejora continua.* Mexico: Compañia Editorial Continental Mexico.

Vinca, L. (2011). *Que es ISO 9001.* Obtenido de ¿Qué es ISO 9001:2008?: http://www.normas9000.com/que-es-iso-9000.html

WordPress. (2013). *ADMINISTRACION DE REDES DE COMPUTADORES.* Obtenido de http://camiloangel.wordpress.com/2010/09/03/%C2%BFque-es-un-activo-de-informacion./

Zarabanda, M. I. (28 de 5 de 2014). Propuesta de Implementación de una Arquitectura Segura para activos de información de la Universidad de Boyacá.

ANEXOS

9.1 Anexo A

RESÚMEN DE LA NORMA TÉCNICA PERUANA NTP ISO 27002:2008.

Cláusulas, Objetivos de control y Controles de la NORMA TÉCNICA PERUANA NTP ISO 27002:2008.

A.5 Política de seguridad

A.5.1 Política de seguridad de la información Objetivo de control: 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.		
A.5.1.1	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 requieran.

A.5.1.2	Revisión de la política de seguridad de información	Control La política será revisada en intervalos planificados, y en caso de cambios que la afecten, asegurar que siga siendo apropiada, conveniente y efectiva.

Tabla 47: Política de seguridad

Fuente: NTP ISO 27002:2008

A.6 Seguridad organizacional

A.6.1 Organización interna Objetivo de control: Gestionar la seguridad de la información dentro de la organización.

A.6.1.1	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.
A.6.1.2	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.
A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	Control Todas las responsabilidades sobre la seguridad de información deben ser claramente definidas.
A.6.1.4	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.

A.6.1.5	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.
A.6.1.6	Contacto con autoridades	Control Se debe mantener contactos apropiados con las autorizaciones relevantes.
A.6.1.7	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.
A.6.1.8	Revisión independiente de seguridad de la información	Control El alcance de la organización para manejar 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.6.2 Seguridad del acceso a terceras partes Objetivo de control: Mantener la seguridad de las instalaciones de procesamiento de la información organizacional que acceden, procesan, comunican o gestionan terceros.		
A.6.2.1	Identificación de riesgos por el acceso de terceros	Control Se evaluará los riesgos asociados con el acceso a las instalaciones de procesamiento de la información organizacional por parte de terceros, y se implementarán controles de seguridad adecuados antes de permitir su acceso.
A.6.2.2	Requisitos de seguridad cuando se trata con clientes	Control Se deben identificar todos los requisitos de seguridad antes de dar acceso a clientes a los activos o a la información de la organización.

A.6.2.3	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.

Tabla 48: Seguridad organizacional

Fuente: NTP ISO 27002:2008

A.7 Gestión de activos

A.7.1 Responsabilidad por los activos Objetivo de control: Mantener la protección apropiada de los activos de la organización.

A.7.1.1	Inventario de activos	Control Se elaborará y mantendrá un inventario de todos los activos importantes que sean claramente identificados.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con las instalaciones de procesamiento de información deben ser propiedad3 de una parte designada de la organización.
A.7.1.3	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.7.2 Clasificación de la información Objetivo de control: Asegurar que los activos de información reciban un nivel de protección adecuado		
A.7.2.1	Guías de clasificación	Control La información debe ser clasificada en términos de su valor, requisitos legales, sensibilidad y criticidad para la organización.

A.7.2.2	Etiquetado y tratamiento de la información	Control Se definirá e implementará un conjunto de procedimientos apropiados para etiquetar y manejar información de conformidad con el esquema de clasificación adoptado por la organización.

Tabla 49: Gestión de Activos

Fuente: NTP ISO 27002:2008

A.8 Seguridad en recursos humanos

A.8.1 Previo al empleo Objetivo de control: Asegurar que los empleados, contratistas y usuarios externos entiendan sus responsabilidades y que estos sean adecuados a los roles para los cuales han sido considerados y reducir así el riesgo de estafa, fraude o mal uso de las instalaciones.

A.8.1.1	Roles y responsabilidades	Control Se definirán y documentarán los roles de seguridad y las responsabilidades de los empleados, contratistas y usuarios externos en concordancia con la política de seguridad de la información de la organización.
A.8.1.2	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.
A.8.1.3	Términos y condiciones de la relación laboral	Control Los empleados, contratistas y terceros suscribirán un acuerdo de confidencialidad como parte de los términos y condiciones iniciales de su empleo en donde se señalará la responsabilidad del empleado en cuanto a la seguridad de la información.

A.8.2 Durante el empleo Objetivo de control: 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.		
A.8.2.1	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.
A.8.2.2	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.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario para los empleados que hayan cometido una violación de seguridad.
A.8.3 Finalización o cambio de empleo Objetivo de control: Asegurar que los empleados, contratistas y usuarios externos dejen o cambien de organización de una forma ordenada.		
A.8.3.1	Responsabilidades de finalización	Control Debe informarse sobre los incidentes de seguridad a través de canales administrativos adecuados tan pronto como sea posible.
A.8.3.2	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.

A.8.3.3	Retiro de los derechos de acceso	Control El derecho de acceso a la información y a las instalaciones de procesamiento de información, que se les otorga a los empleados, contratistas y usuarios externos, debe ser removido cuando termine su empleo, contrato o acuerdo; o modificado ante cambios.

Tabla 50: Seguridad en recursos humanos

Fuente: NTP ISO 27002:2008

A.9 Seguridad física y del entorno

A.9.1 Áreas seguras Objetivo de control: Prevenir accesos no autorizados, daños e interferencias contra los locales y la información de la organización.		
A.9.1.1	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.
A.9.1.2	Controles físicos de entradas	Control Las áreas seguras estarán protegidas mediante controles de acceso adecuados para garantizar que únicamente personal autorizado pueda ingresar.
A.9.1.3	Seguridad de oficinas, despachos y recursos	Control Se deben designar y mantener áreas seguras con el fin de proteger las oficinas, despachos e instalaciones.
A.9.1.4	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.

A.9.1.5	El trabajo en las áreas seguras	Control Se debe designar y mantener protección física y pautas para trabajar en áreas seguras.
A.9.1.6	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.9.2 Seguridad de los equipos Objetivo de control: Prevenir pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización.		
A.9.2.1	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.
A.9.2.2	Suministro eléctrico	Control El equipamiento se protegerá de fallas de energía y otras anomalías eléctricas causadas por fallo en el suministro eléctrico.
A.9.2.3	Seguridad del cableado	Control Se protegerá el cableado de energía y telecomunicaciones que transportan datos o respaldan servicios de información frente a interceptaciones o daños.
A.9.2.4	Mantenimiento de equipos	Control El equipamiento recibirá un adecuado mantenimiento para garantizar su continua disponibilidad e integridad.
A.9.2.5	Seguridad de equipos fuera de los locales de la organización	Control Se debe aplicar seguridad al utilizar equipamiento para procesar información fuera de los locales de la organización tomando en cuenta los diferentes riesgos en los que se incurre.

A.9.2.6	Seguridad en el re-uso o eliminación de equipos	Control Todos los equipos que contienen almacenamiento de datos deben ser revisados con el fin de asegurar que los datos sensibles y los software con licencia han sido removidos o sobrescritos antes de desecharlos o reutilizarlos.
A.9.2.7	Retiro de propiedad	Control Los equipos, información y software no deben ser retirados fuera de la organización sin una autorización previa.

Tabla 51: Seguridad física y del entorno

Fuente: NTP ISO 27002:2008

A.10 Gestión de comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades de operación Objetivo de control: Asegurar la operación correcta y segura de los recursos de procesamiento de información.		
A.10.1.1	Documentación de procedimientos operativos	Control Los procedimientos operativos deberán estar documentados, mantenidos y estar disponibles a todos los usuarios que lo requieran.
A.10.1.2	Gestión de cambios	Control Se controlarán los cambios en las instalaciones y sistemas de procesamiento de la información.
A.10.1.3	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.

A.10.1.4	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.10.2 Gestión de entrega de servicios externos Objetivo de control: Implementar y mantener un nivel apropiado de seguridad de información y servicios de entrega en concordancia con los acuerdos de servicios de entrega por parte de terceros.		
A.10.2.1	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.
A.10.2.2	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 auditorías con regularidad.
A.10.2.3	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 de riesgos.
A.10.3 Planificación y aceptación del sistema Objetivo de control: Minimizar el riesgo de fallas de los sistemas.		
A.10.3.1	Gestión de la capacidad	Control Se monitorearán las demandas de capacidad y se harán las proyecciones de futuros requisitos de capacidad para asegurar el desarrollo requerido por el sistema.

A.10.3.2	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.10.4 Protección contra software malicioso Objetivo de control: Proteger la integridad del software y de la información.		
A.10.4.1	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.
A.10.4.2	Controles contra software móvil	Control Donde sea autorizado el uso de software móvil, la configuración debe asegurar que este opere de acuerdo a una política de seguridad clara y definida.
A.10.5 Gestión interna de respaldo y recuperación Objetivo de control: Mantener la integridad y disponibilidad del procesamiento de información y servicios de comunicación.		
A.10.5.1	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.10.6 Gestión de seguridad de redes Objetivo de control: Asegurar la salvaguarda de información en las redes y la protección de la infraestructura de soporte.		
A.10.6.1	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.

A.10.6.2	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.10.7 Utilización y seguridad de los medios de información Objetivo de control: Prevenir daños, modificaciones o destrucciones a los activos e interrupciones de las actividades del negocio.		
A.10.7.1	Gestión de medios removibles	Control Deben de existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Se eliminarán los medios de forma segura cuando ya no se necesiten, utilizando procedimientos formales.
A.10.7.3	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.
A.10.7.4	Seguridad de la documentación de sistemas	Control La documentación de los sistemas se protegerá de accesos no autorizados.
A.10.8 Intercambio de información Objetivo de control: Mantener la seguridad de información y el intercambio de software dentro de la organización y con entidades externas.		
A.10.8.1	Políticas y procedimientos para el intercambio de información	Control Se deben establecer políticas, procedimientos y controles para proteger el intercambio de información durante el uso de todo tipo de recursos de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben de establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.

A.10.8.3	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 organización.
A.10.8.4	Seguridad del correo electrónico	Control La información contenida en correos electrónicos debe ser protegida apropiadamente.
A.10.8.5	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.10.9 Servicios de comercio electrónico Objetivo de control: Mantener la seguridad en los servicios de comercio electrónico y la seguridad en su uso.		
A.10.9.1	Seguridad en comercio electrónico	Control El comercio electrónico será protegido frente a actividades fraudulentas, controversias contractuales y divulgación o modificación de información.
A.10.9.2	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.
A.10.9.3	Información disponible públicamente	Control Se protegerá la integridad de la información públicamente disponible para prevenir modificaciones no autorizadas.
A.10.10 Monitoreo Objetivo de control: Detectar actividades de procesamiento de información no autorizadas.		

A.10.10.1	Registro de auditoría	Control Se deben producir y guardar, por un periodo acordado, los registros de auditoría 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.
A.10.10.2	Uso del sistema de monitoreo	Control Se deben establecer procedimientos para monitorear las instalaciones de procesamiento de información y los resultados del monitoreo de actividades deben ser revisados regularmente.
A.10.10.3	Protección de la información de registro	Control Las instalaciones e información de registro deben ser protegidas contra acceso forzado y no autorizado.
A.10.10.4	Registros de administrador y operador	Control Las actividades del administrador y operadores deben ser registradas.
A.10.10.5	Registros con faltas	Control Las faltas deben ser registradas, analizadas y se deben tomar acciones apropiadas.
A.10.10.6	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 tiempo actual acordado.

Tabla 52: Gestión de comunicaciones y operaciones

Fuente: NTP ISO 27002:2008

A.11 Control de accesos

A.11.1 Requisitos de negocio para el control de accesos Objetivo de control: Controlar los accesos a la información.

A.11.1.1	Política de control de accesos	Control Se debe establecer, documentar y revisar una política de control de accesos, basado en requisitos de acceso de seguridad y del negocio.
A.11.2 Gestión de acceso de usuarios Objetivo de control: Asegurar que el acceso de usuarios es autorizado y prevenir el acceso no autorizado a los sistemas de información.		
A.11.2.1	Registro 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 de información.
A.11.2.2	Gestión de privilegios	Control Se restringirá y controlará la asignación y uso de privilegios.
A.11.2.3	Gestión de contraseñas de usuario	Control Se controlará la asignación de contraseñas a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	Control La gerencia conducirá un proceso formal y de manera periódica para revisar los derechos de acceso del usuario.
A.11.3 Responsabilidades de los usuarios Objetivo de control: Prevenir el acceso no autorizado de usuarios y el compromiso o robo de la información o de las instalaciones de procesamiento.		
A.11.3.1	Uso de contraseñas	Control Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.
A.11.3.2	Equipo informático de usuario desatendido	Control Se exige al usuario que asegure protección adecuada a un equipo desatendido.

A.11.3.3	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.11.4 Control de acceso a la red		
A.11.4.1	Política de uso de los servicios de la red	Control Los usuarios deben tener acceso directo únicamente a los servicios cuyo uso está específicamente autorizado.
A.11.4.2	Autenticación de usuarios para conexiones externas	Control Deben usarse apropiados métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Autenticación de equipos en la red	Control Se debería considerar equipos con identificación automática para autentificar conexiones desde ubicaciones y equipos específicos.
A.11.4.4	Protección para la configuración de puertos y diagnóstico remoto	Control Debe controlarse la seguridad en el acceso lógico y físico para el diagnóstico y configuración de puertos.
A.11.4.5	Segregación en las redes	Control Los grupos de servicios, usuarios y sistemas de información deben ser segregados en las redes.
A.11.4.6	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 política de control de acceso y los requisitos de las aplicaciones de negocio (véase 11.1).

A.11.4.7	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.11.5 Control de acceso al sistema operativo		
A.11.5.1	Procedimientos seguros de conexión	Control Se usará un proceso de registro de conexión (login) seguro para acceder a los servicios de información.
A.11.5.2	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.
A.11.5.3	Sistema de gestión de contraseñas	Control Sistemas de gestión de contraseñas proveerán medios efectivos e interactivos, cuyo objetivo es asegurar contraseñas de calidad.
A.11.5.4	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.
A.11.5.5	Desconexión automática de terminales	Control Las sesiones inactivas deben cerrarse luego de un periodo definido de inactividad.
A.11.5.6	Limitación del tiempo de conexión	Control Se usará restricciones de tiempos de conexión para ofrecer seguridad adicional para las aplicaciones de alto riesgo.
A.11.6 Control de acceso a las aplicaciones e información Objetivo de control: Evitar el acceso no autorizado a la información contenida en los sistemas.		

A.11.6.1	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 con la política de control de acceso.
A.11.6.2	Aislamiento de sistemas sensibles	Control Los sistemas sensibles tendrán un ambiente de cómputo dedicado (aislado).
A.11.7 Informática móvil y teletrabajo Objetivo de control: Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y facilidades de teletrabajo.		
A.11.7.1	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.
A.11.7.2	Teletrabajo	Control Se desarrollarán e implementaran políticas, procedimientos y estándares para las actividades de teletrabajo.

Tabla 53: Control de accesos

Fuente: NTP ISO 27002:2008

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.12.1 Requisitos de seguridad de los sistemas de información Objetivo de seguridad: Garantizar que la seguridad esté incluida dentro de los sistemas de información.		
A.12.1.1	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.12.2 Proceso correcto en aplicaciones Objetivo de control: Prevenir errores, pérdidas, modificaciones no autorizadas o mal uso de los datos del usuario en las aplicaciones.		
A.12.2.1	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.
A.12.2.2	Control del proceso interno	Control Se incorporarán verificaciones y validaciones para detectar cualquier corrupción de los datos procesados.
A.12.2.3	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.
A.12.2.4	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.12.3 Controles criptográficos Objetivo de control: Proteger la confidencialidad, autenticidad o integridad a través de medios criptográficos.		
A.12.3.1	Política de uso de los controles criptográficos	Control Debe desarrollarse e implementarse una política sobre el uso de controles criptográficos para proteger la información.
A.12.3.2	Gestión de claves	Control Se usará un sistema de gestión de claves con el fin de apoyar el uso de técnica criptográficas dentro de la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo de control: Asegurar la seguridad de los archivos del sistema.		

