FACULTAD DE INGENIERÍA

CARRERA PROFESIONAL DE INGENIERÍA DE SISTEMAS

INFORME DE SUFICIENCIA PROFESIONAL

"IMPLEMENTACIÓN DE LA NTP ISO/IEC 27001:2014 PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN DE LA AUTORIDAD PORTUARIA NACIONAL, CALLAO - 2017"

PARA OBTENER EL TÍTULO DE

INGENIERO DE SISTEMAS

AUTOR

JOSHIMAR JAPHET CASTRO SIGUAS

ASESOR

ING. RAMON JOHNY PRETELL CRUZADO

LIMA, PERÚ, JULIO DE 2018

DEDICATORIA

A mis padres, por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más. A mis profesores, gracias por su tiempo, por su apoyo, así como por la sabiduría que me transmitieron en el desarrollo de mi formación profesional.

AGRADECIMIENTO

Agradezco a Dios por protegerme durante todo mi camino y darme fuerzas para superar obstáculos y dificultades a lo largo de toda mi vida.

A Naysha, por acompañarme durante todo este arduo camino y compartir conmigo alegrías y fracasos.

Al Ing. Johny Pretell, profesor de la carrera de Ingeniería de Sistemas, por su valiosa guía y asesoramiento a la realización de este informe.

Gracias a todas las personas que ayudaron directa e indirectamente en la realización de este proyecto.

RESUMEN

El proyecto descrito en el presente documento tuvo como objetivo la Implementación de la NTP ISO/IEC 27001:2014, para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional, para su realización se aplicó la Norma Técnica Peruana ISO/IEC 27001:2014, la cual estuvo dividido en 3 etapas y tuvo como alcance los procesos de REDENAVES, Gestión de Licencias y Gestión de los Sistemas de Información en su sede central ubicado en el Callao.

Los resultados que se obtuvieron permitieron determinar de forma real que, al implementar la Norma Técnica Peruana ISO/IEC 27001:2014, se obtuvo un mayor nivel de uso de documentos tales como procedimientos, política y otros, que favorecieron a la institución para descubrir las irregularidades en la seguridad de la información plasmado en varios métodos de seguridad para resguardarla. Así mismo, el Plan de Tratamiento de Riesgos, posibilitó la reducción de los niveles de riesgos de los activos de información, respecto a las amenazas y vulnerabilidades en la institución, esto plasmado en una metodología para mitigarlos a través de actividades y poder minimizar los impactos a los activos de información. Finalmente, con el Plan de Capacitación y Concientización se logró incrementar la conciencia en temas relacionados a seguridad de la información y se impulsó al personal a comprometerse a resguardar su información y mitigar riesgos en favor de la institución.

Palabras clave: Riesgos, amenaza, vulnerabilidad, NTP ISO/IEC 27001:2014, ISO 27002, Sistemas de Información.

ABSTRACT

The project described in this document was aimed at the implementation of the NTP ISO / IEC 27001: 2014, to improve the management of security in the information systems of the National Port Authority, for its implementation the ISO Peruvian Technical Standard was applied. / IEC 27001: 2014, which was divided into 3 stages and had the scope of the processes of REDENAVES, Licensing Management and Information Systems Management at its headquarters located in Callao.

The results that were obtained allowed to determine in a real way that, when implementing the Peruvian Technical Standard ISO / IEC 27001: 2014, a higher level of use of documents such as procedures, politics and others was obtained, which favored the institution to discover the irregularities in the security of information embodied in various security methods to protect it. Likewise, the Risk Treatment Plan enabled the reduction of risk levels of information assets, with respect to threats and vulnerabilities in the institution, this reflected in a methodology to mitigate them through activities and to minimize the impacts to information assets. Finally, with the Training and Awareness Plan, awareness was raised on issues related to information security and staff were encouraged to commit to safeguarding their information and mitigating risks in favor of the institution.

Keywords: Risks, threat, vulnerability, NTP ISO / IEC 27001: 2014, ISO 27002, Information Systems.

ÍNDICE DE CONTENIDO

CAPÍTULO II. MARCO TEÓRICO

CAPÍTULO III. DESARROLLO DEL PROYECTO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Este proyecto tuvo como propósito, implementar la NTP ISO/IEC 27001:2014 Sistema de Gestión de Seguridad de la Información, en cumplimiento de la Resolución Ministerial N° 004-2016-PCM, referido a la obligación de la implementación de la mencionada norma en las instituciones pertenecientes al sector informático del estado. Esta Norma Técnica, se implementó en la Autoridad Portuaria Nacional, entidad dedicada a la promoción del sector portuario en el país.

La seguridad de la información, se entiende cómo aquellas técnicas preventivas que las organizaciones adquieren para resguardar y proteger sus activos de información, para mantener la confidencialidad, integridad y disponibilidad de los mismos.

Por lo tanto, la principal característica del Sistema de Gestión de Seguridad de la Información es mantener la disponibilidad, confidencialidad, integridad de los activos de información, en donde debe realizarse una gestión de riesgos a los activos de los procesos core, dando lugar a implantar controles de seguridad que mitigarán posibles riesgos que afecten a dichos activos.

Es por ello, que la Autoridad Portuaria Nacional en cumplimiento a la Resolución Ministerial de la Presidencia del Consejo de Ministros, decide implantar controles, procedimientos y políticas de seguridad para asegurar la disponibilidad, integridad y confidencialidad de la información; asegurando que el acceso a la información se realice por personal autorizado para su uso, se encuentre apto y permanezca de tal forma que no pueda ser editada.

Este documento a fin de dar una clara descripción del proyecto se ha dividido en cuatro capítulos: El capítulo I, muestra el diagnóstico inicial, la justificación, los objetivos, la participación del bachiller y la descripción del proyecto. El capítulo II, describe las bases conceptuales y teóricas relacionadas al Sistema de Gestión de Seguridad de la Información. El capítulo III, presenta el desarrollo del proyecto, la metodología aplicada y las etapas de organización, planificación, despliegue del proyecto, control y seguimiento y cierre del proyecto. Finalmente, el capítulo IV, plantea las conclusiones y recomendaciones para futuros proyectos de similar naturaleza.

CAPÍTULO I

ASPECTOS GENERALES DEL PROYECTO

1.1 Diagnóstico Inicial

1.1.1 Antecedentes

El 1 de marzo del 2003 fue promulgada la Ley N° 27943, Ley del Sistema Portuario Nacional, cuya finalidad es promover el desarrollo y la competitividad de los puertos, facilitar el transporte multimodal, modernizar los puertos y desarrollar las cadenas logísticas que existen en los terminales portuarios. (Nacional, Oficina de Tecnologías de la Información, 2016)

La ley del Sistema Portuario Nacional (LSPN) creó a la Autoridad Portuaria Nacional como una institución pública del tipo Organismos Técnico Especializado, quien se encarga del desarrollo del Sistema Portuario Nacional, se encuentra adscrita al Ministerio de Transportes y Comunicaciones (MTC) dependiendo del ministro, de derecho público interno patrimonio propio, y con autonomía administrativa, facultades normadas por delegación del Ministerio de Transportes y Comunicaciones. (Nacional, Oficina de Tecnologías de la Información, 2016)

La Autoridad Portuaria Nacional se encuentra encargada del desarrollo del Sistema Portuario Nacional, fomentando la inversión privada de los puertos a nivel nacional, tiene como objetivo establecer y conformar una sólida comunidad marítimo – portuaria enlazando a los agentes de desarrollo marítimo – portuario, que establecen un objetivo común: el fortalecimiento de la competitividad de los puertos nacional frente al fenómeno al fenómeno de la globalización y a los retos planteados por la necesidad de desarrollar a plenitud su sector exportador. (Nacional, Oficina de Tecnologías de la Información, 2016)

Asimismo, la Autoridad Portuaria Nacional se encuentra certificada en ISO 9001:2015 en los procesos de: Gestión de Licencias, REDENAVES (Recepción y Despacho de Naves), Control y Fiscalización, Atención al usuario y Gestión Documentaria.

Figura 1. Certificación en ISO 9001:2015 Autoridad Portuaria Nacional (2018).

Misión

Conducir el Sistema Portuario Nacional, planificando, promoviendo, normando y supervisando su desarrollo, con el fin de lograr su competitividad y sostenibilidad. (Nacional, Misión, 2016)

Visión

Ser reconocida como la institución líder en la conducción del desarrollo del SPN. (Nacional, Misión, 2016)

Valores

- Liderazgo y autoridad.
- Eficiencia y calidad.
- Ética y transparencia.
- Trabajo en equipo.
- Responsabilidad Social,
- Compromiso.