A.12.4.1	Control del software en producción	Control Se pondrá en práctica procedimientos para controlar la implementación del software en sistemas operacionales.
A.12.4.2	Protección de los datos de prueba del sistema	Control Se protegerán y controlarán los datos de prueba los cuales deben ser seleccionados cuidadosamente.
A.12.4.3	Control de acceso a la librería de programas fuente	Control El acceso a las librerías de programas fuente debe ser restringido.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo de control: Mantener la seguridad del software de aplicación y la información.		
A.12.5.1	Procedimientos de control de cambios	Control La implementación de cambios se controlará estrictamente mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de los cambios en el sistema operativo	Control Cuando los sistemas operativos son cambiados, se deben de revisar 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.
A.12.5.3	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 y todos estos cambios deben ser estrictamente controlados.
A.12.5.4	Fuga de información	Control Se deben de prevenir las oportunidades de fuga de información.
A.12.5.5	Desarrollo externo del software	Control La organización debe supervisar y monitorear el desarrollo externo de software.

A.12.6 Gestión de vulnerabilidades técnicas Objetivo de control: Reducir los riesgos que son el resultado de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	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.

Tabla 54: Adquisición de sistemas de información, desarrollo y mantenimiento

Fuente: NTP ISO 27002:2008

A.13 Gestión de incidentes en la seguridad de información

A.13.1 Reportando eventos y debilidades en la seguridad de información Objetivo de control: 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.		
A.13.1.1	Reportando eventos de la seguridad de información	Control Los eventos en la seguridad de información deben ser reportados lo más rápido posible a través de canales apropiados.
A.13.1.2	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.13.2 Gestión de los incidentes y mejoras en la seguridad de información Objetivo de control: Asegurar que un alcance consistente y efectivo sea aplicado en la gestión de incidentes de la seguridad de información.		

A.13.2.1	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.
A.13.2.2	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.
A.13.2.3	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.

Tabla 55: Gestión de incidentes en la seguridad de información

Fuente: NTP ISO 27002:2008

A.14 Gestión de la continuidad del negocio

A.14.1 Aspectos de la gestión de continuidad del negocio en la seguridad de información Objetivo de control: 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.		
A.14.1.1	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.

A.14.1.2	Continuidad del negocio y evaluación de riesgos	Control Los eventos que pueden causar interrupciones en los procesos del negocio deben ser identificados así como las probabilidades e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o reparar operaciones y asegurar la disponibilidad de información al nivel y tiempo requerido, siguiendo las interrupciones o fallas a los procesos críticos del negocio.
A.14.1.4	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 de prueba y mantenimiento.
A.14.1.5	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.

Tabla 56: Gestión de la continuidad del negocio

Fuente: NTP ISO 27002:2008

A.15 Cumplimiento

A.15.1 Cumplimiento de los requisitos legales Objetivo de control: Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de cualquier requisito de seguridad.

A.15.1.1	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.
A.15.1.2	Derechos de propiedad intelectual (DPI)	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.
A.15.1.3	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.
A.15.1.4	Protección de los datos y privacidad de la información personal	Control Se aplicarán controles para proteger información personal en conformidad con la legislación correspondiente y si es aplicable, con las cláusulas contractuales.
A.15.1.5	Prevención en el mal uso de las instalaciones de procesamiento de la información	Control Los usuarios deben ser disuadidos de utilizar las instalaciones del procesamiento de información para propósitos no autorizados.
A.15.1.6	Regulación de los controles criptográficos	Control Se implementarán controles para permitir el cumplimiento de los acuerdos nacionales, leyes y reglamentos.
A.15.2 Cumplimiento con las políticas y estándares de seguridad y del cumplimiento técnico Objetivo de control: Asegurar el cumplimiento de los sistemas con las políticas y normas de seguridad organizacionales.		

A.15.2.1	Cumplimiento con los estándares y la política de seguridad	Control Los gerentes deben tomar acciones para garantizar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se lleven a cabo correctamente con el fin de garantizar el cumplimiento de laspolíticas y estándares de seguridad.
A.15.2.2	Comprobación del cumplimiento técnico	Control Debe verificarse regularmente el cumplimiento de la implementación de normas de seguridad en los sistemas de información.
A.15.3 Consideraciones sobre la auditoría de sistemas Objetivo de control: Maximizar la efectividad y minimizar las interferencias en el proceso de		
A.15.3.1	Controles de auditoría de sistemas	Control Se planificarán cuidadosamente las auditorías de los sistemas operacionales a fin de minimizar el riesgo de interrupciones a los procesos de negocio.
A.15.3.2	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.

Tabla 57: Cumplimiento

Fuente: NTP ISO 27002:2008

9.2 Anexo B

Formato e Inventario de Activos

ENTRADAS

Plantilla para el Talento Humano

Personas

PERSONAL OFICIALES DE LA COMANDANCIA OPERACIONES GUARDACOSTAS SIMTRAC Y COSPAS SARSAT

No.	Grad.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
1	C DE N	SGC	HINOJOSA LÓPEZ MANUEL	00803558	SIMTRAC COSPAS SARSA	
2	C DE N	SGC	MEIER VON SCHIERENBECK Martínez Werner	02833645		
3	C DE N	SGC	PAREDES BLANCO	046373632		
4	C DE F	SGC	SANTA MARÍA Oliva Enrique	08474635		
5	C DE C	CG	ESPINOZA Oré Crishan	00913650		
6	C DE C	CG	SEMINARIO Seminario	05241190		
7	TTE 1	CG	LUN PUN Torres Victor	01018139		

No.	Grad.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
8	TTE 1	CG	NUÑES DEL PRADO Altamirano Angela Katerine	01019181		
9	TTE 2	CG	PAREDES VALDIVIA	06542901		
10	AFRA	CG	PÉREZ Pinto André	00076624		
11	AFRA	CG	MALDONADO Portal Norma Franshesca	00020758		

Tabla 58 Censo Personal Oficiales

Fuente: Elaborado por los Autores

PERSONAL SUBALTERNO DE LA COMANDANCIA OPERACIONES GUARDACOSTAS SIMTRAC Y COSPAS SARSAT

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
1	TS2	Man.	MASSA Dueñas José Antonio	02782911	SIMTRAC COSPAS SARSAT	
2	TS2	ECO	ARRELUCEA DEL POZO VICTOR	03846653		
3	T3	CCG	TENORIO QUISPE RICARDO	09753287		
4	T3	CCG	LUQUE TOVAR WALTER	03241569		
5	T3	TEL	CASAS CHUCHON NILTON	00933454		
6	T3	ECO	CHATO CHÁVEZ JUAN F.	00937484		
7	T3	COT	SALAS VERA JORGE	01992600		

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
8	OM1	Pda.	REBAZA Chumacero Michael	00060082		
9	OM1	Man.	VENTURA Luyo Rolando Alexander	01914753		
10	OM2	Eco.	CHÁVEZ REYNA	07633748		
11	OM3	Ccg.	TRIGOSO Vásquez Mónica Paola	01033748		
12	OM3	Man.	BUSTAMANTE Huaco Roberto	00075590		

Tabla 59: Censo Personal Subalterno

Fuente: Elaborado por los Autores

PERSONAL SUBALTERNO DE LA COMANDANCIA OPERACIONES GUARDACOSTAS

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
1	TS1	Mot.	LIMO Calderón Luís Enrique	04715627	OPERACIONES	
2	TS2	Tel.	CUMPALLI Loza Manuel Alberto	05753648	LOGÍSTICA	
3	TS2	Eco	ARRELUCEA	083554122	SECRETARIA	
4	T1	Oes.	TORRES Camarena Dionisio	00762854	OPERACIONES	
5	T1	Ccg.	ACOSTA Ramos Domingo Elías	02856232	GRUPO DE OPERACIONES ESPECIALES	
6	T1	Señ.	PARRA Moreno Pablo	04830039	OPERACIONES	

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
7	T1	Señ.	ZAVALA Muro Enrique Raúl	06884532	SECRETARIA	
8	T2.	Mot.	QUENTA Flores Julio Alberto	03813320	OPERACIONES	
9	T2	Man.	TAPIA Alzamora Humberto	02897076	GRUPO DE OPERACIONES ESPECIALES	
10	T2	Ccg.	CALDERÓN Contreras Carlos	03876445	GRUPO DE OPERACIONES ESPECIALES	
11	T2	Ccg.	LOAYZA Callo Manuel	06827445	GRUPO DE OPERACIONES ESPECIALES	
12	T3	Int.	TASAYCO Wong Roberto	03977092	OPERACIONES	
13	T2	Tel.	RIOS Martínez Ángel Gustavo	05823766	LOGÍSTICA	
14	T3	Tel.	CABRERA Olivos Robert Juan	02990295	TALLER ELECTRÓNICA	
15	T3	Tel.	CASAS Chuchon Nilton	00933454	TALLER MECÁNICA	
16	T3	Ccg.	DEL CARPIO Escudero Cristian	02934565	OPERACIONES	
17	T3	Aba.	HUAQUI Llata Willy	02989037	LOGÍSTICA	
18	T3	Ccg.	HUMAREDA Domínguez Iván	02919357	GRUPO DE OPERACIONES ESPECIALES	
19	T3	Ccg.	NAVARRO Neyra Oscar Miguel	06862731	TALLER DE ELECTRÓNICA	
20	T3	Ccg.	PÉREZ Dávila Manuel	02935533	OPERACIONES	

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
21	T3	Sad.	TÚPAC YUPANQUI Marín Jorge Luis	01901485	LOGÍSTICA	
22	T3	Ccg.	ALIAGA		SECRETARIA	
23	OM1	Ima.	ZAGACETA Daza Carlos Alberto	02965355	OPERACIONES	
24	OM1	Enf.	ALEGRÍA Carlín John Alejandro	01983532	GRUPO DE OPERACIONES ESPECIALES	
25	OM1	Sad.	CARPIO Nole Cinthia Paola	01037122	OPERACIONES	
26	OM1	Mot.	ESPINOZA Godoy Edward	01043146	SECRETARIA	
27	OM1	Art.	HUAMANI Chirinos Ismael Antero	01977842	OPERACIONES	
28	OM1	Ccg.	PAICO Santamaría Arturo	01983891	GRUPO DE OPERACIONES ESPECIALES	
29	OM1	Mau.	ROJAS Díaz Nelson	05961506	GRUPO DE OPERACIONES ESPECIALES	
30	OM1	Pon.	RAMÍREZ Alvino Alex	00982490	GRUPO DE OPERACIONES ESPECIALES	
31	OM1	Ccg.	SARAVIA Saravia Edgar Iván	00982994	OPERACIONES	
32	OM1	Mot.	TERRONES Huailla Frank Richard	00984942	LOGÍSTICA	
33	OM1	Tel.	ZAVALETA Perea Arturo	02907690	TALLER ELECTRÓNICA	
34	OM1	Man.	AMARO Nazario Noé	00974778	TALLER MECÁNICA	

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
35	OM1	Mot.	HUAMANCHUMO Palma Miguel Ángel	0955664	OPERACIONES	
36	OM2	Ele.	ARROYO Papa Julio	00976763	LOGÍSTICA	
37	OM2	Ccg.	DELGADO Fernández Jesús	01971888	GRUPO DE OPERACIONES ESPECIALES	
38	OM2	Mot.	CARPIO Gómez Marco Antonio	00053211	TALLER DE ELECTRÓNICA	
39	OM2	Man.	CASTILLO Siclla Celestino	00081486	OPERACIONES	
40	OM2	Ccg.	MENDOZA Redhead Ronald Jesús	01030371	LOGÍSTICA	
41	OM2	Ccg.	NAVINTA Chávez Edwin David	01000524	SECRETARIA	
42	OM2	Ccg.	LOPEZ Lacunce José	01979851	OPERACIONES	
43	OM2	Ccg.	ORTIZ Rodríguez Flavio	00974973	GRUPO DE OPERACIONES ESPECIALES	
44	OM2	Ccg.	PIZARRO López María Aurora	01034340	OPERACIONES	
45	OM2	Ccg.	SALAZAR Contreras Saraly Shirley	01036634	SECRETARIA	
46	OM2	Ccg.	SÁNCHEZ Arquinigo María Isabel	02047251	OPERACIONES	
47	OM2	Ccg.	MEZA Tiza Priscilla Pilar	01022672	GRUPO DE OPERACIONES ESPECIALES	

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
48	OM2	Ccg.	TONCCONI Barrionuevo Víctor	00096027	GRUPO DE OPERACIONES ESPECIALES	
49	OM2	Ccg.	VALLADOLID Castañeda Gianfranko	01017548	GRUPO DE OPERACIONES ESPECIALES	
50	OM2	Ccg.	MATOS Carhuas Paulo Isidoro	01021655	OPERACIONES	
51	OM2	Man.	RENGIFO Vela Edward	05984439	LOGÍSTICA	
52	OM2	Tel.	SALVADOR Ríos Eduardo	00992422	TALLER ELECTRÓNICA	
53	OM3	Mot.	HUANCAHUIRI Silvera Carlos	01008730	TALLER MECÁNICA	
54	OM3	Adm.	ESPINOZA Dávila Cinthya Clara	00077823	OPERACIONES	
55	OM3	Ccg.	SEMINARIO Alzamora Edward	01970306	LOGÍSTICA	
56	OM3	Señ.	LÓPEZ Collazos Walter	00064294	GRUPO DE OPERACIONES ESPECIALES	
57	OM3	Ccg.	SOTO Cotos Elizabeth	01027797	TALLER DE ELECTRÓNICA	
58	OM3	Tel.	ZAMORA Valles Dimas	02933548	OPERACIONES	
59	OM3	Eco.	GONZÁLES Tinco Víctor	02040669	LOGÍSTICA	
60	OM1	Man.	VIVANCO Valerio Juan	00987967	SECRETARIA	
61	OM3	Adm.	DÍAZ Tineo Juan Carlos	00050891	OPERACIONES	

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
62	Cb1.	Pon.	QUISPE Morales Ana María	00141045	GRUPO DE OPERACIONES ESPECIALES	
63	CB1.	Ccg.	VARGAS Herrera Reyna	00192272	OPERACIONES	
64	CB1.	Ccg.	PAUCCA Calla Eduardo	01103180	SECRETARIA	
65	CB1.	Ccg.	HUARANCCAY Auccapuclla Mayumi	00199175	OPERACIONES	
66	MAR.	Ccg.	BUSTAMANTE Díaz Gilmer	03111374	GRUPO DE OPERACIONES ESPECIALES	

Tabla 60: Censo Personal Subalterno

Fuente: Elaborado por los Autores

PERSONAL MARINERÍA DE LA COMANDANCIA OPERACIONES GUARDACOSTAS

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
1	Cb1	Ccg.	RODRÍGUEZ Crispín Silvana	02033513		
2	Cb1	Ccg.	ASALDE Santamaría Manuel Iván	00012671		
3	Cb1	Ccg.	RIVAS Rivas Jennyfer Ruth	00076752		
4	Cb1	Ccg.	LLAMACPONCCA Uñapillco Martha	00071948		
5	Cb2.	Ccg.	HUARANCCAY Auccapuclla Mayumi	00199175		

Nº	Grd.	Esp.	Apellidos y Nombre	CIP. Nº	Área de Destaque	Cargo
6	Mar.	Ccg.	ACUÑA Urimachea Antoni Jossimar	00162243		

Tabla 61: Censo Personal Marinería

Fuente: Elaborado por los Autores

NOTA: Los cargos por ser de responsabilidad interna de la Marina de Guerra del Perú en la Comandancia de Operaciones Guardacostas no serán llenados.

Plantilla para los Recursos Tecnológicos

ÁREA SISTEMA DE INFORMACIÓN Y DE MONITOREO DE TRÁFICO ACUÁTICO – SIMTRAC

Servidores

SERVIDORES									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
1	HP	Proliant T350 G6	4/300 Gb		Red Hat Linux	Servidor Aplicación y Base de Datos	Themis y Oracle	2009	OL
2	HP	Proliant DL180 G6	3/300 Gb		Red Hat Linux	Servidor Base de Datos Back Up	Oracle	2009	OL
3	HP	Proliant DL160 G6	2/300 Gb		Red Hat Linux	Servidor Web	Apache y Tomcat	2009	OL
4	Compatible	Core 2 Duo E8400	1/500 Gb	2 Gb	Centos Linux	Servidor de Correo	PostFix	2009	OL
5	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	2 gb	Win 7	Servidor de Cartografía	Cartografía	2009	OL

Tabla 62: Inventario Servidores SIMTRAC

Fuente: Elaborado por los Autores

Estaciones de Trabajo

Estaciones de Trabajo									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
1	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	4 gb	Win 7	PC Adm Sala de Servidores		2009	O
2	Compatible	i3 3.33 Ghz	1/250 Gb	2 gb	Win 7	PC Adm Sala de Servidores		2009	O
3	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	4 gb	Win 7	PC AIS Comunicación con Italia		2009	O
4	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	4 gb	Win 7	PC Seguridad Wira		2009	O

Estaciones de Trabajo									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
5	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	4 gb	Win 7	PC Cliente Themis		2009	O
6	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	4 gb	Win 7	PC AIS Cliente		2009	O
7	Compatible	i5 -2500 3.30 Ghz	1/500 Gb	4 gb	Win 7	PC Ploteo Embarcaciones		2009	O
8	Compatible	i3 3.33 Ghz	1/250 Gb	2 gb	Win 7	PC AIS Internacional		2007	OL
9	Compatible	Core 2 Duo E8400	1/500 Gb	2 Gb	Win 7	PC Tráfico Marítimo		2007	OL
10	HP	HP Compaq 6000			Win7	PC Secretari Jefe		2009	OL

Tabla 63: Inventario Estaciones de Trabajo SIMTRAC

Fuente: Elaborado por los Autores

Equipos de Comunicación

Equipos de Comunicación									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
1	Check Point	Safe Office 10000				Seguridad de la Red		2009	O
2	HP	Switch V1910-24G				Comunicación		2009	O
3	HP	Switch V1910-24G				Comunicación		2009	O
4	UNITY	UPS ABEST				Back Up Energía Eléctrica para Servidores		2009	O

Tabla 64: Inventario Equipos de Comunicación SIMTRAC

Fuente: Elaborado por los Autores

ÁREA COSPAS SARSAT

Servidores

SERVIDORES									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
1	HP	Proliant ML370	4 / 76 Gb		Windows 2000 Server	Servidor LEOLUT 200	Comunicaciones Satélite LEOSAR	2006	OL
2	HP	AlphaServer DS15	2 / 25 Gb		Open VMS Alpha Server	Servidor OCC200	Sistema OCC200	2006	OL
3	HP	Prolaint DL380 G7				Servidor OCC600		2012	O
4	HP	Prolaint DL380 G7				Servidor GEO SP		2012	O
5	HP	Prolaint DL380 G6				Servidor GEOFP		2012	O
6	HP	Prolaint DL380 G6				Servidor MEO LUT		2012	O
7	HP	Prolaint ML110				WEB		2006	OL

Tabla 65: Inventario Servidores COSPAS SARSAT

Fuente: Elaborado por los Autores

Estaciones de Trabajo

Estaciones de Trabajo									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
1	HP	XW4200			Windows XP	Cliente OCC200	Interface OCC200	2006	OL
2	HP	XW6200			Windows XP	Servidor /Cliente SarMaster	SarMaster	2006	OL

Estaciones de Trabajo									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
3	HP					Cliente OCC600	Cliente OCC600	2012	O
4	Compatibles				Win 7	Administrativo	Officina	2013	O
5	Compatibles				Win 7	Administrativo	Officina	2010	OL
6	Compatibles				Win 7	Administrativo	Officina	2010	OL

Tabla 66: Inventario Estaciones de Trabajo COSPAS SARSAT

Fuente: Elaborado por los Autores

Equipos de Comunicación

Equipos de Comunicación									
Núm.	Marca	Modelo o Procesador	HD	RAM	SO	Servicio	Sistema	Fecha Ingreso	Estado
1	3COM	4226T				Switch	(comoperguard)	2009	OL
2	Cisco	1800 Series				Router	Telefónica	2009	OL
3	RAD	FOMi-E1T1				Transformador de Fibra a Ethernet	Telefónica	2009	OL
4	ATRAN	-				Comunicador de Router a Transformador de Fibra a Ethernet	Telefónica	2009	OL
5	REXIS	TELDAT				Modem	Telefónica para línea AFTN	2000	OL
6	Black Box	724-746-5500				Switch convertidor Fibra a Ethernet		2006	OL

Tabla 67: Inventario Equipos de Comunicaciones COSPAS SARSAT

Fuente: Elaborado por los Autores

Plantilla para los Sistemas de Información

ÁREA SISTEMA DE INFORMACIÓN Y DE MONITOREO DE TRÁFICO ACUÁTICO - SIMTRAC

Núm.	Tipo de sistema	Nombre	Proveedor	Versión	Responsable	Fecha Ingreso	Estado
1	Aplicación principal	THEMIS	CLS Perú		Administrador de Red	2010	OL
2	Base de Datos	ORACLE	CLS Perú			2010	O
3	Base de Datos	BACK UP ORACLE	CLS Perú			2010	O
4	Página Web	APACHE TOMCAT	CLS Perú			2011	OL
5	Correo	POSTFIX	Comopergu ard			2012	O
6	Sistema de Identificació n Automática	AIS	Comopergu ard			2009	OL
7	Sistema de Radares	PEGASE	CLS Perú			2012	OL

Tabla 68: Inventario Sistemas de Información SIMTRAC

Fuente: Elaborado por los Autores

ÁREA COSPAS SARSAT

Núm.	Tipo de sistema	Nombre	Proveedor	Versión	Responsable	Fecha Ingreso	Estado
1	Conectividad Satélites LEOSAR	LEO LUT	Honeywell			2006	O
2	Conectividad Satélites GEOSAR	GEO LUT SP	Honeywell			2013	O

Núm.	Tipo de sistema	Nombre	Proveedor	Versión	Responsable	Fecha Ingreso	Estado
3	Conectividad Satélites GEOSAR	GEO LUT FP	Honeywell			2013	O
4	Aplicación Principal	OCC200	Honeywell			2006	O
5	Aplicación Principal	OCC600	Honeywell			2013	O
6	Conectividad Satélites MEOSAR	MEOLUT	Honeywell			2013	O
7	Cartografía	SARMASTER	Honeywell			2006	O
8	Endian	ENDIAN FIREWALL	Endian			2011	O

Tabla 69: Inventario Sistemas de Información COSPAS SARSAT

Fuente: Elaborado por los Autores

Leyenda

Estado	
Operativo	O
Operativo con Limitaciones	OL
No Operativo	NO

Tabla 70: Leyenda Estado

Fuente: Elaborado por los Autores

9.3 Anexo C

HERRAMIENTAS PROPUESTAS PARA LA FASE DE VERIFICAR EL PLAN DE SGSI

1. GRÁFICOS DE CONTROL

Esta herramienta es de gran utilidad en el momento del análisis de tendencias de los indicadores trazados. Consiste en determinar gráficamente los límites bajo los cuales se considera que determinado indicador está bajo control o dentro de las especificaciones aceptadas tal como se muestra a continuación:

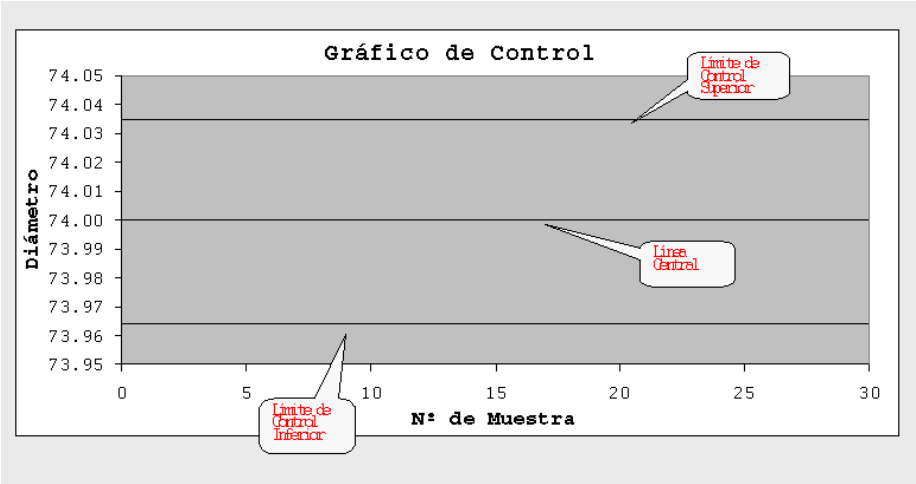

Ilustración 43: Gráfico de control. Límites

Fuente: (ESAN, 2013)

Una vez construida la plantilla se grafica los valores de la medición realizada

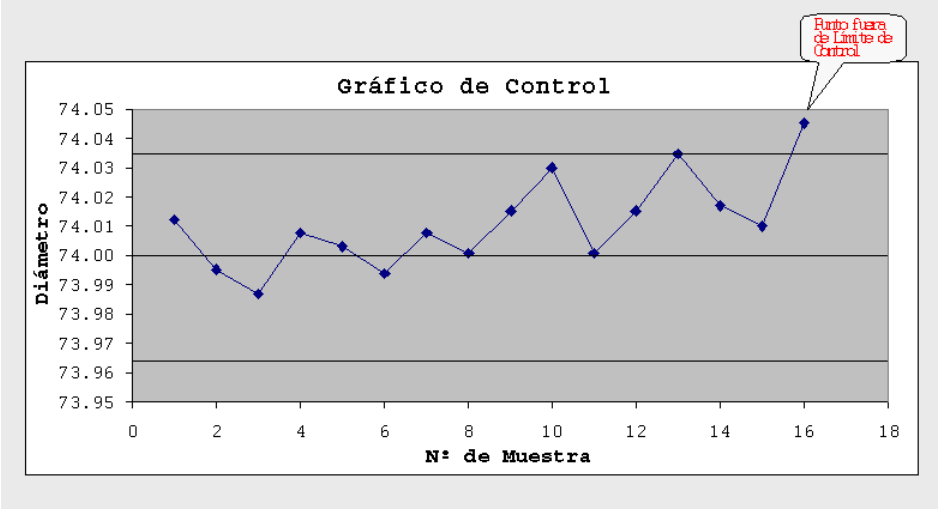

Ilustración 44: Gráfico de Control. Punto fuera de especificación

Fuente: (ESAN, 2013)

Después del séptimo dato se puede empezar a analizar las tendencias del indicador con el fin de tomar decisiones, a continuación se enuncia comportamientos típicos y como analizarlos.

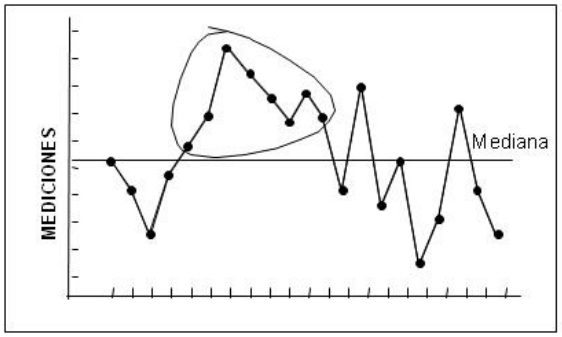

Ilustración 45: Gráfico de Control. Análisis respecto a la Mediana

Fuente: (ESAN, 2013)

Siete o más puntos seguidos en el mismo lado de la mediana indican una variación en el proceso. (Si los datos son simétricos se puede usar la media como promedio en lugar de la mediana).

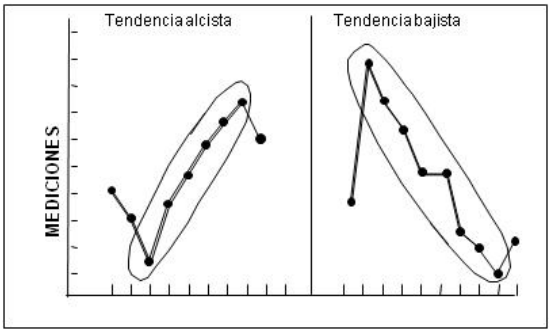

Ilustración 46: Gráfica de Control. Tendencias

Fuente: (ESAN, 2013)

Seis o más puntos seguidos con incremento o decremento continuo indican una tendencia. (Se debe empezar a contar en el punto en el que cambia la dirección).

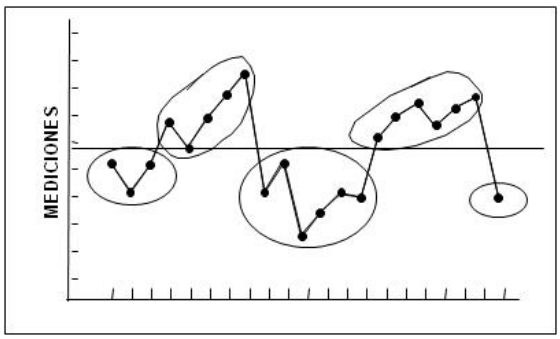

Ilustración 47: Gráfica de Control. Tendencias

Fuente: (ESAN, 2013)

Muy pocos datos agrupados indican una desviación en la media del proceso, un ciclo o una tendencia.

Demasiados datos agrupados indican muestreo desde dos fuentes, sobrecompensación o un sesgo.

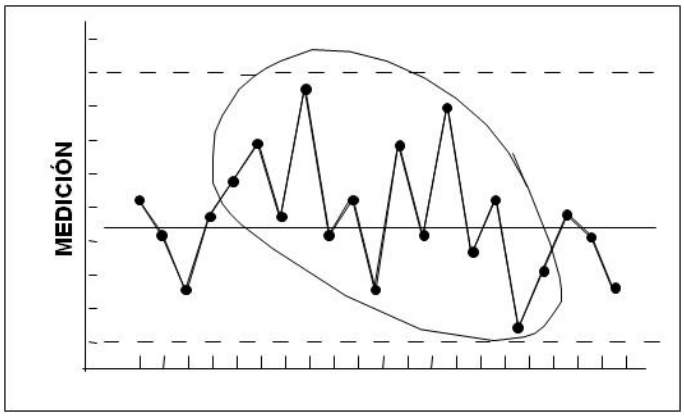

Ilustración 48: Gráfica de Control. Dispersión

Fuente: (ESAN, 2013)

14 o más puntos seguidos alternando arriba y abajo indican problemas de sesgo o de muestreo.

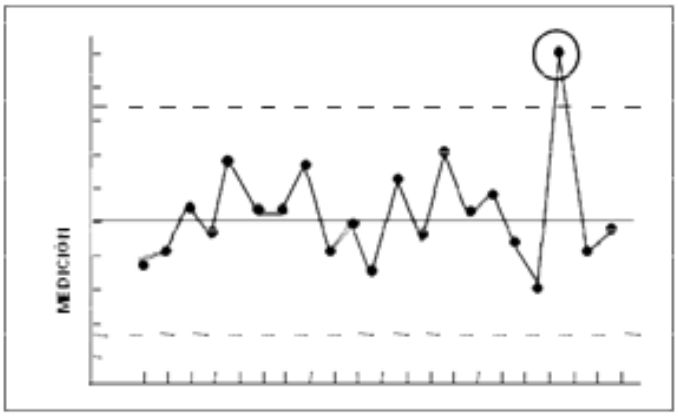

Ilustración 49: Gráfica de Control. Dispersión

Fuente: (ESAN, 2013)

Uno o más puntos fuera de los límites de control indican una diferencia en estos puntos.

El análisis de los datos y tendencias permiten anticiparse con acciones preventivas a hechos que más adelante pueden causar problemas el interior de SGSI. Un adecuado seguimiento garantiza acciones oportunas.

2. PLAN DE VERIFICACIÓN DEL PLAN DE SGSI

Este documento especifica los riesgos, controles, responsables, objetivos de control y los indicadores como herramienta para evaluar la eficiencia y establecer el cumplimiento de los del Plan de SGSI.

Plan de Verificación del Plan de Sistema de Gestión de Seguridad de la Información.