Oficina de Tecnologías de la Información

La oficina de Tecnologías de la Información es un órgano de apoyo dependiente de la Gerencia General encargada de diseñar, planificar, coordinar y ejecutar las actividades relacionadas con la tecnología de la información y estadística de la institución. (Nacional, Oficina de Tecnologías de la Información, 2016)

Entre sus funciones están las siguientes:

- Planificar, organizar, coordinar, ejecutar, supervisar y evaluar las actividades relacionadas a las tecnologías de la información y sistemas de información, las cuales estén enmarcadas en los planes institucionales. (Nacional, Oficina de Tecnologías de la Información, 2016)
- Formular y actualizar los Planes de Seguridad de Información y los Planes de Continuidad y Recuperación ante Desastres, así como supervisar la implementación de las políticas, procedimientos y recomendaciones

asociadas a la seguridad de información y riesgos en tecnologías de la información. (Nacional, Oficina de Tecnologías de la Información, 2016)

- Identificar, actualizar, estandarizar y optimizar los procesos instituciones en coordinación con las unidades orgánicas, para lograr su eficiencia. (Nacional, Oficina de Tecnologías de la Información, 2016)
- Brindar el soporte técnico oportuno a todas las dependencias de la institución. (Nacional, Oficina de Tecnologías de la Información, 2016)
- Promover el uso de Tecnologías de la Información en la APN y el SPN. (Nacional, Oficina de Tecnologías de la Información, 2016)
- Administrar y controlar el equipamiento informático, de comunicaciones y licencias de software, así como la racionalización de su uso de acuerdo a los objetivos de la institución. (Nacional, Oficina de Tecnologías de la Información, 2016)
- Formular y controlar la ejecución del Plan Anual Operativo Informático. (Nacional, Oficina de Tecnologías de la Información, 2016)

1.1.2 Planteamiento del Problema

El gestionar un Sistema de Gestión de Seguridad de la Información en una organización no es muy compleja si es asociado a lo técnico, el problema surge cuando se le da un punto de vista organizativo, es por ello, qué se deben adoptar buenas prácticas relacionadas a la seguridad de la información que ayudan a eliminar posibles riesgos que afecten a los activos de información vulnerando su disponibilidad, integridad y confidencialidad, según el informe de PWC en el año 2017, indicó que en América del Sur, el 72% de las empresas están utilizando servicios de seguridad gestionadas para la ciberseguridad y privacidad, al realizarse un diagnóstico inicial en la Autoridad Portuaria Nacional respecto al cumplimiento de la ISO 27001:2013, el resultado fue que los usuarios no estaban concientizados en temas de seguridad de la información, la institución desconocía los riesgos de seguridad a los que estaban expuestos, es por ello, que de acuerdo a la resolución ministerial N° 004-2016-PCM aprobado el 08 de enero de 2016 con apoyo de la Secretaria de Gobierno Digital (SeGDi) antes ONGEI (Oficina Nacional de Gobierno Electrónico e Informática), se decide implementar la NTP ISO/IEC 27001:2014 aprobado bajo memorando N° 152-2015-PCM/ONGEI el cual

recomienda la aplicación y uso de la norma mencionada a todas las instituciones integrantes del sector informático en un plazo de 2 años, con el objetivo de crear un programa de seguridad de la información para mantener la confidencialidad, integridad y disponibilidad de la información.

1.1.3 Usuarios finales del Proyecto

- Jefe de TI.
- Oficial de Seguridad de la Información.
- Usuarios de todas las áreas.
- Comité de Seguridad de la Información.

1.2 Justificación

Debido a la implementación del Sistema de Gestión de Seguridad de la Información se dio cumplimiento a la Resolución Ministerial N° 004-2016 PCM que indica que “las instituciones pertenecientes al sector informático deben implementar la NTP ISO/IEC 27001:2014” “Tecnologías de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requisitos”. Cabe resaltar que, si la institución no cumple con dicha resolución, se vería expuesta a una serie de multas por parte del ente regulador, y al realizar las auditorías internas como lo indica la norma en su requisito 9.2 “Auditorías internas”, la institución se vería expuesta a una serie de riesgos asociados a sus activos de información.

En conjunto con lo antes mencionado, dicha institución obtuvo algunas otras ventajas importantes:

- **Conveniencia**

  Al implementar la NTP ISO/IEC 27001:2014, permitió disminuir significativamente los riesgos que puedan afectar el desarrollo del negocio, la competitividad y rentabilidad asociado a los objetivos planteados por la institución.

- **Implicaciones prácticas**

  Se mejoraron los conocimientos de los usuarios en seguridad de la información a través de capacitaciones in house y clases virtuales, así mismo, se desarrollaron políticas, procedimientos y formatos que ayudaron a prevenir la fuga de información y generación de evidencias.

1.3 Objetivos

1.3.1 Objetivo General

Implementar la NTP ISO/IEC 27001:2014, para mejorar la gestión de la seguridad en los sistemas de información de la Autoridad Portuaria Nacional.

1.3.2 Objetivos Específicos

- Establecer un marco de gestión de la seguridad de la información claro y estructurado.
- Cumplir con la Resolución Ministerial N° 004-2016-PCM.
- Identificar y mitigar riesgos de seguridad de la información a los que se encuentran expuestos los procesos que forman parte del alcance.
- Identificar cíclicamente las debilidades de seguridad y las áreas a mejorar, a través de la ejecución de auditorías al SGSI.
- Incrementar las capacidades y habilidades de la Gestión de la Seguridad de la Información y sus mejores prácticas, del personal a cargo de esta gestión, mediante talleres de capacitación.

1.4 Participación del Bachiller en el Proyecto

El bachiller durante el proyecto ha desempeñado sus funciones laborando en la oficina de tecnologías de información de la Autoridad Portuaria Nacional (véase Figura 2).

1.4.1 Funciones del Bachiller en el Proyecto

- Apoyo en la elaboración de procedimientos, política, instructiva y directiva de TI.
- Apoyo en la implementación del SGSI.

- Apoyo en el registro de la normatividad en el banco de normas informáticas.
- Apoyo en registro de avance de actividades para los indicadores de gestión del plan operativo informático.

1.4.2 Aporte del Bachiller en el Proyecto

- Participación en la elaboración y/o actualización de los documentos del SGSI en todas las fases del proyecto.
- Participación en la difusión del SGSI mediante capacitaciones al personal.
- Participación en la elaboración de los proyectos de resolución de gerencial general y resoluciones de presidencia de directorio para la aprobación del comité de seguridad y para la aprobación de documentos del SGSI que una vez aprobados se publicaron en la intranet.
- Se apoyó en la realización de indicadores para el Plan Estratégico de Tecnologías de la Información (PETI) de la Oficina de Tecnologías de la Información.

1.4.3 Organigrama de la Institución

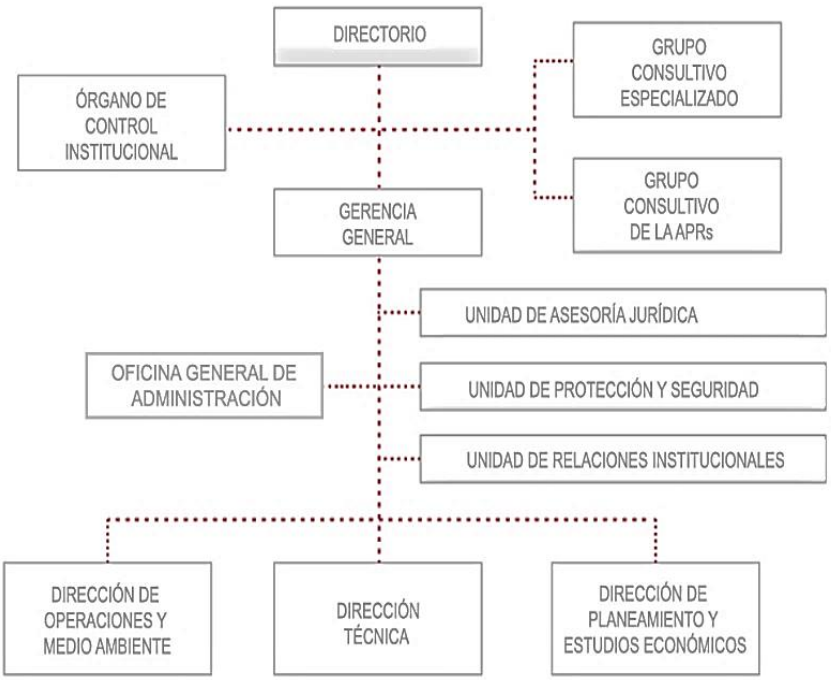


Figura 2. Organigrama de la Autoridad Portuaria Nacional – Autoridad Portuaria Nacional (2017).

La oficina del Tecnologías de información se encuentra dentro de la Oficina General de Administración como un área de apoyo.