Plan de Verificación del Plan de Sistema de Gestión de Calidad

PLAN DE VERIFICACIÓN DEL PLAN DE SGSI					
Riesgo a Controlar	Método de control			Objetivo de Control	Indicador
	Control Implementado	Registro	Responsable		

Tabla 71: Plan De Verificación del Plan De SGSI

Fuente: Elaborado por los Autores

9.4 Anexo D

HERRAMIENTAS PROPUESTAS PARA LA FASE DEL ACTUAR EL PLAN DE SGSI

1. DIAGRAMA CAUSA – EFECTO

   Muy útil para causas de un problema determinado, la metodología consiste en reunir un grupo interdisciplinario que esté involucrado en el proceso, evaluar cada una de las variables que pueden llegar a afectar el resultado de la operación en que se detectó el problema (Mano de obra, Maquina, Material, Métodos, etc.) cualquier variable puede incluirse dentro del diagrama, las anteriores son las más comunes pero el grupo está en la facultad de manejar las variables a analizar según considere conveniente. Fuente: (ESAN, 2013)

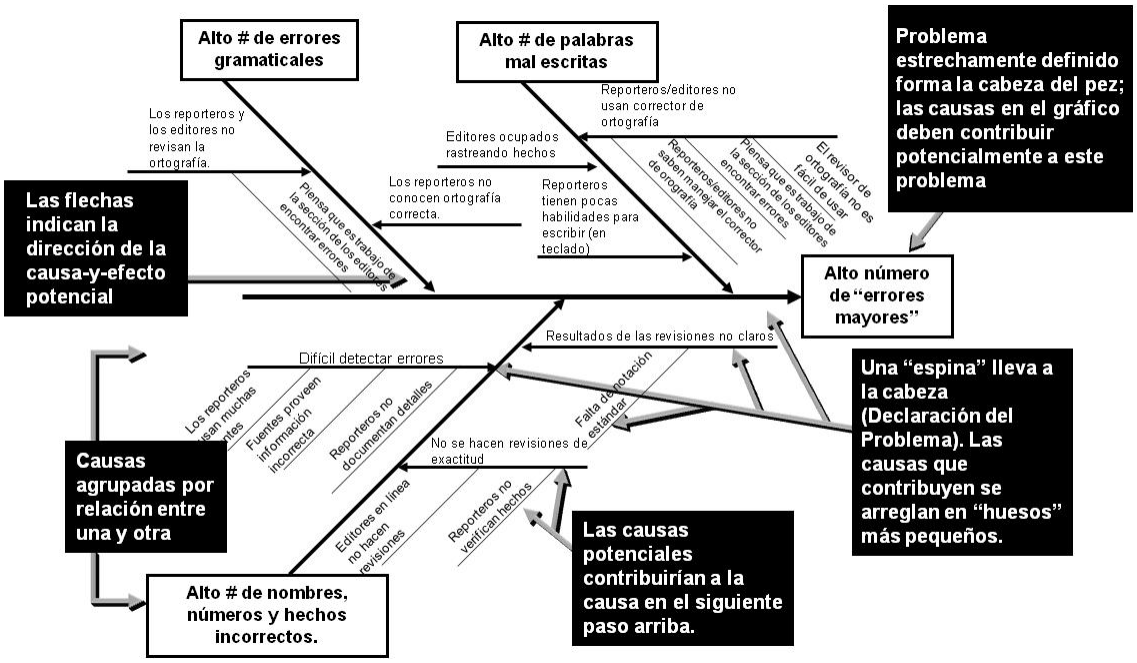

Ilustración 50: Diagrama Causa Efecto

Fuente: (ESAN, 2013)

La grafía anterior muestra la construcción del diagrama, el problema es la cabeza del mismo de la cual salen las variables a analizar, una en cada espina principal.

Se realiza entonces una lluvia de ideas para asignar una posible causa del problema principal en cada una de las variables analizadas, en adelante se debe repetir el proceso para identificar 2 o 3 sub causas de la causa principal determinada para cada variable. De esta forma van surgiendo diferentes posibles causas del problema a solucionar, una vez se lleve el cuadro con 3 niveles de profundidad, se deben priorizar cuales de las causas encontradas atacar teniendo en cuenta la complejidad y el impacto de atacar una o la otra.

2. LOS 5 ¿Por qué?

Esta metodología complementa al diagrama causa efecto, trabajándolas unidas hacen una herramienta muy efectiva en la detección de causa raíz de un problema.

El diagrama de causa efecto se determinan diferentes posibles causas de un determinado problema, los 5 porque consiste en preguntar como mínimo 5 veces ¿Por qué sucede determinada causa?, dando respuesta a 5 porque se llega a un nivel de profundidad que permite determinar la causa raíz del problema. Una acción para mitigar una causa raíz asegura que el problema desaparezca y no se vuelva a repetir. Fuente: (ESAN, 2013)

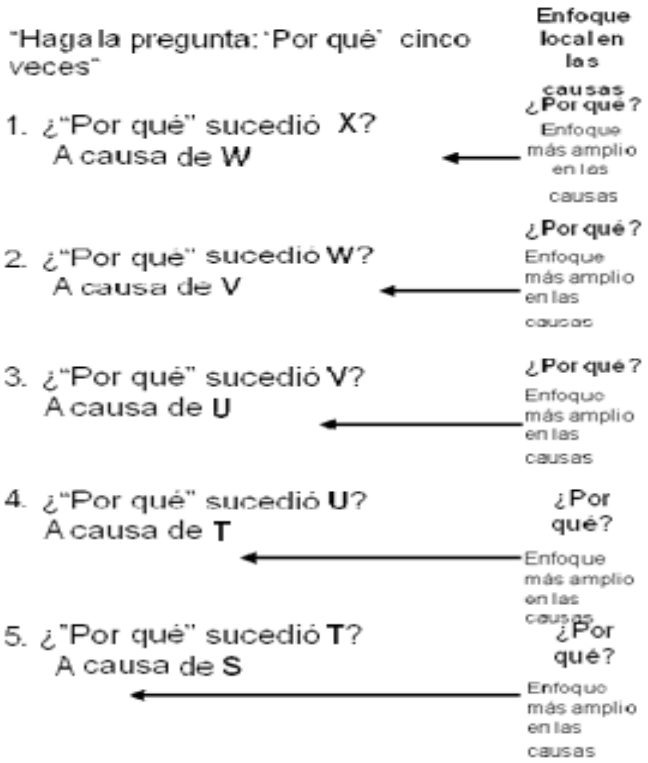

Ilustración 51: Diagrama de los 5 ¿Por qué?

Fuente: (ESAN, 2013)

Las anteriores dos herramientas se proponen para determinar de manera efectiva en poder identificar y realizar acciones correctivas y preventivas, las acciones como tal dependen del tipo de problema, no existe una metodología para determinar la forma de proceder para resolver determinado problema, esto depende de la creatividad y conocimiento del grupo dispuesto para buscar la solución.

9.5 Anexo E

PLAN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA COMANDANCIA DE OPERACIONES GUARDACOSTAS

El Plan de Sistema de Gestión de Seguridad de Información de la Comandancia de Operaciones y Guardacostas para las áreas de COSPAS-SARSAT y SIMTRAC, consiste en un proceso ordenado que consiste en establecer los mecanismos necesarios de seguridad de manera documentada y conocida por todos los miembros

Este Plan de SGSI ha sido un estudio para mejorar la seguridad de información, para lo cual se realizó un cruce de información debidamente analizada entre el problema actual de seguridad de información de la Comandancia de Operaciones y Guardacostas y la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008, teniendo como resultado este documento para su implementación.

CONTROLES A IMPLEMENTAR EN LAS ÁREAS COSPAS- SARSAT Y SIMTRAC.

1. El control sobre los “Derechos de Propiedad Intelectual” que se encuentra en la cláusula “CUMPLIMIENTO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Dentro de los procesos y procedimientos establecidos se establecerá el cumplimiento de las restricciones legales, reguladoras y contractuales para el uso de material protegido por los derechos de la propiedad intelectual.

Protección de la propiedad intelectual:

- Se creara una política de derechos de autor del software definida por el área legal para estos productos.
- Se adquirirán solamente software de propietarios legales con licencias asegurando el derecho de autor.
- Concientizaremos a los usuarios sobre el derecho de autor en las adquisiciones dando a conocer las medidas de sanciones al violar estos derechos.
- Realizar registros del software para tener un control de la propiedad intelectual.
- Controlaremos la cantidad de usuarios que ingresen a los sistemas sin autorización.
- Controlaremos por medio de inventarios el software con licencias autorizados a utilizarse.
- Se efectuaran auditorias periódicas.
- Se controlaran el uso de software y de la información obtenida en las redes públicas.

2. El control sobre “Salvaguarda de los Registros de la Organización” que se encuentra en la cláusula “CUMPLIMIENTO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Se protegerán los registros de importancia en la comandancia por las posibles pérdidas, destrucción y falsificación.

- Se clasificaran los registros según sea el tipo; se guardaran los registros manteniendo su seguridad por el tiempo que se encuentren retenidos.

- Se mantendrá un control de los medios de almacenamiento por su deterioro en el tiempo según especificaciones del fabricante; incluyendo procedimientos para tener acceso a ellos.
- Se mantendrá un sistema que permita el almacenamiento y con la propiedad de poder recuperarse en el momento que se requieran.
- Crearemos guías sobre las retenciones, almacenamientos, tratamientos y eliminación de los registros para las personas responsables en la comandancia.
- Se confeccionara una agenda o calendario de la retención con periodos de caducidad de los registros.

3. El control sobre “Protección de los datos y de la Privacidad de la Información Personal” que se encuentra en la cláusula “CUMPLIMIENTO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Se protegerán los datos y su privacidad de acuerdo a las legislaciones organizacionales.

- Crearemos una política de protección a los datos que se difundirá a todo el personal con el respectivo procedimiento a seguir.
- Se cumplirán las leyes de la protección de datos bajo una estructura de gestionable apropiada.
- Se designara un encargado para esta responsabilidad que ayude a entender y seguir los procedimientos de este servicio.
- Controles de mejores prácticas habituales para conseguir la seguridad de la información:

4. El control sobra “Documento de política de seguridad de la información” que se encuentra en la cláusula “POLÍTICA DE SEGURIDAD” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Esta cláusula está desarrollada en el punto página 183 Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008

5. El control sobre “Asignación de Responsabilidades Sobre Seguridad de la Información” que se encuentra en la cláusula “ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Esta cláusula TRES (3) está desarrollada en el punto página 164 Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008

6. El control sobre “Conocimiento, Educación y Entrenamiento de la Seguridad de Información” que se encuentra en la cláusula “SEGURIDAD EN RECURSOS HUMANOS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Brindaremos capacitaciones a los empleados; y si es necesario a los contratistas con los conocimientos y actualizaciones necesarias para la función de su trabajo.

Esto de la siguiente forma:

- Induciendo al empleado en los procesos necesarios para la designación de la seguridad de la información antes de conceder acceso a los sistemas de información o servicios.
- Los entrenamientos contemplaran los procesos de seguridad, responsabilidades legales y controles de la comandancia; así como el correcto uso de la información.

7. El control sobre “Validación de los Datos de Entrada” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Se validaran el ingreso de la información a los sistemas garantizando que sean correctos. Se consideraran:

- Que no se dupliquen las entradas detectando los errores de fuera de rango, caracteres inválidos, datos incompletos y datos no autorizados.
- Se verificara el contenido periódicamente de las claves para su validez e integridad.
- Verificaremos que los archivos físicos no tengan cambios no autorizados en sus ingresos de datos.
- Confeccionaremos procedimientos para los posibles errores de validación.
- Se otorgaran responsabilidades de los encargados en la entrada de datos.
- Todo lo efectuado se registrara y esto será un procedimiento de los datos de entrada.

8. El control sobre “Control del proceso interno” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Se integrara un sistema que nos permita monitorear los ingresos corruptos o con errores o por acciones negativas al sistema.

Aseguraremos con restricciones el riesgo de fallos al proceso; se considerara:

- Las funciones agregar y eliminar para modificaciones en los datos.
- Programas que aseguren la recuperación luego que se produzcan las fallas.
- Protegeremos la entrada de datos contra ataques usando corridas o desbordes de buffers.

En este punto se verificaran los accesos teniendo una documentación apropiada con lo siguiente:

- Un control de sesiones.
- Un control de tiempo de uso del sistema.
- Un control del perfil de ingreso con sus actividades.
- Un control que verifique que el sistema está operando adecuadamente.
- Se crearan registros de todas las actividades.

9. El control sobre “Integridad de Mensajes” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Asegurar la autenticidad e integridad de los mensajes con la creación de controles aceptados por la comandancia y que cumplan con las normativas de la misma.

La comandancia conviene en usar criptografías como medio adecuado para autenticación; esta será realizada por un área específica de la marina de guerra encargada de estos procedimientos.

10. El control sobre “Validación de los Datos de Salida” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

La validación de datos salientes se realizara por medio de encriptación de la VPN con el proveedor de servicio de datos externos; estas contienen:

- Veracidad de los datos para ser usados en el sistema.
- Un control que permita que asegure el correcto funcionamiento de todos los datos.
- Un registro de actividades y tareas para validar los datos de salida.

11. El control sobre “Control de las Vulnerabilidades Técnicas” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Mantener siempre informado de las vulnerabilidades del sistema; y evaluar a la comandancia sobre tales vulnerabilidades para tomar medidas apropiadas.

Se realizaran los inventarios técnico respectivo a fin de gestionar las vulnerabilidades; este inventario contemplara al proveedor de software, sus versiones y los responsables de estas aplicaciones en la comandancia.

Localizando las vulnerabilidades técnicas:

- Se definirán roles y responsabilidades en la gestión de vulnerabilidades así como su respectivo monitoreo de las mismas.
- Los recursos destinados para identificar las vulnerabilidades y su monitoreo serán actualizados de acuerdo a los cambios de inventarios.
- Verificaremos las vulnerabilidades con los riesgos asociados a ellos para posteriores acciones a tomar en cuenta.
- Siendo la vulnerabilidad alta las acciones a tomar serán de acuerdo a los controles de la gestión del cambio (ver 12.5.1).
- Si existen ecualizaciones se verificaran primero los riesgos de esta actualización; estos deberán ser evaluados antes de su instalación.
- Llevar un registro de ingresos para los procedimientos realizados.
- Los sistemas de mayor riesgo siempre serán tratados con prioridad.

12. El control sobre “Aprendiendo de Los Incidentes en La Seguridad de Información” que se encuentra en la cláusula “GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Se utilizara una tarea que permita monitorear y cuantificar los costos de los incidentes en la seguridad de la información.

La información obtenida en la evaluación de los incidentes en la seguridad de la información se usara para visualizar los que se repiten o sean de gran impacto.

13. El control sobre “Recolección de Evidencia” que se encuentra en la cláusula “GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Los datos históricos servirán como evidencias que serán recolectadas, retenidas y presentadas según sean necesarias para implicancias legales correspondientes.

Existen procesos disciplinarios en la comandancia a los que se les integrara las evidencias necesarias para dicho propósito.

Usaremos:

- Evidencias que puedan ser usadas en las cortes militares y civiles; para esto los sistemas deben cumplir estándares para que la evidencia sea utilizada.
- De alta calidad y completa evidencia del acto en cuestión; debe ser confiable sin manipulación alguna durante el periodo de la evidencia.
- En documentos físicos; se tendrán registro de su hallazgo desde quien lo encontró, donde, cuando y un testigo del encuentro.
- En medios informáticos; se tomaran en cuenta las copias de seguridad e información de los discos duros. Se registraran todas las acciones realizadas a los medios o dispositivos de evidencia.

Los trabajos forenses solo se realizaran en la copia del material en evidencia. El material debe ser íntegro y protegido; las posibles copias requeridas serán supervisabas y registradas de cuando, donde, como y con qué herramienta fue realizado.

14. El control sobre la “Incluyendo la Seguridad de Información En El Proceso De Gestión De La Continuidad Del Negocio” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Propondremos un proceso de gestión de desarrollo y mantenimiento para la continuidad del negocio que trate la seguridad de la información para dicha continuidad.

Consideraremos:

- Hacer entender los riesgos de la organización desde sus vulnerabilidades e impacto identificando y priorizando sus procesos críticos.
- Identificaremos los activos que estén en los procesos críticos del negocio.
- Sensibilizar sobre el impacto que causaría la interrupción del negocio.
- Aconsejaremos la adquisición de seguros que serán parte del proceso de continuidad de negocios.
- Implementaremos controles de prevención.
- Asegurar la seguridad del personal y la protección de las instalaciones y propiedad de la comandancia.
- Se formulara y documentara planes de continuidad de negocio a la par con la seguridad de la información.
- Incorporaremos la gestión de la continuidad del negocio en los procesos de la organización.