1.4.4 Organización del Proyecto

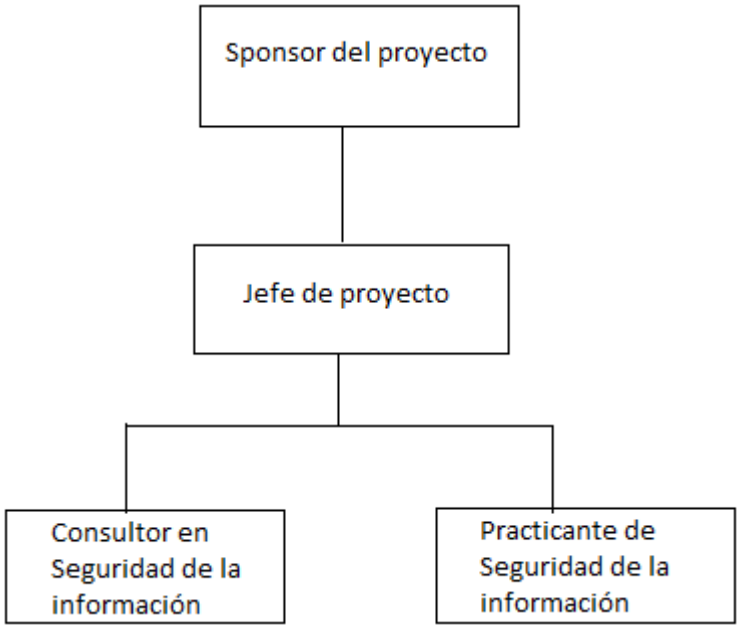


Figura 3. Organización del proyecto “Implementación de la NTP ISO/IEC 27001:2014”. Adaptado del Acta de Inicio del proyecto (2017).

1.5 Descripción del Proyecto

1.5.1 Enfoque del Proyecto

El proyecto estuvo enfocado a la Implementación de la NTP ISO/IEC 27001:2014 para mejorar la Gestión de la Seguridad en los Sistemas de Información de la Autoridad Portuaria Nacional.

1.5.2 Alcance del Proyecto

A continuación, se detalla el alcance del proyecto implementado, que está divido en 3 Fases:

Fase I – Organización del Proyecto.

Fase II – Planificación del SGSI.

Fase II – Despliegue del SGSI.

1.5.3 Entregables del Proyecto

- Formatos del Sistema de Gestión de Seguridad de la Información.
- Documentos externos que son requisitos de la NTP ISO/IEC 27001:2014.
- Manuales
  - Manual de Sistema de Gestión de Seguridad de la Información.
  - Manual de Funciones y Responsabilidades del SGSI.
  - Manual de Indicadores del SGSI.
- Metodología de Gestión de Riesgos y Oportunidades.
- Políticas:
  - Política de Seguridad de la Información.
  - Política de Seguridad Física y del Ambiente.
  - Política de Seguridad de las Operaciones.
  - Política de Seguridad de las Comunicaciones.
  - Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.
  - Política de Relaciones con los Proveedores.
  - Política de Cumplimiento.
  - Política de Gestión de Incidentes de Seguridad de la Información.
  - Política de Seguridad Ligada a los RRHH.
  - Política de Gestión de Activos.
  - Política de Control de Accesos.
  - Política de Organización de la Seguridad de la Información.
- Procedimientos:
  - Procedimiento de Inventario de Activos.
  - Procedimientos de Gestión de Cumplimiento.
  - Procedimiento de Relación con Proveedores.
  - Procedimiento de Creación y Actualización de Información Documental del SGSI.
  - Procedimiento de Control de Información Documental del SGSI.
  - Procedimiento de Seguridad y Correcto Uso de las Instalaciones.
  - Procedimiento de Gestión de Cambios.
  - Procedimiento de Mantenimiento de Equipos.
  - Procedimiento de Respaldo de Información.
  - Procedimiento de Gestión de Incidentes.

- Procedimiento de Seguridad de las Comunicaciones.

- Resoluciones:
  - Resolución de Acuerdo de Directorio – Modificación del Comité de Seguridad de la Información.
  - Resolución de Gerencia General – Aprobación de los documentos del SGSI.

1.5.4 Cronograma del Proyecto

El proyecto tuvo una duración de 8 meses calendario y las actividades se describen en el (Anexo 1 - Cronograma del Proyecto).

1.5.5 Dificultades del Proyecto

Durante la planificación y la ejecución del proyecto se presentaron las siguientes dificultades:

- Resistencia al cambio por parte de los usuarios al uso de nuevas políticas y procedimientos implementados por la Norma.
- Falta de compromiso por parte del Comité del SGSI para la aprobación y difusión de los documentos desarrollados por la Norma.
- Demora en la realización de las capacitaciones por inasistencias por parte de los usuarios de la entidad.
- Falta de conocimiento por parte de las personas integrantes del desarrollo del proyecto.

CAPÍTULO II

MARCO TEÓRICO

2.1 Sistemas de Información

Existen varios significados de sistemas de información que ponen énfasis en alguno de sus componentes desde el punto de vista de Sistemas, así por ejemplo para Alejandro Peña, citado en (Miranda, 2012), los sistemas de información representan conjuntos de elementos interrelacionados que responden a las demandas de información de una organización, convirtiéndose herramientas de apoyo para la toma de decisiones y el desarrollo de acciones en la organización.

Según Jane y Kenneth, (Citado en Miranda, 2012), un sistema de información se define como:

> Un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Teniendo muy en cuenta el equipo computacional necesario para que el sistema de información pueda operar y el recurso humano que interactúa con el Sistema de Información, el cual está formado por las personas que utilizan el sistema. (párr. 1)

También Manuel Peralta define, “Un sistema de información (SI) es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listo para su uso posterior, generados para cubrir una necesidad u objetivo” (Miranda, 2012, párr.1).

2.1.1 Estructura de un Sistema de Información

Según Sánchez, “Los elementos que conforman un sistema de información automatizado son: datos, información, personas, procedimientos, hardware y red de comunicaciones y software” (Izamorar, 2017, párr. 1).

Datos: “se define como hechos que deben estar registrados en una base de datos informatizada” (Izamorar, 2017, párr. 1).

Información: “se define al conjunto de datos que han sido debidamente procesados haciendo uso de algún software, en donde el resultado obtenido de este proceso es beneficioso para poder tomar una buena decisión” (Izamorar, 2017, párr. 1)

Personas: “se refiere al grupo de personas que tienen el rol de usuarios directos e indirectos (llamados también usuarios finales, son lo que reciben informes y resultados)” (Izamorar, 2017, párr. 1)

Procedimientos: Se refiere a aquellos procesos de un sistema de información que se encuentran documentados, indicando de qué manera debe realizarse, Para el caso de los sistemas de información se incluyen los manuales de usuario y documentos que detallen las tareas que deben realizar todas las personas involucradas en el sistema (Izamorar, 2017, párr. 1)

Hardware y Red de comunicaciones: “este componente consiste en tener implementado el equipo necesario para el funcionamiento de los sistemas de información, como ordenadores, impresoras, etc., Así como los dispositivos necesarios para el intercambio de información entre diferentes ordenadores” (Izamorar, 2017, párr. 1)

Software: consiste tanto en el software del sistema, que controla el funcionamiento del hardware (sistemas operativos, software de comunicaciones, utilidades, etc.) como en el software de la aplicación, que consiste en todos los programas directamente relacionados con los procesos de datos del sistema de información que estamos considerando. (Izamorar, 2017, párr. 1)

.

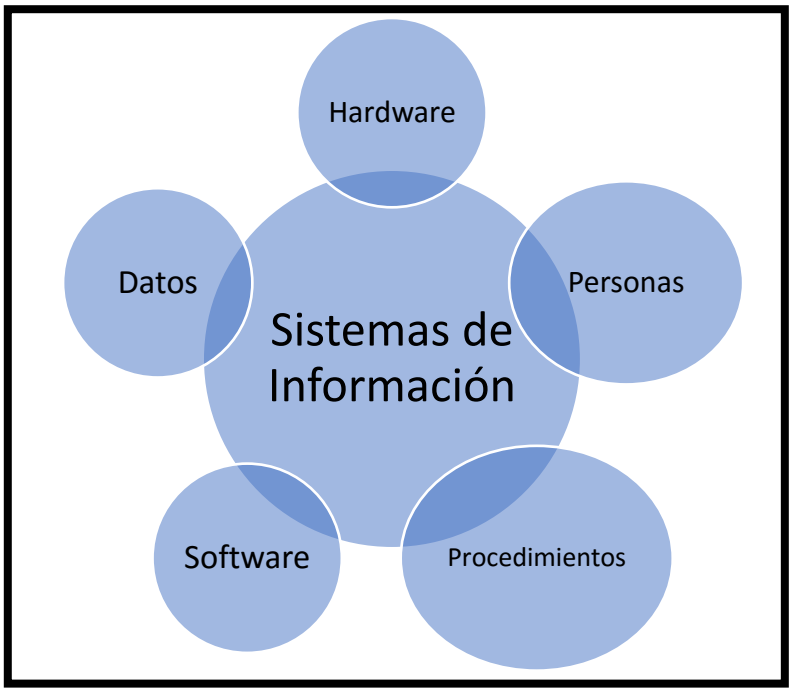


Figura 4. Estructura de un Sistema de Información. Adaptado de Descripción de los Sistemas de Información (2015).

2.2 Seguridad de la Información

En la actualidad existen diferentes tipos de definiciones sobre seguridad de la información que se basan en los resultados de su implementación y en asegurar los activos de una organización, por ejemplo, para Nuhad Ponce (s.f.), Seguridad de la Información tiene como objetivo asegurar la protección de los datos para mitigar su extravío y que no sufran alteraciones no autorizada. Dichas técnicas deben asegurar en primer lugar la confidencialidad, integridad y disponibilidad de los datos. La seguridad de la Información debe conformarse de controles, políticas, procedimientos, concientización y capacitación que aseguren que en la organización se tomen las precauciones necesarias para preservar los elementos de la información.

La norma ISO 27000 define a la seguridad, disponibilidad, integridad y confidencialidad de la información de la siguiente manera:

- La seguridad de Información “es la preservación de la confidencialidad, integridad y disponibilidad de la información” (ISO 27000, 2012, párr. 17).

- La disponibilidad es la “Propiedad de la información que debe estar accesible y utilizable cuando lo requiera una entidad autorizada” (ISO 27000, 2012, párr. 13).

- La Integridad es la “Propiedad de la información relativa a su exactitud y completitud” (ISO 27000, 2012, párr. 23).

- La Confidencialidad es la “Propiedad de la información que debe ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados” (ISO 27000, 2012, párr. 21).

2.2.1 Tipos de Seguridad

La tipificación de seguridad va a depender del tipo de activo que se quiere proteger, es decir, los recursos del sistema de información que son obligatorios para el funcionamiento de la organización de forma correcta, se pueden identificar

tipos de seguridad como, seguridad física y lógica, seguridad pasiva y activa (C Seaoane, 2010, párr. 2).

Los tipos de seguridad antes mencionados se describen como:

- “Seguridad física: es aquella que trata de proteger el hardware (los equipos informáticos, el cableado, etc.) de los posibles desastres naturales (terremotos, tifones, etc.) de incendios, inundaciones, sobrecargas eléctricas, de robos y demás amenazas” (C Seaoane, 2010, párr. 2).

- “Seguridad lógica: complemento de la seguridad física, protegiendo el software los equipos informáticos, es decir, las aplicaciones y los datos de usuario” (C Seaoane, 2010, párr. 4).

- “Seguridad activa: conjunto de medidas que previenen e intentan evitar los daños en los sistemas informáticos” (C Seaoane, 2010, párr. 2).

- “Seguridad pasiva: complemento de la seguridad activa, se encarga de minimizar los efectos que haya ocasionado algún percance” (C Seaoane, 2010, párr. 6).

2.2.2 Modelo de madurez de la Seguridad

Para ISOTools Excellence “La gestión de la Seguridad de la Información pasa por niveles o escalones, cada uno con su costo asociado y su contexto de aplicabilidad” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 6). Con el tiempo ha ido progresando y ahora se le conoce como Sistemas de Gestión de la Seguridad de la Información basados en la norma ISO 27001. Los niveles son los siguientes:

- Nivel 0, “el sentido común” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 7).
- Nivel 1, “el cumplimiento de la legislación obligatoria” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 8).

- Nivel 2, “evaluación del proceso de Gestión de Seguridad” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 9).
- Nivel 3, “analizar el riesgo y la gestión de su resolución” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 10).
- Nivel 4, “adquisición de productos para integrarlos en los Sistemas de Gestión” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 11).
- Nivel 5, “integración de los componentes certificados en sistemas compuestos y su certificación” (PMG-SSI, ISO 27001: El modelo de madurez de la seguridad de la información, 2015, párr. 12).

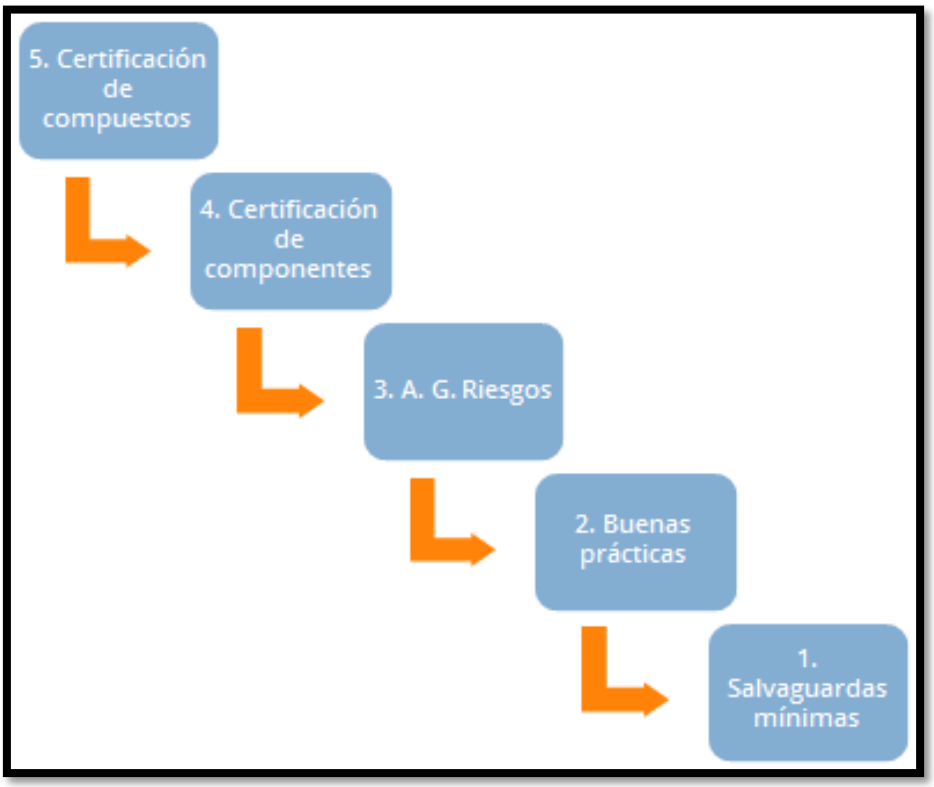


Figura 5. Modelo de madurez de la Seguridad de la Información – PMG-SSI (2015).

2.2.3 El Ciclo de Mejora Continua

Implementar un SGSI (Sistema de Gestión de Seguridad de la Información) basado en la norma ISO 27001, presenta un sistema de gestión basado en el ciclo de Deming que supone la implementación de un Sistema de Gestión basado en la mejora continua y constante evolución para adaptarse a los cambios. El ciclo de Deming enfocado al SGSI se describe de la siguiente manera: (ISOTools, ISO 27001: Pilares fundamentales de un SGSI, 2015, párr. 4).

- Planificar: Se define el alcance y la política de seguridad, se debe comenzar realizando un análisis de riesgos que refleje la situación actual de la entidad, al obtener dicha situación se define el plan de tratamiento de riesgos, que lleva a la implementación de controles de los diferentes riesgos no asumidos por la dirección (ISOTools, ISO 27001: Pilares fundamentales de un SGSI, 2015, párr. 15).

- Hacer: “Esta fase se centra en el plan de tratamiento de riesgos, se incluye la información y la concientización de los usuarios en materia de seguridad y se definen indicadores para los diferentes controles implementados” (ISOTools, ISO 27001: Pilares fundamentales de un SGSI, 2015, párr. 16).

- Verificar: “esta fase conlleva la realización de revisiones en la cual se comprobará la correcta implementación del SGSI, realizando auditorías internas y siendo revisado por la alta dirección de la empresa” (ISOTools, ISO 27001: Pilares fundamentales de un SGSI, 2015, párr 17).

- Actuar: “Es el resultado obtenido de las auditorías, es donde se deben implementar las diferentes acciones correctivas, preventivas o de mejora” (ISOTools, ISO 27001: Pilares fundamentales de un SGSI, 2015, párr 18).