15. El control sobre “Continuidad del Negocio y Evaluación de Riesgos” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue.

Esta cláusula está desarrollada en el punto 10.1.2.1.2 Del Análisis Realizado en base a la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.

16. El control sobre “Redacción e Implantación de Planes de Continuidad que incluyen La Seguridad de Información” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Desarrollaremos planes de mantenimiento y recuperación de las operaciones del negocio asegurando la disponibilidad de la información en el tiempo necesario en una interrupción o falla de los procesos críticos.

Consideraremos:

- Los procedimientos de emergencia y acuerdos de responsabilidades.
- Aceptaremos ciertas pérdidas de información y servicios que no comprometan a la comandancia.
- Evaluaremos escalas de tiempo para la recuperación y restauración de las operaciones por medio de procedimientos.
- Evaluaremos procedimientos operativos para la recuperación y restauración total.
- Documentar siempre los procedimientos acordados.
- Pruebas y mejoramiento de los planes acordados.

17. El control sobre “Marco de Planificación para La Continuidad del Negocio” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Crear una estructura de planes para la continuidad del negocio asegurando que los planes sean consistentes y nos permitan priorizar la seguridad, pruebas y mantenimiento.

El plan de continuidad de negocio estará limitado al alcance especificando claramente en que momentos se tomara acción de dicho plan incluyendo los procedimientos dentro de la gestión de cambios de la comandancia.

Determinando la envergadura de la comandancia se tendrán en cuenta uno o más planes con sus respectivos propietarios.

Se consideraran:

- Que los planes describan los procedimientos antes de dicha acción.
- Las acciones a tomar en caso de emergencias que amenacen a las actividades de la organización.
- Acciones necesarias de respaldo que permitan restablecer a la organización y volverla operativa en el tiempo requerido.
- Tareas requeridas que permitan terminar con la restauración y que las operaciones de la organización vuelvan a la normalidad.
- Los mantenimientos preventivos respectivos al plan realizando las pruebas necesarias para conocer su efectividad.
- Acciones de concientización de los procedimientos de la organización que aseguren su total entendimiento.

- Los responsables de las acciones críticas tendrán suplentes que permitan activar el plan en caso de pruebas, emergencia, respaldo y activación.

18. El control sobre “Prueba, Mantenimiento y Reevaluación de Los Planes de Continuidad” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” está recomendada por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 y su implementación es como sigue:

Implementación del control:

Estos planes serán evaluados constante mente con el fin de actualizarlos y probar sus resultados.

Las pruebas consistirá en que los equipos de recuperación estarán atentos a sus responsabilidades para la continuidad de la organización y aseguramiento de la información conociendo sus roles dentro del plan.

La confección del plan de pruebas contendrá las fechas de estas mismas y la realización una por una.

Contemplaremos:

- Las pruebas en varios casos.
- Entrenamiento al equipo con simulaciones de los casos que podrían suceder.
- Las acciones para la recuperación de los sistemas de información.
- Las acciones a tomar para recuperación de la organización se al caso en un lugar diferente al actual.
- Que los proveedores de servicios cumplan los compromisos establecidos para la recuperación.

Relacionaremos las principales medidas de seguridad directamente con las áreas del SIMTRAC y del COSAS - SARSAT, los controles y su implementación, tomando como base la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 - Ver Anexo 2 -.

1. El control sobre “Documento de Política de Seguridad de La Información” que se encuentra en la cláusula “POLÍTICA DE SEGURIDAD” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no existen políticas de seguridad.

Implementación del control:

Se iniciara con la concientización de las jefaturas de la comandancia comprometiéndolos a apoyar las distintas políticas que se implementaran en la seguridad de la información.

En principio se creara un documento de seguridad de la información que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Se definirá los objetivos de la seguridad de la información.
- Dentro de los objetivos de la jefatura es apoyar a los objetivos de la seguridad de la información.
- Un alcance que contendrá los objetivos de control, la evaluación de riesgos y la gestión de riesgos.
- Una breve explicación para los requisitos legislativos y contractuales; requisitos de formación en seguridad; gestión de la continuidad del negocio y las consecuencias de las violaciones de la política de seguridad.

- Definiciones de las responsabilidades generales y específicas de la gestión de la seguridad de la información y de las incidencias de seguridad.
- Referencias de documentos que sustentarían la política.

2. El control sobre “Asignación de Responsabilidades sobre Seguridad de La Información” que se encuentra en la cláusula “ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay un responsable de las áreas vulnerables; no existen documentos de seguridad.

Implementación del control:

Se consolidara las responsabilidades para la seguridad de la información esto en base a las políticas de seguridad para los activos creando procesos de seguridad claros; esto estará especificado en una guía que tendrá las ubicaciones, sistemas o servicios específicos; contendrá también la responsabilidad del proceso del plan de continuidad de negocio.

También contendrá:

- Identificación de los activos y procesos de seguridad por cada uno de los sistemas.
- Se nombrara al responsable del activo o procedimiento de seguridad documentando su responsabilidad.
- Se definirá y documentara los niveles de seguridad.

3. El control sobre “Acuerdos de Confidencialidad” que se encuentra en la cláusula “ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD” es

obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay acuerdos de confidencialidad internas.

Implementación del control:

Los acuerdos de confidencialidad para la comandancia serán identificados y revisados continuamente anexando los requisitos indispensables para la protección de la información considerando los términos legales para este fin.

Consideraremos:

- La interpretación y clara definición de la información que será protegida.
- Acordar un tiempo de confidencialidad para la información o sin límite de tiempo.
- Las acciones necesarias al culmino de un acuerdo si es el caso.
- La responsabilidad y acciones a tomar para evitar acceso a la información no autorizada.
- Al propietario de la información; secretos de la comandancia y propiedad intelectual todo relacionado con la protección de la información.
- Los permisos de utilización de la información y los derechos y deberes de usarla.
- Procedimientos para las notificaciones del uso de información confidencial.
- Procedimientos para la destrucción de la información cuando esta sea cesada.
- Tomar acciones en caso no se cumpla este acuerdo.

4. El control sobre “Inventario de Activos” que se encuentra en la cláusula “CLASIFICACIÓN Y CONTROL DE ACTIVOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a

la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay seguridad para los activos.

Implementación del control:

Serán identificados los activos de información con un inventario que será actualizado cada vez que se adquiera un activo.

El inventario estará descrito en un documento que incluirá toda la información que nos permita la recuperación de los mismos en caso de desastres; este debe discriminar entre los activos más importantes para que la organización sigua funcionando; aparte de los detalles de los activos como marca, modelo, entre otros; este debe contener a los propietarios de estos activos.

5. El control sobre “Propiedad de Los Activos” que se encuentra en la cláusula “CLASIFICACIÓN Y CONTROL DE ACTIVOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay seguridad para los activos.

Implementación del control:

No hay un área de sistemas designada en la comandancia; pero si un administrador de la red o responsable de los sistemas quien será el que tenga los procesos de información designados de la organización.

Se responsabilizara a los propietarios de los activos en las siguientes acciones:

- Que aseguren la información y los activos correspondientes clasificándolos apropiadamente.

- Definir y revisar cada cierto tiempo las restricciones de acceso considerando las políticas de control utilizadas.

6. El control sobre “Inclusión de La Seguridad en Las Responsabilidades y Funciones Laborales” que se encuentra en la cláusula “SEGURIDAD EN RECURSOS HUMANOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no están delimitados los roles del personal.

Implementación del control:

La comandancia tiene a bien elaborar los contratos por un área legal responsable; por lo tanto se inicializara con las funciones, responsabilidades y con un acuerdo de confidencialidad que también será documentada con los expedientes del contratado.

A los responsables de la seguridad se les comunicara de manera clara sus funciones durante su clasificación.

Las funciones de seguridad y responsabilidades contendrán:

- Implementadas y realizadas en coincidencia con las políticas de seguridad de la organización vistas en el punto 5.1.
- Deberán proteger los activos no autorizados de ser adulterados por alguna forma o razón.
- Tendrán procesos y actividades especiales para su ejecución.
- Al responsable asignado deberá tomar las acciones pertinentes según sea el caso.
- Serán reportados los incidentes que alteren la seguridad de la organización o que puedan ser un riesgo potencial.

7. El control sobre “Perímetro de Seguridad Física” que se encuentra en la cláusula “SEGURIDAD FÍSICA Y DEL ENTORNO” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay seguridad en la red.

Implementación del control:

Se realizara una nueva arquitectura de red con un cableado estructurado acorde a las nuevas tendencias tecnológicas; un nuevo data center de la misma manera y la seguridad requerida para dicho fin.

Pautas para el perimetraje de la seguridad física:

- Acorde con la evaluación de riesgos la seguridad estará definida; esto también en concordancia con los requisitos de seguridad del activo.
- En la construcción del edificio los muros de acceso deberán estar debidamente sólidos y los accesos contendrán equipos biométricos para los accesos a los ambientes que requieran la seguridad respectiva.
- Tendrá contemplado un área de recepción y control de acceso.
- Contemplara barreras de seguridad en todo el edificio evitando así entradas no autorizadas y contaminación del entorno.
- Tanto las salidas de emergencias y puertas de escape tendrán algún dispositivo de visualización o sonoro para saber dónde se encuentran en el momento de un incidente real; estos lugares serán evaluados y probados su resistencia en concordancia de los estándares requeridos para dicho fin.
- El área de procesamiento de información será separada físicamente para que no sean manipuladas por terceros.

8. El control sobre “Planificación de La Capacidad” que se encuentra en la cláusula “GESTIÓN DE COMUNICACIONES Y OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay seguridad para los activos.

Implementación del control:

Por buenas practicas es recomendable no exceder del 20% de la capacidad máxima, por lo tanto los activos de información de la comandancia se tendrá que velar y monitorear que siempre tenga capacidad adecuada para su seguridad, lo cual la norma recomienda lo siguiente:

Se creará un documento de la capacidad de seguridad de la información que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Se deberá planificar los tiempos de llegada los recursos y sus costos, lo cual la gerencia tiene que monitorear la utilización de los recursos.
- La Gerencia deberá utilizar herramientas tecnológicas para determinar la tendencia de uso, relativamente al negocio.
- Los administradores deberán de analizar esta información y prever posibles amenazas sobre la seguridad de información y se deberá planificar el Plan de Acción respectivo.

9. El control sobre “Controles de Red” que se encuentra en la cláusula “GESTIÓN DE COMUNICACIONES Y OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay seguridad en la red.

Implementación del control:

Las redes es una pieza fundamental para la seguridad de información en cualquier organización, lo cual la norma recomienda lo siguiente:

Se creará un documento de la seguridad de red que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- En la comandancia debe de separar la responsabilidad operativa y la operación operativa de las computadoras.
- La comandancia tiene que establecer responsabilidades para la administración de equipos remotos.
- La comandancia debe establecer procedimientos para proteger la confidencialidad e integridad de los datos que pasan a través de la red.
- La comandancia deberá contar con un registro y monitoreo de acciones de seguridad.
- La comandancia debe de realizar coordinaciones para verificar si se están aplicando los controles en toda la infraestructura de red.

10. El control sobre “Seguridad en La Mensajería Electrónica” que se encuentra en la cláusula “GESTIÓN DE COMUNICACIONES Y OPERACIONES” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay seguridad en la red.

Implementación del control:

Los correos electrónicos es una fuente de información que debe ser protegida, lo cual la norma recomienda lo siguiente:

Se creará un documento de la seguridad de red, respecto a la seguridad de correos electrónicos, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- La comandancia debe de establecer la protección de ingreso de correos.
- La comandancia debe establecer aquellas direcciones permitibles.
- La comandancia debe considerar las firmas digitales.
- La comandancia debe establecer una política para el personal autorizado que tenga correo para acceder desde wifi o acceso público de internet.

11. El control sobre “Política de Control de Accesos” que se encuentra en la cláusula “CONTROL DE ACCESOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no se toman en cuenta las políticas de acceso a las áreas vulnerables.

Implementación del control:

Los accesos a cualquier fuente de información deberán estar documentada, revisada y tiene que estar alineada a los requerimientos de seguridad y del negocio, lo cual la norma recomienda lo siguiente:

Se creará un documento de control de acceso, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- La comandancia debe identificar toda la información sobre el acceso a las aplicaciones con sus respectivos riesgos.
- La comandancia debe realizar políticas para la distribución de información y autorizaciones, lo cual debe tener coherencia entre control de accesos y clasificación de información.

- La comandancia debe establecer perfiles de acceso de usuario estandarizados.
- La comandancia debe tener la administración de acceso distribuido de la red con su rol de control respectivo.
- La comandancia debe de controlar el acceso a las áreas, solo para aquellas personas que se encuentre en el registro de usuario.
- La comandancia debe de generar periódicamente el monitoreo sobre el retiro de acceso a aquellas personas que ya no laboran o se desvinculen del área de sistemas.

12. El control sobre “Registro de Usuarios” que se encuentra en la cláusula “CONTROL DE ACCESOS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no hay un control de usuarios.

Implementación del control:

Un procedimiento adecuado de registro de usuario actualizando las altas y bajas de usuarios, garantiza un seguro acceso de los sistemas, lo cual la norma recomienda lo siguiente:

Se creará un documento de registro de usuario, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Implementar la utilización de un identificador único para cada usuario, con esta acción se vincularía a los usuarios con sus acciones.
- Realizar un control de comprobación de autorización de usuario.
- Se debe de entregar a los usuarios una relación de sus derechos de acceso.
- Se debe de cumplir la negación de acceso a menos que hayan completado los procedimientos de autorización.

- Realizar un mantenimiento del registro de autorización de acceso del servicio.
- Monitorear periódicamente la eliminación de identificadores y cuentas de usuario redundantes.
- Asegurar la no reasignación de usuarios con identificadores de usuarios dados de baja.

13. El control sobre “Fuga de Información” que se encuentra en la cláusula “ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS” es obtenida por la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: fuga de información.

Implementación del control:

La fuga de información debe de ser prevenida, lo cual la norma recomienda lo siguiente:

Se creará un documento de fuga de información, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Detectar todos los medios de salida de información como puerto usb, correos, carpetas compartidas, etc.
- Monitorear periódicamente las actividades del personal y del sistema, bajo las normas legales.
- Monitorear el uso de recursos en sistemas de cómputo.

14. El control sobre “Continuidad del Negocio y Evaluación de Riesgos” que se encuentra en la cláusula “GESTIÓN DE CONTINUIDAD DEL NEGOCIO” es obtenida por la NORMA TÉCNICA PERUANA NTP-

ISO/IEC 27001:2008 es asociada a la deficiencia encontrada en la organización y su implementación es como sigue:

Deficiencia: no existe un plan de continuidad de negocio.

Implementación del control:

La continuidad del negocio es el punto más común y difícil que debe afrontar cualquier organización, identificar sus causas y darle pronta solución, lo cual la norma recomienda lo siguiente:

Se creará un documento de continuidad del negocio, que será distribuido en toda la comandancia escrito en forma entendible y que contendrá:

- Identificar los eventos que puedan causar interrupciones en los procesos de negocio.
- Se debe de evaluar los riesgos para determinar su probabilidad e impacto de dichas interrupciones, debe incluir aspectos de seguridad de información, debe ser cuantificable y priorizar a los alineamientos de los objetivos de La Comandancia, incluyendo impacto de las interrupciones tiempos aceptables de la interrupción y prioridades de recuperación.
- Desarrollar un Plan Estratégico con un enfoque global de la continuidad del negocio a partir de la evaluación de riegos.
- Una vez aprobada el Plan Estratégico la jefatura de La Comandancia deberán respaldarla y desarrollar un Plan de Implementación de dicha estrategia.

9.6 Anexo F

Un punto de partida de la seguridad de la información es considerar las recomendaciones de las NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008 en las mejores prácticas habituales para conseguir dicha seguridad.

- Controles esenciales para una Organización desde un punto de vista legislativa:

15. CUMPLIMIENTO

15.1 Cumplimiento con los requisitos legales

OBJETIVO: Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad.