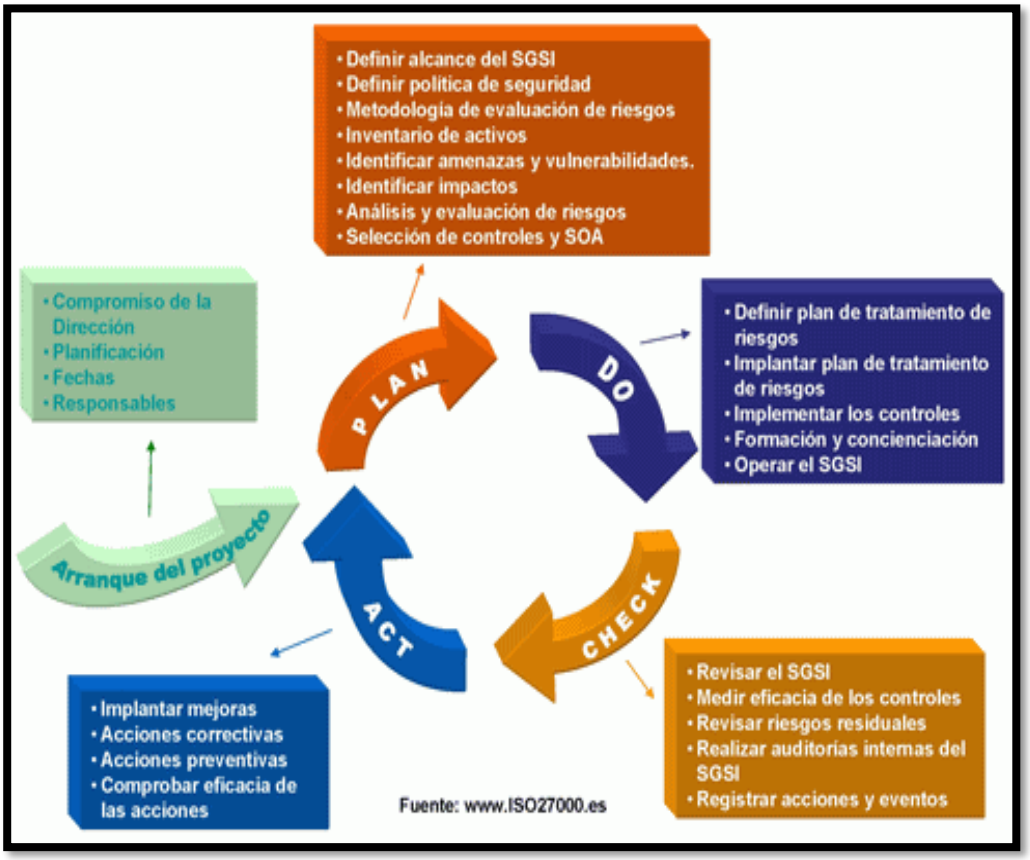


Figura 6. Ciclo PDCA enfocado a ISO 27001. ISO27000, (s.f.).

2.3 Gestión de la Seguridad de la Información

Para la ISO 27000 define al SGSI como, “conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información” (ISO 27000, 2012, párr. 21).

El objetivo del SGSI es la preservación de los pilares de la información, junto a los procesos y sistemas que hacen uso de ella, La confidencialidad, integridad y disponibilidad de la información ayudan a mantener la rentabilidad, los niveles de competitividad, la imagen empresarial que son necesarios para los objetivos de la organización (ISO27000, 2012, párr. 11).

Figura 7. Documentación del SGSI. ISO 27000 (2014).

Documentos de Nivel 1

- **Manual de seguridad:** “es el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI” (ISO27000, 2012, párr. 2).

Documentos de Nivel 2

- **Procedimientos: “**documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información” (ISO27000, 2012, párr. 3).

Documentos de Nivel 3

- **Instrucciones, checklist y formularios:** “documentos que describen cómo se realizarán las tareas y las actividades específicas relacionadas con la seguridad de la información” (ISO27000, 2012, párr. 4).

Documentos de Nivel 4

- **Registros: “**documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos” (ISO27000, 2012, párr. 5).

De manera específica, ISO 27001, indica que un SGSI debe estar formado por los siguientes documentos:

- **Alcance del SGSI:** “ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas” (ISO27000, 2012, párr. 11).

- **Política y objetivos de seguridad:** “documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información” (ISO27000, 2012, párr. 12).

- **Procedimientos y mecanismos de control que soportan al SGSI:** “aquellos procedimientos que regulan el propio funcionamiento del SGSI” (ISO27000, 2012, párr. 13).

- **Enfoque de evaluación de riesgos:** “descripción de la metodología a emplear, desarrollando criterios de aceptación de riesgo y fijación de niveles de riesgo aceptable” (ISO27000, 2012, párr. 14).

- **Informe de evaluación de riesgos:** “estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización” (ISO27000, 2012, párr. 15).

- **Plan de tratamiento de riesgos:** “documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información” (ISO27000, 2012, párr. 16).

- **Procedimientos documentados:** “todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados” (ISO27000, 2012, párr. 16).

- **Registros:** “documentos que proporcionan evidencia de la conformidad con los requisitos y del funcionamiento eficaz del SGSI” (ISO27000, 2012, párr. 17).

- **Declaración de aplicabilidad:** “documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones” (ISO27000, 2012, párr. 18).

2.4 Estándares para la Gestión de la Seguridad de la Información

El Sistema de Gestión de Seguridad de la Información está basado en la ISO 27001 que contiene los requisitos del SGSI, es certificable para empresas y personas.

Este estándar internacional se publicó el 15 de octubre de 2005, tiene su origen en la BS 7799-2:2002. En su Anexo A, enumera los objetivos de controles y controles que desarrolla la ISO 27002:2005, con el fin de que las organizaciones selecciones los controles para el desarrollo de su SGSI, no es una obligación implementar todos los controles del anexo, por lo tanto, las organizaciones deberán argumentar sólidamente la no aplicabilidad de los controles no implementados (ISO27000.es, 2012, párr. 5).

Así mismo existen otros estándares que apoyan a la ISO 27001 para que se implemente de una forma correcta los cuales son:

- ISO/IEC 27002: fue publicada el 1 de Julio de 2007, adoptó ese nuevo nombre de su antecesor ISO 17799:2005. Esta ISO, te brinda una serie de buenas prácticas las cuales describen los objetivos de control y controles recomendados en cuanto a seguridad de la información. Su uso no es certificable para empresas. Actualmente se encuentra en su versión

2013 y cuenta con 35 objetivos de control, 114 controles y 14 dominios (ISO27000.es, 2012, párr. 6).

- ISO/IEC 27003: Publicada el 01 de febrero de 2010 y actualizada el 12 de abril de 2017, no es certificable para empresas y es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación (ISO27000.es, 2012, párr. 7).

- ISO/IEC 27004: Publicada el 15 de diciembre de 2009 y revisada en diciembre de 2016, no es certificable para empresas y es una guía para el desarrollo y utilización de métricas y técnicas de medidas aplicables para determinar la eficacia de un SGSI (ISO27000.es, 2012, párr. 8).

- ISO/IEC 27005: Publicada en segunda edición el 1 de junio de 2011, no es certificable para empresas y proporciona directrices para la gestión del riesgo en la seguridad de la información (ISO27000.es, 2012, párr. 9).

2.4.1 COBIT

Según el portal de ESAN define a COBIT como, “marco de trabajo que permite comprender el gobierno y la gestión de las Tecnologías de la Información de una organización, así como evaluar el estado en que se encuentran las TI en la empresa” (ESAN, 2016, párr. 1)

COBIT se divide en 4 dominios:

- Planear y Organizar (PO): “Proporciona dirección para la entrega de soluciones (AI) y la entrega de servicios” (Institute, 2007, párr. 4).
- Adquirir e Implementar (AI): “Proporciona las soluciones y las pasa para convertirlas en servicios” (Institute, 2007, párr. 5).
- Entregar y Dar Soporte (DS): “Recibe las soluciones y las hace utilizables para los usuarios finales” (Institute, 2007, párr. 6).
- Monitorear y Evaluar (ME): Monitorear todos los procesos para asegurar que se siga la dirección provista” (Institute, 2007, párr. 7).

Planear y Organizar (PO): Este dominio organiza y cubre las estrategias y ayuda a identificar cómo el área de TI contribuye al logro de objetivos, así mismo, ayuda a realizar la visión estratégica planteada para que sea comunicada y administrada desde diferentes puntos de vista de la organización (Institute, 2007, párr. 8).

Adquirir e Implementar (AI): Ayuda a realizar las estrategias de TI, las soluciones de TI que requieren ser identificados, desarrollados y adquiridos de tal manera que se implementen e integren a los procesos del negocio, así mismo, el cambio y el mantenimiento de los sistemas son cubiertos por este dominio garantizando que las soluciones satisfagan los objetivos del negocio (Institute, 2007, párr. 15).

Entregar y Dar Soporte (DS): “Cubre la entrega de los servicios requeridos por la organización, incluyendo los servicios prestados, gestión de la seguridad y de continuidad, soporte a usuarios, administración de datos e infraestructura” (Institute, 2007, párr. 21).

Monitorear y Evaluar (ME): “Este dominio cubre la gestión del desempeño, monitoreo de control interno, cumplimiento legal y aplicación del gobierno” (Institute, 2007, párr. 27).

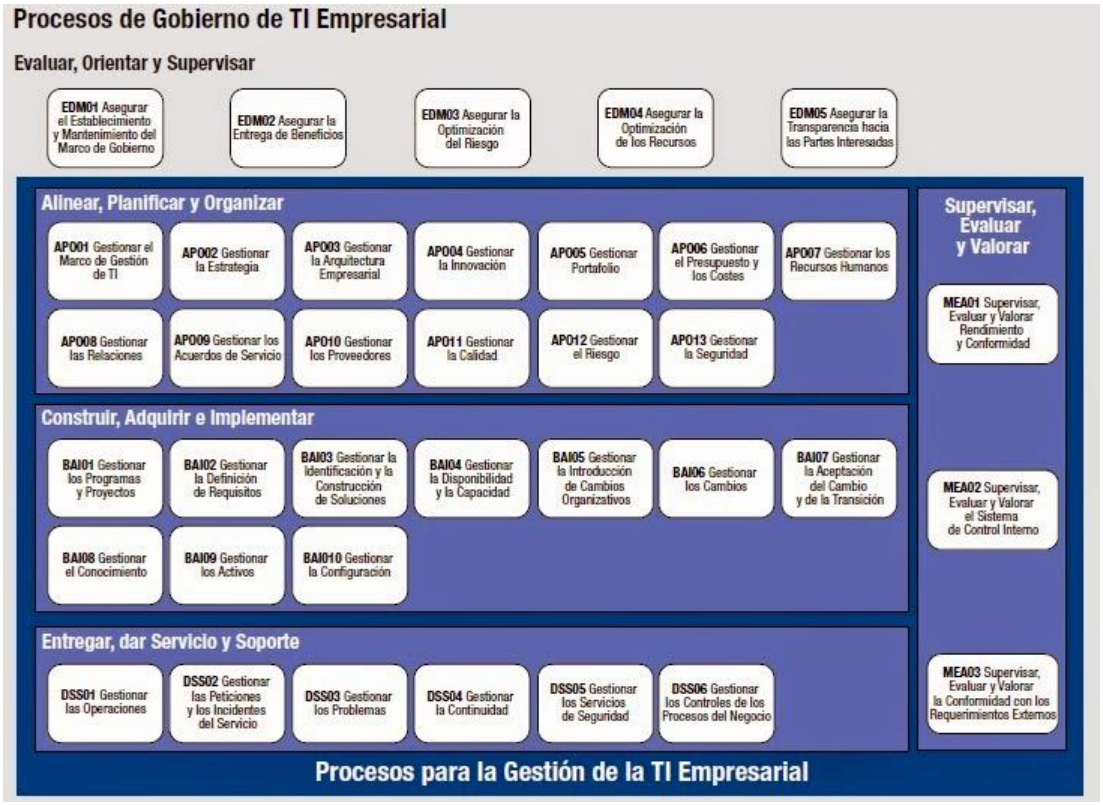


Figura 8. Procesos de gobierno de TI empresarial. Recuperado de COBIT 4.1.

2.3.2 COBIT y la Seguridad de la Información

De acuerdo a los dominios de COBIT brinda una serie de controles que apoyan a la seguridad de la información, donde se plantea la idea de que la Seguridad de la Información es una disciplina transversal, los cuales brindan una guía básica para definir, operar y monitorear un sistema para gestión de la seguridad, como son:

- Dominio: Alinear, Planificar y Optimizar (APO)
    - Proceso APO12 Gestionar el Riesgo: “Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa” (ISACA, 2012, pág. 107)
    - Proceso APO13 Gestionar la Seguridad: “Definir, operar y supervisar un sistema para la gestión de la seguridad de la información” (ISACA, 2012, pág. 113)

- Dominio: Construir, adquirir e implementar (BAI)
    - Proceso BAI04 Gestionar la disponibilidad y la capacidad: Ayuda a nivelar las necesidades actuales y futuras en disponibilidad, rendimiento y capacidad suministrando servicios efectivos en costos, incluyendo la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, analizando el impacto del negocio y evaluando el riesgo, planificando e implementando acciones para alcanzar los requerimientos identificados (ISACA, 2012, pág. 141)
    - Proceso BAI07 Gestionar la aceptación del cambio y la transición: Aceptar formalmente y hacer operativas las nuevas soluciones, incluir la planificación, la conversión de los datos y los sistemas, realizando pruebas de aceptación, comunicando y preparando el lanzamiento, el paso a producción de los procesos de negocio y servicios TI nuevos, el soporte en producción y revisando la post implementación (ISACA, 2012, pág. 153)
- Dominio: Entrega, Servicio y Soporte (DSS)
    - Proceso DSS05 Gestionar servicios de seguridad: “Protección de la información y de esa forma mantener un nivel aceptable de la gestión de riesgo de acuerdo con la política de seguridad de la información. Estableciendo roles de seguridad y privilegios de acceso a la información” (ISACA, 2012, pág. 191)

NTP ISO/IEC 27001:2014

La NTP ISO/IEC 27001:2014, es una traducción de la Norma Internacional ISO 27001:2013, que en la actualidad es difundida por el Instituto Nacional de la Calidad (INACAL), esta Norma, te especifica una serie de requisitos de seguridad de la información a cumplir por la organización para poder implementar, establecer, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. La Norma en mención puede ser implementada en pequeñas, medianas y grandes organizaciones ya que con la ayuda de los controles del Anexo A, ayudarán a identificar, analizar y mitigar posibles riesgos

que afecten a los activos de información de la organización, dicha Norma es certificable para organizaciones y personas ya que contiene las bases para una buena gestión de la seguridad de la información.

La Norma Técnica Peruana ISO/IEC 27001:2014, se divide en 4 fases de acuerdo al ciclo de mejora continua o también llamado Ciclo PDCA, (Plan – Do – Check – Act) que permitirán implementar de forma correcta la gestión de la seguridad de la información:

- Fase de Planificación: Ayuda a la organización a planificar su política de seguridad y sus objetivos de seguridad de la información que estarán alineados a la política general de seguridad de la información, así mismo, la organización decidirá dentro de los 114 controles, cuales aplican a su mismo.

- Fase de Implementación: En esta fase se desarrolla el punto anterior, implementando los controles que aplican y haciéndole seguimiento para la generación de evidencia.

- Fase de Revisión: Es la fase de la realización de auditorías para medir la efectividad de los controles implementados y verificar si el SGSI, cumple con los objetivos planificados.

- Fase de Mejora: En esta fase se mejorarán los puntos débiles que fueron hallados en las auditorías del punto anterior.

La Norma se divide en 7 requisitos que son los siguientes, empezando desde la Cláusula número 4:

- 4. Contexto de la organización: Se definen los requerimientos del contexto interno y externo del SGSI y se identifican los requisitos de las partes interesadas.

- 5. Liderazgo: Se define la política de seguridad de la información y sus objetivos que estarán alineados a los objetivos del negocio.

- 6. Planificación: Se identifican los riesgos y oportunidades de seguridad de la información, en relación a los activos de información.

- 7. Soporte: En este requisito se evalúan los recursos con los que la organización cuenta, así mismo, se verifica que el personal que implementará el SGSI esté capacitado y se comunica a las partes interesadas.

- 8. Operación: Se identifican los riesgos asociados a la confidencialidad, integridad y disponibilidad y se establecen indicadores para medir la efectividad del SGSI.

- 9. Evaluación del desempeño: Se desarrollan los planes de acción para mitigar las no conformidades identificadas en las auditorías internas.

- 10. Mejora: Se establecen acciones correctivas para las no conformidades y evitar que se repitan.

De igual manera, la Norma Técnica Peruana ISO/IEC 27001:2014 (Ver anexo 2), brinda 14 dominios, 35 objetivos de control y 114 controles, organizados de la siguiente manera:

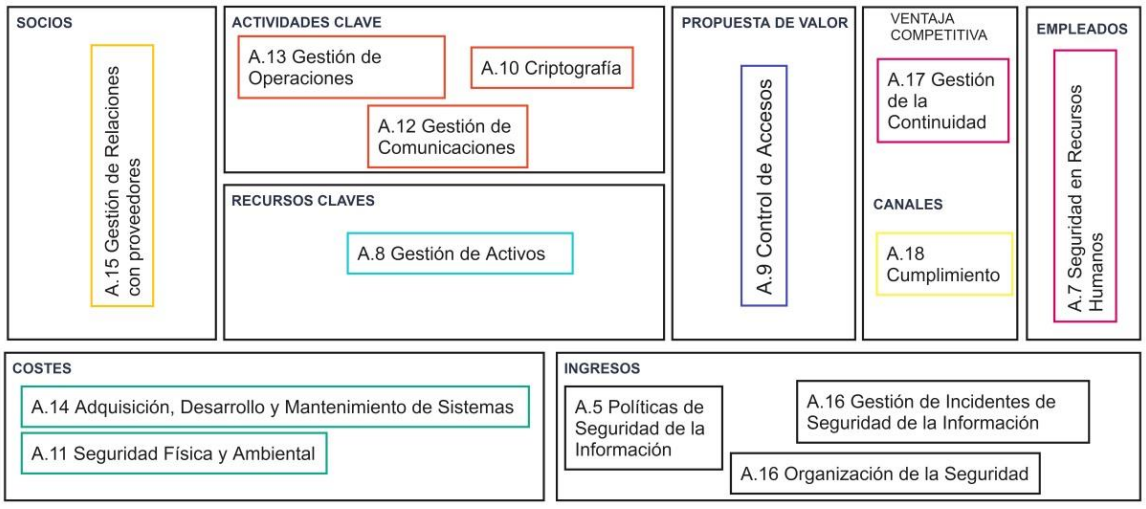


Figura 9. Controles de la NTP ISO/IEC 27001:2014. Adaptado de Seguridad en el Dialecto del jefe - Incibe (2016).