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

Se debería buscar el asesoramiento sobre requisitos legales específicos de los asesores legales de la organización, o de profesionales del derecho calificados. Los requisitos legales varían de un país a otro, al igual que en el caso de las transmisiones internacionales de datos (datos creados en un país y transmitidos a otro).

15.1.2 Derechos de propiedad intelectual (DPI) Control

Se deberían implantar los procedimientos apropiados para asegurar el cumplimiento de las restricciones legales, reguladoras y contractuales sobre el

uso del material protegido por derechos de propiedad intelectual y sobre el uso de productos de software propietario.

Guía de Implementación

Las siguientes pautas deben ser consideradas para proteger cualquier material que pueda ser considerado propiedad intelectual:

a) publicar una política de conformidad de los derechos de autor del software que defina el uso legal de los productos de software e información.
b) adquirir software solamente a través de fuentes conocidas para asegurar que el copyright no sea violado.
c) mantener la concientización sobre los derechos de autor del software y la política de adquisiciones, publicando la intención de adoptar medidas disciplinarias para el personal que los viole.
d) mantener los registros apropiados de activos e identificar todos los activos con requerimientos para proteger los derechos de la propiedad intelectual
e) mantener los documentos que acrediten la propiedad de licencias, material original, manuales, etc.
f) implantar controles para asegurar que no se exceda el número máximo de usuarios permitidos.
g) comprobar que sólo se instale software autorizado y productos bajo licencia.
h) establecer una política de mantenimiento de las condiciones adecuadas de la licencia.
i) establecer una política de eliminación de software o de su transferencia a terceros.
j) usar herramientas adecuadas de auditoria;
k) cumplir los términos y condiciones de uso del software y de la información obtenida de redes públicas.

l) no duplicar, convertir en otro formato o extraer de grabados comerciales (audio, filmaciones) lo que no sea permitido por la ley de copyright.

m) no copiar parcial o totalmente libros, artículos, reportes u otros documentos que no sean permitidos por la ley de copyright.

Otra Información

Los derechos de la propiedad intelectual incluyen al software o copyright del documento, derechos de diseño, marca registrada, patente y fuentes de licencia de código.

Los productos de software propietario son suministrados usualmente bajo un acuerdo de licencia que especifica los términos y condiciones, por ejemplo limitar el uso de productos para maquinas especificas o limitar el copiado solamente en la creación de las copias de respaldo. La situación de los derechos de la propiedad intelectual requiere ser esclarecido por el personal.

Los requisitos legislativos, regulatorios y contractuales pueden indicar restricciones en el copiado de material propietario. En particular, pueden requerir que solo se utilice el material que sea desarrollado por la organización o que sea licenciado o provisto por el creador a la organización. La infracción de copyright puede llevar a acciones legales que pueden involucrar procedimientos criminales.

15.1.3 Salvaguarda de los registros de la organización

Control

Se deberían proteger los registros importantes de la organización frente a su pérdida, destrucción y falsificación en concordancia con los requisitos regulatorios, contractuales y de negocio.

Guía de Implementación

Se debería clasificar los registros por tipos: registros contables, registros de bases de datos, registros de transacciones, registros de auditoria y procedimientos operativos, cada tipo con los detalles de sus plazos de retención y medios de almacenamiento (papel, microfichas, soporte magnético u óptico). Las claves criptográficas relacionadas con archivos cifrados o firmas digitales (véase el inciso 12.3) se deberían guardar de forma segura con el fin de habilitar el encriptado de los registros por el tamaño de tiempo que estos se encuentran retenidos.

Se debería considerar la posibilidad de degradación de los medios utilizados para almacenar los registros. Se deberían implantar procedimientos para su almacenamiento y utilización de acuerdo con las recomendaciones del fabricante. Para un almacenamiento a largo plazo, se puede considerar el uso de papel o de microfichas.

Cuando se utilicen medios electrónicos de almacenamiento se deberían incluir procedimientos que aseguren la capacidad de acceso a los datos (o sea, la legibilidad tanto del medio como del formato) durante el plazo de retención, como objeto de salvaguardarlos contra su pérdida por futuros cambios de tecnología.

Se deberían elegir los sistemas de almacenamiento de datos para que éstos puedan recuperarse a tiempo y en un formato aceptable, dependiendo de los requisitos.

El sistema de almacenamiento y utilización debería asegurar una identificación clara de los registros y de su periodo de retención legal o regulatorio. Esto debería permitir la destrucción apropiada de los registros tras dicho periodo cuando ya no los necesite la organización.

Para dar cumplimiento a éstas obligaciones la organización debería dar los pasos siguientes:

a) se debería publicar guías sobre la retención, almacenamiento, tratamiento y eliminación de los registros y la información.
b) se debería establecer un calendario de retenciones que identifique los períodos para cada tipo esencial de registros.
c) se debería mantener un inventario de las fuentes de información clave.
d) se deberían implantar los controles y medidas apropiadas para la protección de los registros y la información esencial contra su pérdida, destrucción o falsificación.

Otra Información

Es necesario guardar de forma segura ciertos registros, tanto para cumplir ciertos requisitos legales o regulatorios, como para soportar actividades esenciales del negocio. Por ejemplo, los registros que puedan requerirse para acreditar que la organización opera dentro de las reglas estatutarias o regulatorias, para asegurar una defensa adecuada contra una posible acción civil o penal, o bien para confirmar el estado financiero de la organización respecto a los accionistas, socios y auditores. La legislación nacional u otros reglamentos suelen establecer el plazo y contenido de la información a retener.

Para mayor información sobre el manejo de los registros organizacionales, se puede consultar la ISO 15489-1.

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

Control

La protección de datos y la privacidad debe ser asegurada como se requiere en la legislación, las regulaciones y, si es aplicable, en las cláusulas contractuales.

Guía de Implementación

Se debería implementar y desarrollar una política organizacional de privacidad y de protección de datos. Esta política debe ser comunicada a todo el personal implicado en el procesamiento de información personal.

El cumplimiento de la legislación de protección de datos personales requiere una estructura y controles de gestión apropiados. Este objetivo suele alcanzarse con mayor facilidad, designando un encargado de dicha protección que oriente a los directivos, usuarios y proveedores de servicios sobre sus responsabilidades individuales y sobre los procedimientos específicos a seguir. La responsabilidad para maniobrar información personal y asegurar el conocimiento de los principios de protección de datos debe ser confrontado con la legislación y regulaciones actuales. Se debería implementar medidas técnicas y organizacionales apropiadas para proteger la información personal.

Otra Información

Muchos países han establecido legislación colocando controles y medidas para el tratamiento y transmisión de datos personales (en general la información sobre personas físicas que pueda identificarlas). Dependiendo de la legislación nacional actual, estos controles y medidas suponen ciertas obligaciones a quien recoja, procese, ceda o comunique información personal, y puede restringir la posibilidad de transferir estos datos a otros países.

- Controles de mejores prácticas habituales para conseguir la seguridad de la información:

5. POLÍTICA DE SEGURIDAD

5.1 Política de seguridad de la información

OBJETIVO: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

5.1.1 Documento de política de seguridad de la información

Control

La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.

Guía de implementación

Debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento debería contener como mínimo la siguiente información:

a) una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información (véase el capítulo de Introducción).
b) el establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información.
c) un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión del riesgo.

d) una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización, por ejemplo:
1) conformidad con los requisitos legislativos y contractuales.
2) requisitos de formación en seguridad.
3) gestión de la continuidad del negocio.
4) consecuencias de las violaciones de la política de seguridad.
e) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad.
f) las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible.

Otra información

La política de seguridad debe ser parte de un documento general de la política empresarial. Se debe tener cuidado al distribuir la política de seguridad fuera de la organización con el fin de no compartir información confidencial.

6. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

6.1 Organización interna

OBJETIVO: Gestionar la seguridad de la información dentro de la organización.

Debería establecerse una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de la organización.

Es conveniente organizar foros de gestión adecuados con las gerencias para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implantación de la seguridad en toda la organización.

Si fuera necesario, debería facilitarse el acceso dentro de la organización a un equipo de consultores especializados en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad para mantenerse al día en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como tener un punto de enlace para tratar las incidencias de seguridad. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información.

6.1.3 Asignación de responsabilidades sobre seguridad de la información

Control

Deberían definirse claramente las responsabilidades.

Guía de implementación

La asignación de responsabilidades sobre seguridad de la información deben hacerse en concordancia con la información de la política de seguridad (véase capítulo 4). Las responsabilidades para la protección de activos individuales y para llevar a cabo procesos de seguridad específicos deben ser claramente identificadas. Esta asignación, debería completarse, dónde sea necesario, con una guía más detallada para ubicaciones, sistemas o servicios específicos. Deberían definirse claramente las responsabilidades locales para activos físicos y de información individualizados y los procesos de seguridad como, por ejemplo, el plan de continuidad del negocio.

Los propietarios de los activos de información pueden delegar sus responsabilidades de seguridad en directivos a título individual o en proveedores de servicios. Sin embargo, el propietario sigue manteniendo la

responsabilidad última sobre la seguridad del activo y debería estar capacitado para determinar que cualquier responsabilidad delegada se ha cumplido correctamente.

Es esencial que se establezcan claramente las áreas de las que cada directivo es responsable; en particular deberían establecerse las siguientes:

a) deberían identificarse claramente los activos y los procesos de seguridad asociados con cada sistema específico.
b) debería nombrarse al responsable de cada activo o proceso de seguridad, y deberían documentarse los detalles de esta responsabilidad.
c) deberían definirse y documentarse claramente los niveles de autorización.

Otra información

Muchas organizaciones nombran un director de seguridad de la información como el responsable del desarrollo e implantación de la seguridad y para dar soporte a la identificación de las medidas de control.

Sin embargo, la responsabilidad de proporcionar recursos e implantar las medidas de control suele recaer en ciertos directivos. Una práctica habitual consiste en designar un propietario de cada activo de información, que se convierte así en responsable de su seguridad cotidiana.

6.1.5 Acuerdos de confidencialidad

Control

Requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información deben ser identificadas y revisadas regularmente.

Guía de implementación

Confidencialidad o acuerdos de no divulgación deben anexar los requerimientos para proteger información confidencial usando términos ejecutables legales. Para identificar requerimientos de confidencialidad o acuerdos de no divulgación, se deben considerar los siguientes elementos:

a) una definición de la información a ser protegida;
b) duración esperada del acuerdo, incluyendo casos donde la confidencialidad pueda necesitar ser mantenida indefinidamente.
c) acciones requeridas cuando un acuerdo sea finalizado.
d) responsabilidades y acciones de los signatarios para evitar acceso desautorizado a la información.
e) propiedad de la información, secretos del comercio y de la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial.
f) la permisión de utilizar información confidencial y los derechos del signatario para usar la información.
g) el derecho de auditar y monitorear actividades que impliquen información confidencial.
h) procesos para notificar y reportar acceso desautorizado a aberturas de información confidencial.
i) términos para que la información sea retornada o destruida en la cesación del acuerdo.
j) acciones prevista que se tomará en caso de una abertura de este acuerdo.

Basado en los requerimientos de la seguridad de una organización, otros elementos pueden ser necesarios en una acuerdo de confidencialidad o de no-acceso.

Los acuerdos de confidencialidad y de no-acceso deben conformarse con todas las leyes aplicables y las regulaciones para la jurisdicción a la cual aplica (véase el inciso 15.1.1).

Los requerimientos para acuerdos de confidencialidad y de no-acceso deben ser revisados periódicamente y cuando ocurran cambios que influyan en estos requerimientos.

Otra información

Los acuerdos de confidencialidad y de no-acceso protegen información organizacional e informan a los signatarios de sus responsabilidades a proteger, usando y accediendo a información de forma responsable y autorizada.

Puede ser necesario para una organización, usar diferentes formas de acuerdos de confidencialidad o de no-acceso en diferentes circunstancias.

8. SEGURIDAD EN RECURSOS HUMANOS

8.2 Durante el empleo

OBJETIVO: Asegurar que los empleados, contratistas, y usuarios de terceros estén conscientes de las amenazas y riesgos en el ámbito de la seguridad de la información, y que están preparados para sostener la política de seguridad de la organización en el curso normal de su trabajo y de reducir el riesgo de error humano.

Las responsabilidades de la gerencia deben ser definidas para asegurar que la seguridad sea aplicable a través del empleo de un individuo dentro de la organización.

Un nivel adecuado de conocimiento, educación y entrenamiento en procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información debe ser provista a todos los empleados, contratistas y usuarios de terceros con el fin de minimizar los posibles riesgos de seguridad. Se debe establecer un proceso disciplinario formal para maniobrar aberturas de seguridad.

8.2.2 Conocimiento, educación y entrenamiento de la seguridad de información

Control

Todos los empleados de la organización y donde sea relevante, contratistas y usuarios de terceros deben recibir entrenamiento apropiado del conocimiento y actualizaciones regulares en políticas y procedimientos organizacionales como sean relevantes para la función de su trabajo.

Guía de implementación

El entrenamiento en el conocimiento debe empezar con una inducción formal del proceso designado para introducir la política de seguridad de la organización y las expectativas, antes conceder acceso a la información o al servicio.

El entrenamiento en curso debe incluir requisitos de seguridad, responsabilidades legales y controles del negocio, así como prácticas en el uso correcto de los recursos de tratamiento de información (procedimientos de concesión (log-on), uso de paquetes de software e información en el proceso disciplinario (véase el inciso 8.2.3)).

Otra información

El conocimiento sobre seguridad, educación y actividades de entrenamiento deben ser de acuerdo y pertinentes al papel de la persona, las responsabilidades y habilidades deben incluir la información sobre las amenazas conocidas que permitan informar al consejo de seguridad superior a través de los caminos apropiados los eventos relacionados con la seguridad de información (véase el inciso 13.1).

Si se entrena para reforzar el conocimiento, permitirá a los individuos reconocer la seguridad de la información, los problemas y causas, y responder según las necesidades de su papel de trabajo.

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

12.2 Seguridad de las aplicaciones del sistema

OBJETIVO: Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones.

Se deberían diseñar dentro de las aplicaciones (incluidas las aplicaciones escritas por los usuarios) las medidas de control. Éstos deberían incluir la validación de los datos de entrada, el tratamiento interno y los datos de salida.

Se podrá requerir controles adicionales para sistemas que procesen o tengan impacto en información sensible, con mucho valor o críticas. Estos controles deben ser determinados en base a los requisitos de seguridad y la evaluación de riesgos.

12.6 Gestión de la vulnerabilidad técnica

OBJETIVO: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

La gestión de la vulnerabilidad técnica debe ser implementada de una manera efectiva, sistemática y respetable con medidas tomadas para confirmar su efectividad. Estas consideraciones deben incluir los sistemas operativos y otras aplicaciones en uso.

13. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE INFORMACIÓN

13.2 Gestión de las mejoras e incidentes en la seguridad de información

OBJETIVO: Asegurar un alcance consistente y efectivo aplicado a la gestión de incidentes en la seguridad de información.

Las responsabilidades y procedimientos deben establecerse para maniobrar los eventos y debilidades en la seguridad de información de una manera efectiva una vez que hayan sido reportados. Un proceso de mejora continua debe ser aplicado en respuesta al monitoreo, evaluación y gestión general de los incidentes en la seguridad de información.

Donde se requiera evidencia, esta debe ser recolectada para asegurar el cumplimiento de los requisitos legales.

14. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

Relacionaremos las principales medidas de seguridad directamente con las áreas del SIMTRAC y del COSAS - SARSAT, los controles y su implementación, tomando como base la NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008.

5. POLÍTICA DE SEGURIDAD

5.1 Política de seguridad de la información

OBJETIVO: Dirigir y dar soporte a la gestión de la seguridad de la información en concordancia con los requerimientos del negocio, las leyes y las regulaciones.

La gerencia debería establecer de forma clara las líneas de la política de actuación y manifestar su apoyo y compromiso a la seguridad de la información, publicando y manteniendo una política de seguridad en toda la organización.

5.1.1 Documento de política de seguridad de la información

Control

La gerencia debería aprobar, publicar y comunicar a todos los empleados, en la forma adecuada, un documento de política de seguridad de la información.

Debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento debería contener como mínimo la siguiente información:

a) una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información (véase el capítulo de Introducción).
b) el establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información.
c) un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión del riesgo.
d) una breve explicación de las políticas, principios, normas y requisitos de conformidad más importantes para la organización, por ejemplo:
1) conformidad con los requisitos legislativos y contractuales.
2) requisitos de formación en seguridad.
3) gestión de la continuidad del negocio.
4) consecuencias de las violaciones de la política de seguridad.
e) una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de la información, incluida la comunicación de las incidencias de seguridad.
f) las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta a todos los destinatarios en una forma que sea apropiada, entendible y accesible.

Otra información

La política de seguridad debe ser parte de un documento general de la política empresarial. Se debe tener cuidado al distribuir la política de seguridad fuera de la organización con el fin de no compartir información confidencial.

6. ASPECTOS ORGANIZATIVOS PARA LA SEGURIDAD

6.1 Organización interna

OBJETIVO: Gestionar la seguridad de la información dentro de la organización.

Debería establecerse una estructura de gestión para iniciar y controlar la implantación de la seguridad de la información dentro de la organización.

Es conveniente organizar foros de gestión adecuados con las gerencias para aprobar la política de seguridad de la información, asignar roles de seguridad y coordinar la implantación de la seguridad en toda la organización.

Si fuera necesario, debería facilitarse el acceso dentro de la organización a un equipo de consultores especializados en seguridad de la información. Deberían desarrollarse contactos con especialistas externos en seguridad para mantenerse al día en las tendencias de la industria, la evolución de las normas y los métodos de evaluación, así como tener un punto de enlace para tratar las incidencias de seguridad. Debería fomentarse un enfoque multidisciplinario de la seguridad de la información.

6.1.3 Asignación de responsabilidades sobre seguridad de la información

Control

Deberían definirse claramente las responsabilidades.

Guía de implementación

La asignación de responsabilidades sobre seguridad de la información deben hacerse en concordancia con la información de la política de seguridad (véase capítulo 4). Las responsabilidades para la protección de activos individuales y para llevar a cabo procesos de seguridad específicos deben ser claramente identificadas. Esta asignación, debería completarse, dónde sea necesario, con una guía más detallada para ubicaciones, sistemas o servicios específicos. Deberían definirse claramente las responsabilidades locales para activos físicos y de información individualizados y los procesos de seguridad como, por ejemplo, el plan de continuidad del negocio.

Los propietarios de los activos de información pueden delegar sus responsabilidades de seguridad en directivos a título individual o en proveedores de servicios. Sin embargo, el propietario sigue manteniendo la responsabilidad última sobre la seguridad del activo y debería estar capacitado para determinar que cualquier responsabilidad delegada se ha cumplido correctamente.

Es esencial que se establezcan claramente las áreas de las que cada directivo es responsable; en particular deberían establecerse las siguientes:

a) deberían identificarse claramente los activos y los procesos de seguridad asociados con cada sistema específico.
b) debería nombrarse al responsable de cada activo o proceso de seguridad, y deberían documentarse los detalles de esta responsabilidad.
c) deberían definirse y documentarse claramente los niveles de autorización.

Otra información

Muchas organizaciones nombran un director de seguridad de la información como el responsable del desarrollo e implantación de la seguridad y para dar soporte a la identificación de las medidas de control.

Sin embargo, la responsabilidad de proporcionar recursos e implantar las medidas de control suele recaer en ciertos directivos. Una práctica habitual consiste en designar un propietario de cada activo de información, que se convierte así en responsable de su seguridad cotidiana.

6.1.5 Acuerdos de confidencialidad

Control

Requerimientos de confidencialidad o acuerdos de no divulgación que reflejen las necesidades de la organización para la protección de información deben ser identificadas y revisadas regularmente.

Guía de implementación

Confidencialidad o acuerdos de no divulgación deben anexar los requerimientos para proteger información confidencial usando términos ejecutables legales. Para identificar requerimientos de confidencialidad o acuerdos de no divulgación, se deben considerar los siguientes elementos:

a) una definición de la información a ser protegida.
b) duración esperada del acuerdo, incluyendo casos donde la confidencialidad pueda necesitar ser mantenida indefinidamente.
c) acciones requeridas cuando un acuerdo sea finalizado.
d) responsabilidades y acciones de los signatarios para evitar acceso desautorizado a la información.
e) propiedad de la información, secretos del comercio y de la propiedad intelectual, y cómo esto se relaciona con la protección de la información confidencial.
f) la permisión de utilizar información confidencial y los derechos del signatario para usar la información.
g) el derecho de auditar y monitorear actividades que impliquen información confidencial.

h) procesos para notificar y reportar acceso desautorizado a aberturas de información confidencial.
i) términos para que la información sea retornada o destruida en la cesación del acuerdo.
j) acciones prevista que se tomará en caso de una abertura de este acuerdo.

Basado en los requerimientos de la seguridad de una organización, otros elementos pueden ser necesarios en una acuerdo de confidencialidad o de no-acceso.

Los acuerdos de confidencialidad y de no-acceso deben conformarse con todas las leyes aplicables y las regulaciones para la jurisdicción a la cual aplica (véase el inciso 15.1.1).

Los requerimientos para acuerdos de confidencialidad y de no-acceso deben ser revisados periódicamente y cuando ocurran cambios que influyan en estos requerimientos.

Otra información

Los acuerdos de confidencialidad y de no-acceso protegen información organizacional e informan a los signatarios de sus responsabilidades a proteger, usando y accediendo información de forma responsable y autorizada.

Puede ser necesario para una organización, usar diferentes formas de acuerdos de confidencialidad o de no-acceso en diferentes circunstancias.

7. CLASIFICACIÓN Y CONTROL DE ACTIVOS

7.1 Responsabilidad sobre los activos

OBJETIVO: Mantener una protección adecuada sobre los activos de la organización. Todos los activos deben ser considerados y tener un propietario asignado.

Deberían identificarse los propietarios para todos los activos importantes, y se debería asignar la responsabilidad del mantenimiento de los controles apropiados. La responsabilidad de la implantación de controles debería delegarse. Pero la responsabilidad debería mantenerse en el propietario designado del activo.

7.1.1 Inventario de activos

Control

Todos los activos deben se claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.

Guía de implementación

Una organización debe identificar todos los activos y la documentación de importancia de ellos. El inventario de activos debe incluir toda la información necesaria con el fin de recuperarse de un desastre, incluyendo el tipo de activo, formato, ubicación, información de respaldo, información de licencia y el valor dentro del negocio. El inventario no debe duplicar otros inventarios sin necesidad, pero debe estar seguro de que el contenido se encuentra alineado.

En adición, los propietarios (véase el inciso 7.1.2) y la clasificación de la información (véase el inciso 7.2) debe ser aceptada y documentada para cada uno de los activos. Basado en la importancia del activo, su valor dentro del

negocio y su clasificación de seguridad, se deben identificar niveles de protección conmensurados con la importancia de los activos.

Otra información

Existen muchos tipos de activos, incluyendo:

a) activos de información: archivos y bases de datos, documentación del sistema, manuales de los usuarios, material de formación, procedimientos operativos o de soporte, planes de continuidad, configuración del soporte de recuperación, información archivada.
b) activos de software: software de aplicación, software del sistema, herramientas y programas de desarrollo.
c) activos físicos: equipo de cómputo, equipo de comunicaciones, medios magnéticos (discos y cintas) u otro equipo técnico.
d) servicios: servicios de cómputo y comunicaciones, servicios generales (calefacción, alumbrado, energía, aire acondicionado).
e) personas, y sus calificaciones, habilidades y experiencia.
f) intangibles, como la reputación y la imagen organizacional.

Los inventarios de los activos ayudan a asegurar que se inicie su protección eficaz, pero también se requiere para otros propósitos de la organización, por razones de prevención laboral, pólizas de seguros o gestión financiera. El proceso de constituir el inventario de activos es un aspecto importante de la gestión de riesgos. Una organización tiene que poder identificar sus activos y su valor e importancia relativos (véase también la sección 4).

7.1.2 Propiedad de los activos

Control

Toda la información y los activos asociados con el proceso de información deben ser poseídos por una parte designada de la organización.

Guía de implementación

Los propietarios de los activos deben ser responsables por:

a) asegurar que la información y los activos asociados con las instalaciones de procesamiento de información son apropiadamente clasificadas.
b) definiendo y revisando periódicamente las restricciones de acceso y las clasificaciones, tomando en cuenta políticas de control aplicables.

La propiedad debe ser asignada a:

a) proceso de negocios
b) un conjunto definido de actividades
c) una paliación
d) un conjunto definido de datos

Otra información

Tareas de rutina pueden ser delegadas, como la de un custodio que se ocupa de un activo en una base diaria, pero la responsabilidad recae en el propietario.

En sistemas complejos de información, puede ser útil designar un grupo de activos que actúen juntos para proveer una función particular como services. En este caso, el propietario del servicio es responsable por la entrega del servicio, incluyendo la funcionalidad de los activos a los cual provee.

8. SEGURIDAD EN RECURSOS HUMANOS

8.1 Seguridad antes del empleo1

OBJETIVO: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades y que sean adecuados para los roles para los que han sido

considerados, reduciendo el riesgo de hurto, fraude o mal uso de las instalaciones.

Las responsabilidades de la seguridad se deben tratar antes del empleo en funciones adecuadas descritas y en términos y condiciones del empleo.

Todos los candidatos para empleo, contratistas y usuarios de terceros deben ser adecuadamente seleccionados, especialmente para trabajos sensibles.

Empleados, contratistas y terceros que utilizan las instalaciones del procesamiento de información deben firmar un acuerdo de confidencialidad.

8.1.1 Inclusión de la seguridad en las responsabilidades y funciones laborales

Control

Las funciones y responsabilidades de los empleados, contratistas y terceros deben ser definidas y documentadas en concordancia con la política de seguridad de la organización.

Guía de implementación

Las funciones de seguridad y las responsabilidades deben incluir los siguientes requisitos:

a) implementadas y realizadas en concordancia con la política de seguridad de la organización (véase el inciso 5.1).
b) deben proteger a los activos de un acceso no autorizado, modificación, destrucción o interferencia.
c) ejecutar procesos particulares o actividades.
d) asegurar que la responsabilidad sea asignada al individuo para tomar acciones.

e) reportar eventos de seguridad o eventos potenciales u otro riesgo de seguridad para la organización.

Las funciones de seguridad y la responsabilidad deben ser definidas y comunicadas claramente a los candidatos al trabajo durante el proceso de selección.

Otra información

Las descripciones de trabajo pueden ser usadas para documentar funciones de seguridad y responsabilidades. Las funciones de seguridad y las responsabilidades para individuos no relacionados con el proceso de selección de la organización, como por ejemplo los que se encuentran comprometidos a través de una organización de terceros, debe ser también claramente definida y comunicada.

9. SEGURIDAD FÍSICA Y DEL ENTORNO

9.1 Áreas seguras

OBJETIVO: Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización.

Los recursos para el tratamiento de información crítica o sensible para la organización deberían ubicarse en áreas seguras protegidas por un perímetro de seguridad definido, con barreras de seguridad y controles de entrada apropiados. Se debería dar protección física contra accesos no autorizados, daños e interferencias.

Dicha protección debería ser proporcional a los riesgos identificados.

9.1.1 Perímetro de seguridad física

Control

Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deben ser usados para proteger áreas que contengan información e recursos de procesamiento de información.

Guía de implementación

Las siguientes pautas deben ser consideradas e implementadas donde sea apropiado para los perímetros de seguridad físicos.

a) el perímetro de seguridad debería estar claramente definido y el lugar y fuerza de cada perímetro debe depender de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos;
b) el perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física (por ejemplo no tendrá zonas que puedan derribarse fácilmente). Los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados, por ejemplo, con mecanismos de control, alarmas, rejas, cierres, etc., las puertas y las ventanas deben ser cerradas con llave cuando estén desatendidas y la protección externa debe ser considerado para ventanas, particularmente al nivel del suelo;
c) se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería restringir sólo al personal autorizado;
d) las barreras físicas se deberían extender, si es necesario, desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno;
e) todas las puertas para incendios del perímetro de seguridad deberían tener alarma, ser monitoreadas y probadas en conjunción con

las paredes para establecer el nivel requerido de resistencia en concordancia con los estándares regionales, nacionales e internacionales apropiados; deben operar en concordancia con el código de fuego local como una forma de seguridad;

f) se debe instalar sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales y deben ser regularmente probados para cubrir todas las puertas externas y ventanas de acceso, las áreas no ocupadas deben tener una alarma todos el tiempo, también se debe cubrir otras áreas como las salas de computo o las salas de comunicación;
g) los recursos de procesamiento de información manejadas por la organización deben ser físicamente separadas de las que son manejadas por terceros.

Otra información

La protección física puede ser lograda creando una o más barreras físicas alrededor de las premisas de la organización y los recursos de procesamiento de información. El uso de múltiples barreras nos brinda protección adicional, donde la falla de una sola barrera no significa que la seguridad este inmediatamente comprometida.

Un área de seguridad puede ser una oficina cerrada o diversos espacios rodeados por una barrera continua de seguridad interna. Barreras adicionales y perímetros para controlar el acceso físico pueden ser necesarios entre áreas con requisitos de seguridad diferentes dentro del perímetro de seguridad.

Consideraciones especiales hacia la seguridad en el acceso físico deben ser dadas a edificios donde existan establecidas organizaciones múltiples.

10. GESTIÓN DE COMUNICACIONES Y OPERACIONES

10.3 Planificación y aceptación del sistema

OBJETIVO: Minimizar el riesgo de fallos de los sistemas.

Son necesarios una planificación y preparación para asegurar la disponibilidad de capacidad y de recursos adecuados para entregar el sistema de funcionamiento requerido.

Deberían realizarse proyecciones de los requisitos futuros de capacidad para reducir el riesgo de sobrecarga del sistema.

Se debería establecer, documentar y probar, antes de su aceptación, los requisitos operacionales de los sistemas nuevos.

10.3.1 Planificación de la capacidad

Control

El uso de recursos debe ser monitoreado y las proyecciones hechas de requisitos de capacidades adecuadas futuras para asegurar el sistema de funcionamiento requerido.

Guía de control

Para cada actividad que se esté llevando a cabo o para una actividad nueva, los requisitos de capacidad deben ser identificados. Se debe aplicar el monitoreo de los sistemas con el fin de asegurar, y donde sea necesario, mejorar la disponibilidad y la eficiencia de los sistemas. Controles de detección deben ser instalados pata detectar los problemas en un tiempo debido. Las proyecciones deberían tener en cuenta los requisitos de las nuevas actividades y sistemas, así como la tendencia actual y proyectada de tratamiento de la información en la organización.

Se requiere poner particular atención a cualquier recurso con tiempo de llegada largo o con costos altos; por esto, la gerencia debe monitorear la utilización de los recursos claves del sistema. Se deberían identificar las tendencias de uso, particularmente relativas a las aplicaciones del negocio o a las herramientas de administración de sistemas de información.

Los administradores deberían usar esta información para identificar y evitar los posibles cuellos de botella que puedan representar una amenaza a la seguridad del sistema o a los servicios al usuario, y para planificar la acción correctora apropiada.

10.6 Gestión de seguridad en redes

OBJETIVO: Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.

La gestión de la seguridad de las redes que cruzan las fronteras de la organización requiere una atención que se concreta en controles y medidas adicionales para proteger los datos sensibles que circulan por las redes públicas.

Controles adicionales pueden ser requeridos también con el fin de proteger información sensible pasando sobre redes públicas.

10.6.1 Controles de red

Control

Las redes deben ser manejadas y controladas adecuadamente para protegerse de amenazas y para mantener la seguridad en los sistemas y aplicaciones usando las redes, incluyendo información en tránsito.