2.5 Gestión de riesgos

Para la ISO 27000 la gestión de riesgos lo define como, “actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgo” (ISO 27000, 2012, párr. (5)

La gestión de riesgos representa una serie de actividades para el resguardo de los activos de información, ayudando a la protección y al cumplimiento de sus principales objetivos. Así mismo le permite a la organización balancear los costos operacionales ocasionados por los incidentes de seguridad de la información ligados a la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización (Lujan, s.f., párr. 1).

Figura 10. Gestión de riesgos. Elaboración a partir de las fases de gestión de riesgos definidas por Sánchez, S. (s.f.)

2.5.1 Teorías

Para ISO 27000, “Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias” (ISO 27000, 2012, párr. 6).

De acuerdo con ISO 9001, “Efecto de la incertidumbre en un resultado esperado” (Jimenez, 2014, párr. 6).

Asimismo, para COBIT, define al riesgo de TI como “un riesgo de negocios, específicamente, el riesgo de negocios asociado con el uso, la propiedad, la operación, el involucramiento, la influencia y la adopción de TI dentro de una empresa” (Peña, 2013, párr. 2).

Según ISO 20000 define a riesgo como “efecto de la incertidumbre sobre los objetivos” (Arauzo, s.f., párr. 2).

2.5.2 Elementos de la gestión de riesgos

La ISO 27001 establece directrices para realizar la identificación, evaluación y tratamiento de riesgos, siendo en el SGSI la parte más importante de su implementación ya que ayuda a las organizaciones a identificar sus activos de información los cuales pueden sufrir algún tipo de daño por la activación de una amenaza o una vulnerabilidad.

Los elementos que componen la gestión de riesgos según la ISO 27001 son los siguientes:

- Metodología para la evaluación de riesgos: “El objetivo es hacer que todas las partes de la entidad conozcan tal metodología y la gestión de riesgo se haga de manera homogénea en todas las áreas” (ISOTools, ISO 27001: Evaluación y tratamiento de riesgos en 6 pasos, 2016, párr. (2)

- Implementación de la evaluación de riesgos: “Se debe contabilizar todos los activos que la organización posee, así como las amenazas y debilidades a las que enfrenta, para poder calcular la probabilidad de que suceda la combinación de activos – amenaza – debilidad” (ISOTools, ISO 27001: Evaluación y tratamiento de riesgos en 6 pasos, 2016, párr. (4)

- Informe de evaluación de riesgo: “se documenta todo el análisis realizado en los pasos anteriores” (ISOTools, ISO 27001: Evaluación y tratamiento de riesgos en 6 pasos, 2016, párr. 16).

CAPÍTULO III

DESARROLLO DEL PROYECTO

ESQUEMA DEL PROYECTO POR FASES

Tabla 1

Esquema del proyecto por entregables.

Fase I: Organización	
Actividades	**Entregables**
Taller de sensibilización del SGSI.	Material utilizado para el taller. (Ver Fig. 11)
Fase II: Planificación	
Actividades	**Entregables**
Desarrollo de la Política de Seguridad de la Información y objetivos.	Política de Seguridad y objetivos del SGSI. (Ver Fig. 12 y 13)
Definición de la comprensión de la institución y su contexto.	Documento de Análisis de Contexto Interno y Externo de la Institución. (Ver Fig. 14)
Identificación de las partes interesadas internas y externas.	Documento de identificación de Partes Interesadas Internas y Externas. (Ver Fig. 15)
Definición del alcance del SGSI.	Manual del SGSI. (Ver Fig. 16)
Desarrollo del Manual de Funciones y Responsabilidades del SGSI	Manual de Funciones y Responsabilidades. (Ver Fig. 17)
Desarrollo del procedimiento de Control de Documentos del SGSI.	Procedimiento de control de documentos del SGSI. (Ver Fig. 18)
Desarrollo del Plan de Comunicaciones	Plan de Comunicaciones. (Ver Fig. 19)
Definición de la Metodología de Gestión de Riesgos.	Metodología de Gestión de Riesgos. (Ver Fig. 20)
Diseño de la Matriz de Riesgos	Formato de la Matriz de Riesgos. (Ver Fig. 21)
Identificación, clasificación y evaluación de activos.	Formato del Inventario de Activos. (Ver Fig. 36)

Identificación de análisis y evaluación de riesgos.	Formato de la Matriz de Riesgos. (Ver Fig. 21)
Desarrollo del Plan de Tratamiento de Riesgos.	Formato del Plan de Tratamiento de Riesgos. (Ver Fig. 22)
Fase III: Despliegue	
Actividades	**Entregables**
Desarrollo de la Declaración de Aplicabilidad (SOA)	Formato del SOA. (Ver Fig. 27)
Desarrollo de los controles del Anexo A	
• A.6 Organización de la Seguridad de la Información.	Política de Organización del SGSI. (Ver Fig. 28)
• A.16 Gestión de los incidentes de seguridad de la información.	Política de Gestión de Incidentes, Procedimiento y Formatos. (Ver Fig. 29, 30 y 31)
• A.7 Seguridad de los Recursos Humanos.	Política y Formatos. (Ver Fig. 32, 33)
• A.8 Gestión de Activos.	Política, Procedimientos y Formatos. (Ver Fig. 34, 35 y 36)
• A.9 Control de Accesos.	Política de Gestión de Accesos. (Ver Fig. 37)
• A.10 Criptografía.	Política de Criptografía. (Ver Fig. 38)
• A.11 Seguridad física y del Ambiente.	Política, Procedimientos y Formatos. (Ver Fig. 39, 40, 41 y 42)
• A.12 Seguridad de las Operaciones.	Política, Procedimientos y Formatos. (Ver Fig. 43, 44, 45, 46 y 47)
• A.13 Seguridad de las Comunicaciones.	Política, Procedimientos y Formatos. (Ver Fig. 48, 49, 50 y 51)
• A.14 Adquisición, Desarrollo y Mantenimiento de Software.	Política y Formatos. (Ver Fig. 52 y 53)
• A.15 Relación con Proveedores.	Política, Procedimiento y Formatos. (Ver Fig. 54, 55 y 56)
• A.18 Cumplimiento.	Política, Procedimiento y Formatos. (Ver Fig. 57, 58 y 59)
Relación de Indicadores del SGSI	Formato de Indicadores. (Ver Fig. 60)

Para la participación del bachiller en el proyecto de implementación de la NTP ISO/IEC 27001:2014, se necesitó llevar un curso de certificación internacional en Seguridad de la Información, para obtener los conocimientos, técnicas e interpretación de la Norma para el desarrollo de los controles de la misma, y de esa forma, poder guiar a los usuarios en la interpretación e implementación de las diferentes políticas, procedimientos y manuales.

3.1 Fase I: Organización del proyecto

El proyecto se realizó en 3 fases, teniendo como primera fase a la organización del proyecto.

En esta primera etapa del proyecto se realizaron las siguientes actividades:

- Se desarrolló el taller de sensibilización del SGSI con el objetivo de presentar al personal interno de la organización la importancia y beneficios que brinda una adecuada gestión de riesgos mediante la implementación de un sistema de gestión de seguridad de la información para poder obtener el apoyo institucional.

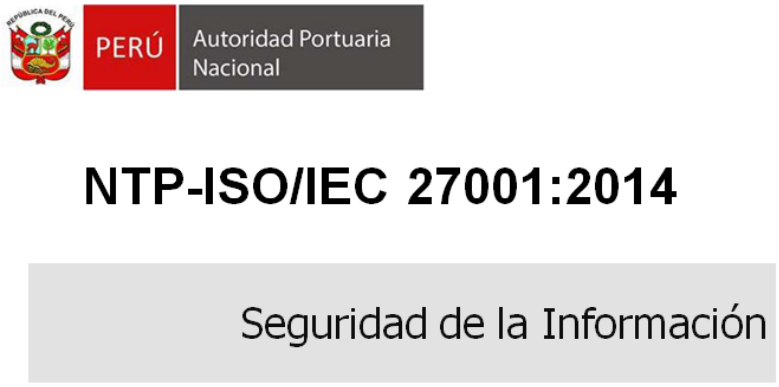


Figura 11. Taller de sensibilización del SGSI. Extraído de la diapositiva del taller.