Guía de Implementación

Los administradores de redes deberían implantar los controles y medidas requeridas para conseguir y conservar la seguridad de los datos en las redes de computadores, así como la protección de los servicios conectados contra accesos no autorizados. En particular, se deberían considerar los controles y medidas siguientes:

a) La responsabilidad operativa de las redes debería estar separada de la operación de los computadores si es necesario (véase el inciso 10.1.3).
b) Se deberían establecer responsabilidades y procedimientos para la gestión de los equipos remotos, incluyendo los de las áreas de los usuarios.
c) Se deberían establecer, si procede, controles y medidas especiales para salvaguardar la confidencialidad y la integridad de los datos que pasen a través de redes públicas, así como para proteger los sistemas conectados (véanse los incisos 11.4 y 12.3). También se deberían requerir controles y medidas especiales para mantener la disponibilidad de los servicios de las redes y de los computadores conectados.
d) Un registro y monitoreo apropiado debe ser aplicado para permitir el registro de acciones relevantes de seguridad.
e) Se deberían coordinar estrechamente las actividades de gestión tanto para optimizar el servicio al negocio como para asegurar que los controles y medidas se aplican coherentemente en toda la infraestructura de tratamiento de la información.

Otra Información

Información adicional en seguridad de redes puede ser encontrada en ISO/IEC 18028.

10.8 Intercambio de información

OBJETIVO: Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones

Se deberían realizar los intercambios sobre la base de acuerdos formales. Se deberían controlar los intercambios de información y software entre organizaciones, que deberían cumplir con toda la legislación correspondiente (véase el capítulo 15).

Se deberían establecer procedimientos y normas para proteger la información de los medios en tránsito.

10.8.4 Seguridad en la mensajería electrónica

Control

La información implicada con la mensajería electrónica debe ser protegida apropiadamente.

Guía de Implementación

Las consideraciones de seguridad para la mensajería electrónica deberían incluir lo siguiente:

a) protección de mensajes de accesos no autorizados, modificaciones o negación del servicio.
b) asegurar una dirección y un transporte correcto del mensaje.
c) confiabilidad y disponibilidad general del servicio.
d) consideraciones legales, por ejemplo los requisitos para firmas electrónicas.
e) obtención de aprobación antes de utilizar servicios externos públicos como mensajería instantánea o archivos compartidos.

f) niveles más fuertes de autentificación del acceso de control de redes públicas accesibles.

Otra Información

La mensajería electrónica como los correos, el intercambio electrónico de datos y la mensajería instantánea, juegan un papel importante en las comunicaciones de negocios. La mensajería electrónica tiene diferentes riesgos que las comunicaciones en papel.

11. CONTROL DE ACCESOS

11.1 Requisitos de negocio para el control de accesos

OBJETIVO: Controlar los accesos a la información.

Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad y negocio.

Se deberían tener en cuenta para ello las políticas de distribución de la información y de autorizaciones.

11.1.1 Política de control de accesos

Control

Una política de control de acceso debe ser establecida, documentada y revisada y debe estar basada en los requerimientos de seguridad y del negocio.

Guía de implementación

Se deberían establecer claramente en una política de accesos las reglas y los derechos de cada usuario o grupo de usuarios. Los controles de acceso son lógicos y físicos (véase el capítulo 9) y estos deben ser considerados juntos. Se

debería dar a los usuarios y proveedores de servicios una especificación clara de los requisitos de negocio cubiertos por los controles de accesos.

Esta política debería contemplar lo siguiente:

a) requisitos de seguridad de cada aplicación de negocio individualmente.
b) identificación de toda la información relativa a las aplicaciones y los riesgos que la información está enfrentando.
c) políticas para la distribución de la información y las autorizaciones (por ejemplo, el principio de suministro sólo de la información que se necesita conocer y los niveles de seguridad para la clasificación de dicha información) (véase el inciso 7.2).
d) coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes.
e) legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios (véase el inciso 15.1).
f) perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajos.
g) administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión.
h) segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos.
i) requerimientos para la autorización formal de los pedidos de acceso (véase el inciso 11.2.1).
j) requerimientos para la revisión periódica de los controles de acceso (véase el inciso 11.2.4).
k) retiro de los derechos de acceso (véase el inciso 8.3.3).

Otra Información

Al especificar las reglas de los controles de accesos se tendrá la precaución de considera:

a) la distinción entre reglas a cumplir siempre y reglas opcionales o condicionales.
b) el establecimiento de las reglas basándose en la premisa “está prohibido todo lo que no esté permitido explícitamente”, premisa que es contraria a la regla “está permitido todo lo que no esté prohibido explícitamente”, considerada más débil o más permisiva.
c) los cambios en las etiquetas de información (véase el inciso 7.2) iniciadas automáticamente por los recursos del tratamiento de la información y las que inicia el usuario manualmente.
d) los cambios en las autorizaciones al usuario realizados automáticamente por el sistema de información y los que realiza un administrador.
e) la distinción entre reglas que requieren o no la aprobación del administrador o de otra autoridad antes de su promulgación.

Las reglas de control de acceso deben ser apoyadas por procedimientos formales y por responsabilidades claramente definidos (véase, por ejemplo, 6.1.3, 11.3, 10.4.1, 11.6).

11.2 Gestión de acceso de usuarios

OBJETIVO: Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información.

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

Estos procedimientos deberían cubrir todas las etapas del ciclo de vida del acceso de los usuarios, desde el registro inicial de los nuevos hasta la baja del registro de los usuarios que ya no requieran dicho acceso a los sistemas y servicios. Se debería prestar especial atención, donde sea apropiado, al necesario control de la asignación de derechos de acceso privilegiados que permitan a ciertos usuarios evitar los controles del sistema.

11.2.1 Registro de usuarios

Control

Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.

Guía de Implementación

Se debería controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro que debería incluir:

a) la utilización de un identificador único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarles de sus acciones. Se debería permitir el uso de identificadores de grupo cuando sea conveniente para el desarrollo del trabajo y estos deben ser aprobados y documentados.
b) la comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información. También puede ser conveniente que la gerencia apruebe por separado los derechos de acceso.
c) verificación de la adecuación del nivel de acceso asignado al propósito del negocio (véase el inciso 11.1) y su consistencia con la política de seguridad de la organización (por ejemplo, su no contradicción con el principio de segregación de tareas (véase el inciso10.1.3).
d) la entrega a los usuarios de una relación escrita de sus derechos de acceso.
e) la petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso.
f) la garantía de que no se provea acceso al servicio hasta que se hayan completado los procedimientos de autorización.

g) el mantenimiento de un registro formalizado de todos los autorizados para usar el servicio.
h) la eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella.
i) la revisión periódica y eliminación de identificadores y cuentas de usuario redundantes (véase el inciso 11.2.4).
j) la garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.

Otra Información

Se debería considerar el establecimiento de roles de acceso a usuario basado en requisitos de negocio que resuman un numero de derechos de acceso en un expediente típico de acceso de usuario. Los pedidos y revisiones de acceso (véase el inciso 11.2.4) son manejadas más fácilmente al nivel de dichos roles que los niveles de derechos particulares.

Se debería considerar la inclusión de cláusulas en los contratos laborales y de servicio que especifiquen sanciones si sus signatarios realizan accesos no autorizados (véase el inciso 6.1.4 y 6.1.5).

12. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

12.5 Seguridad en los procesos de desarrollo y soporte

OBJETIVO: Mantener la seguridad del software de aplicación y la información. Se deberían controlar estrictamente los entornos del proyecto y de soporte.

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

12.5.4 Fuga de Información

Control

Las oportunidades de fuga de información deben ser prevenidas.

Guía de Implementación

Se debe considerar lo siguiente para limitar el riesgo de fuga de información, como por ejemplo a través del uso y explotación de canales cubiertos:

a) escaneo de medios de salida y comunicaciones para información oculta.
b) sistema de modulación y enmascarado, y el comportamiento de las comunicaciones para reducir la probabilidad de que un tercero sea capaz de deducir información desde dicho comportamiento.
c) haciendo uso de los sistemas y software que se consideran de alta integridad, por ejemplo productos evaluados (véase ISO/IEC 15408).
d) monitoreo regular de las actividades del personal y del sistema, donde sea permitido bajo la legislación o regulación existente.
e) monitoreo del uso de recursos en sistemas de cómputo.

Otra Información

Un canal encubierto son trayectorias que no tienen previsto conducir información, pero que sin embargo pueden existir en un sistema o red. Por ejemplo, la manipulación de bits en paquetes de protocolos de comunicación puede ser utilizada como un método oculto de señalar. Debido a su naturaleza, prevenir la existencia de todos los canales cubiertos posibles sería muy difícil, si no es imposible. De todas formas, la explotación de dichos canales es realizado frecuentemente por código Troyano (véase también 10.4.1). Tomando medidas para protegernos contra códigos troyanos, reduce el riesgo de la explotación del canal cubierto.

La prevención de acceso a red no autorizado (véase el inciso 11.4), así como las políticas o procedimientos para que desaliente el mal uso de los servicios de información por parte del personal (véase el inciso 15.1.5), ayudara a protegernos contra canales cubiertos.

14. GESTIÓN DE CONTINUIDAD DEL NEGOCIO

14.1 Aspectos de la gestión de continuidad del negocio

OBJETIVO: Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.

Se debería implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de seguridad (que, por ejemplo, puedan resultar de desastres naturales, accidentes, fallas de equipos o acciones deliberadas) mediante una combinación de controles preventivos y de recuperación. Este proceso debe identificar los procesos críticos de negocio e integrar los requisitos de gestión de la seguridad de información para la continuidad del negocio con otros requisitos de continuidad relacionados con dichos aspectos como operaciones, proveedores de personal, materiales, transporte e instalaciones.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio. Se deberían desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales. La seguridad de información debe ser una parte integral del plan general de continuidad del negocio y de los demás procesos de gestión dentro de la organización.

La gestión de la continuidad del negocio debería incluir en adición al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar

las consecuencias de incidencias dañinas y asegurar la reanudación, a tiempo, de las operaciones esenciales.

14.1.2 Continuidad del negocio y evaluación de riesgos

Control

Los eventos que pueden causar interrupciones a los procesos de negocio deben ser identificados, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de información.

Guía de Implementación

El estudio para la continuidad del negocio debería empezar por la identificación de los eventos (o secuencia de eventos) que pueden causar interrupciones en los procesos de negocio, por ejemplo, una falla del equipo, una inundación o un incendio. Se debería continuar con una evaluación del riesgo para determinar la probabilidad e impacto de dichas interrupciones (en términos tanto de escala de daños como de periodo de recuperación).

La evaluación del riesgo de continuidad de negocio debe ser llevada a cabo con una total implicancia por parte de los propietarios de los recursos y procesos de negocio. Debería considerar todos los procesos del negocio sin limitarse a los dispositivos informáticos, pero debe incluir los resultados específicos para la seguridad de información. Es importante vincular los diferentes aspectos de riesgos para obtener una figura completa de los requerimientos de continuidad de negocio de la organización. La evaluación debe identificar, cuantificar y priorizar los riesgos contra criterios y objetivos relevantes para la organización incluyendo recursos críticos, impactos de las interrupciones, tiempos permisibles de interrupción y prioridades de recuperación.

Se debería desarrollar un plan estratégico para determinar un enfoque global de la continuidad del negocio a partir de los resultados de la evaluación del riesgo. Una vez creada la estrategia, la gerencia deberá respaldarla y crear un plan para implementar dicha estrategia.

9.7 Anexo G

Cuadro Inventario de Activos de Información

INVETARIO DE ACTIVOS DE INFORMACIÓN							
PROCESO	IDENTIFICACIÓN DE ACTIVO	TIPO DE ACTIVO	PROPIETARIO O RESPONSABLE	UBICACIÓN	C	I	D

Tabla 72: Inventario de Activos de Información

Fuente: Elaborado por los Autores

Leyenda de Confidencialidad, Integridad y Disponibilidad

C:	Confidencialidad
I:	Integridad
D:	Disponibilidad

Tabla 73: Leyenda C, I y D

Fuente: Elaborado por los Autores

9.8 Anexo H

Cálculo de Indicadores

CÁLCULO DE INDICADORES	
Riesgo a Controlar	Indicador
No existen políticas de seguridad	núm. personal que conoce las políticas S.I. / total de personal de las áreas
	Cálculo: - Total de empleados = 95 - Meta: 80% = 76 - Personas que conocen las políticas de seguridad: 67 - Logro: X = (67 / 95)*100% - Logro: X = 70%
No hay un responsable de las áreas vulnerables	núm. usuarios que cumplen las políticas S.I. / total de usuarios de las áreas
	Cálculo: - Total de usuarios = 47 - Meta: 100% = 47 - Usuarios que cumplen con las políticas de seguridad: 33 - Logro: X = (33 / 47)*100% - Logro: X = 70%
No hay acuerdos de confidencialidad internas	núm. personal que firma acuerdos / total de acuerdos
	Cálculo: - Total de acuerdos = 50 - Meta: 80% = 40 - Personal comprometida con los acuerdos firmados: 40 - Logro: X = (40 / 50)*100% - Logro: X = 80%
No hay seguridad para los activos	núm. de activos vulnerables / total de activos
	Cálculo: - Total de activos de información = 38 - Meta: 100% = 38 - cantidad de activos vulnerables: 38 - Logro: X = (38 / 38)*100% - Logro: X = 100%
	núm. de activos sin seguridad / total de activos
	Cálculo: - Total de activos de información = 38 - Meta: 100% = 38 - cantidad de activos sin seguridad: 38 - Logro: X = (38 / 38)*100% - Logro: X = 100%
	núm. de activos con propietarios / total de activos

CÁLCULO DE INDICADORES	
Riesgo a Controlar	Indicador
	Cálculo: - Total de activos de información = 38 - Meta: 100% = 38 - cantidad de activos con propietarios: 38 - Logro: X = (38 / 38)*100% - Logro: X = 100%
No están delimitados los roles del personal	funciones realizadas por el usuario / total de usuarios
	Cálculo: - Total de usuarios = 47 - Meta: 100% = 47 - Usuarios que realizan funciones asignadas (roles): 38 - Logro: X = (38 / 47)*100% - Logro: X = 80%
No hay seguridad en la red	equipos de TI autorizados / equipos de TI no autorizados
	Cálculo: - Total de equipos TI no autorizados = 38 - Meta: 100% = 38 - equipos de TI autorizados: 31 - Logro: X = (31 / 38)*100% - Logro: X = 80%
	mensajería spam actual / total de spam
	Cálculo: - Total de mensajes con spam = 15048 - Meta: 100% = 15048 - mensajes con spam actual : 9029 - Logro: X = (9029 / 15048)*100% - Logro: X = 60%
	num de visitantes no autorizados / total de visitantes
	Cálculo: - Total de visitantes = 504 - Meta: 100% = 504 - visitantes no autorizados : 353 - Logro: X = (353 / 504)*100% - Logro: X = 70%
No se toman en cuenta las políticas de acceso a las áreas vulnerables	num de ingreso del personal autorizado / el total de personas ingresantes
	Cálculo: - Total personal ingresantes = 47 usuarios + 13 usuarios extraordinarios = 60 - Meta: 100% = 60 - num personal autorizado : 57 - Logro: X = (57 / 60)*100% - Logro: X = 97%

CÁLCULO DE INDICADORES	
Riesgo a Controlar	Indicador
No hay un control de usuarios	acceso usuario en su guardia / tiempo total de acceso por día
	Cálculo: - Total de acceso por día (horas) = 8 - Meta: 100% (horas) = 8 - Usuarios que cumplen su guardia (horas): 8 - Logro: X = (8 / 8)*100% - Logro: X = 100%
Fuga de información	nivel de seguridad de los documentos / num total de documentos
	Cálculo: - Total de documentos = 9125 - Meta: 100% - nivel de seguridad de los documentos = 9125 - Logro: X = (9125 / 9125)*100% - Logro: X = 100%
	nivel de seguridad de los sistemas / num total de sistemas
	Cálculo: - Total de sistemas = 15 - Meta: 100% - nivel de seguridad de los sistemas = 14 - Logro: X = (14 / 15)*100% - Logro: X = 95%
	nivel de seguridad de usuario / num total de usuarios
	Cálculo: - Total de usuarios = 47 - Meta: 100% - nivel de seguridad de usuarios = 47 - Logro: X = (47 / 47)*100% - Logro: X = 100%
No existe un plan de continuidad de negocio	num de incidentes / num total de incidentes
	Cálculo: - Total de incidentes = 26 - num de incidentes = - Logro: X = (13 / 26)*100% - Logro: X = 50%

Tabla 74: Calculo de los Indicadores

Fuente: Elaborado por los Autores