En la Figura 11, se muestra la portada del taller de sensibilización que estuvo enfocado al personal interno de la Autoridad Portuaria Nacional con el fin de crear conciencia entre los trabajadores respecto a Seguridad de la Información, se llevó a

cabo en 3 sesiones seguidas incluyendo un examen al final de la última sesión, con el fin de medir sus conocimientos y tener indicadores sobre personal capacitado.

El bachiller participó en el desarrollo de las diapositivas para las 3 sesiones y el examen final, funciones que fueron delegadas por el jefe del proyecto, así mismo, participó como apoyo con el consultor en los talleres para absolución de dudas por parte de los participantes.

De acuerdo a las etapas del proyecto, la fase de Organización del proyecto culminó con lo anteriormente mencionado el cual fue revisado y aprobado.

3.2 Fase II: Planificación

En esta segunda etapa del proyecto se realizaron las siguientes actividades de planificación requeridas por la norma de manera metodológica y en concordancia con la política y objetivos del SGSI dentro del alcance del mismo, las cuales se detallan a continuación:

- Se desarrolló la Política de Seguridad de la Información y objetivos.
- Se definió la comprensión de la institución y su contexto.
- Se identificaron las partes interesadas internas y externas de la institución.
- Se determinó el alcance del SGSI, el cual se encuentra en el Manual del SGSI.
- Se desarrollaron las funciones y responsabilidades del comité del SGSI.
- Se definió los formatos para las políticas, procedimientos, manuales, directivas.
- Se verificación las capacidades, competencias y concientización en seguridad de la información.
- Se definió el plan de comunicaciones.
- Se definió la Metodología de Gestión de Riesgos y Oportunidades.
- Se diseñó la Matriz de Riesgos.
- Se identificó, clasificó activos de información.
- Se identificaron, clasificaron y evaluaron riesgos de seguridad de la información.
- Se desarrolló el Plan de Tratamiento de Riesgos.

	POLÍTICA	Código: SGSI-PO-01 Revisión: 12-09-2017 Aprobado: GG Fecha: 12-09-2017 Página: 1 de 1
PERÚ Autoridad Portuaria Nacional	SEGURIDAD DE LA INFORMACIÓN	

Por lo tanto el Gerente General declara los siguientes lineamientos:

- Proteger los activos de información del sistema de gestión de seguridad de la información de la APN frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar su confidencialidad, integridad y disponibilidad.
- Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen.
- Mejorar continuamente la eficacia el sistema de gestión de seguridad de la información a fin de minimizar constantemente los riesgos de la seguridad de la información.
- Cumplir los requisitos legales y regulatorios que afectan a la organización respecto a la seguridad de la información.

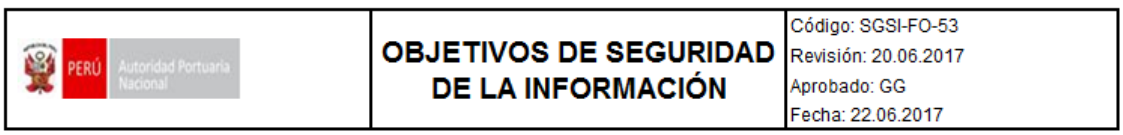
AUTORIDAD PORTUARIA NACIONAL · GERENCIA GENERAL

Guillermo Bounroncle Calixto
Gerente General
APN

Figura 12. Política de Seguridad de la Información - Autoridad Portuaria Nacional.

En la Figura 12, se muestra la Política de Seguridad de la Información donde se muestra los lineamientos aprobados por el Gerente General.

Se participó en el desarrollo de la Política de Seguridad de la Información, de acuerdo a lo que indica la Norma en su requisito 5.2 “La alta dirección debe establecer una política de seguridad de la información, que debe, estar disponible a las partes interesadas y estar comunicada”, cabe resaltar, que luego de haberla formulado, pasó a una etapa de revisión por parte del jefe de proyecto, concluyendo con la aprobación del Comité de Seguridad de la Información para su posterior publicación.



	OBJETIVOS DE SEGURIDAD DE LA INFORMACIÓN	Código: SGSI-FO-53 Revisión: 20.06.2017 Aprobado: GG Fecha: 22.06.2017
PERÚ Autoridad Portuaria Nacional		

Figura 13. Objetivos de seguridad de la Información. Documento interno de la institución.

En la Figura 13, se desarrollaron objetivos de seguridad de la información de acuerdo a como lo indica la cláusula 6.2 de la NTP ISO/IEC 27001:2014, donde indica lo siguiente: “La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Para la elaboración del documento, el bachiller tuvo que interpretar lo que indica la norma “Los objetivos de seguridad de la información debe ser consistentes con la política, ser medibles, ser comunicados y actualizados”, y de esa forma alinear los Objetivos de Seguridad de la Información con la Política de Seguridad de la Información y de esa forma ser revisada por el Comité de Seguridad de la Información para que sea aprobada y difundida entre los responsables de los procesos del alcance.

Nota: Los documentos desarrollados en las diferentes etapas del proyecto son internos.

Figura 14. Contexto interno y externo de la institución. Documento interno de la institución.

En la Figura 14, el bachiller participó en la elaboración del documento en conjunto con el consultor, quienes realizaron un taller con la alta dirección explicando el objetivo del requisito de la norma “La organización debe determinar los aspectos externos e internos que son relevantes para este propósito”, y de esa forma ayudarlos a identificar los aspectos externos e internos relevantes para el logro del SGSI.

Figura 15. Identificación de las partes interesadas internas y externas. Documento interno de la institución.

En la Figura 15, el bachiller participó en la elaboración del documento en conjunto con el consultor, quienes realizaron un taller con la alta dirección explicando el objetivo del requisito de la norma “La organización debe determinar las partes interesadas relevantes al SGSI, pudiendo incluir requisitos legales, regulatorios y

obligaciones contractuales", y de esa forma, ayudarlos a identificar las partes interesadas relevantes al SGSI y los requisitos de las mismas.

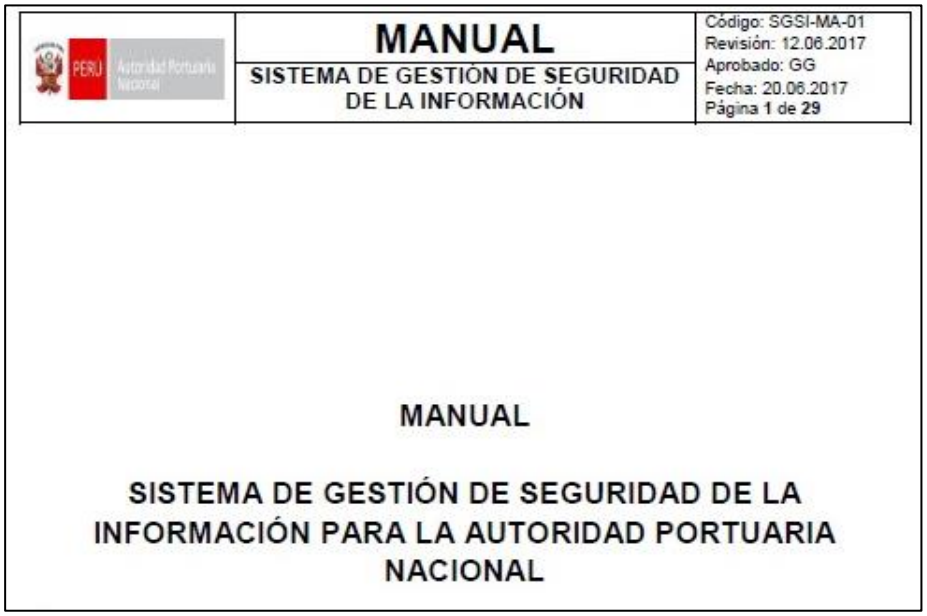


Figura 16. Manual de Seguridad de la Información de la Autoridad Portuaria Nacional. Documento interno de la institución.

En la Figura 16, de acuerdo a las funciones delegadas por el jefe del proyecto, la función del bachiller fue el desarrollo total del mencionado manual, de acuerdo a lo indicado en el requisito 4.3 "Determinar el alcance, las interfaces y dependencias entre actividades realizadas por la organización" y el requisito 4.4 "La organización debe establecer, implementar, mantener y mejorar el SGSI de acuerdo a los requisitos de la NTP ISO/IEC 27001:2014", realizando reuniones con el Comité de Seguridad de la Información para identificar los controles que serán implementados.

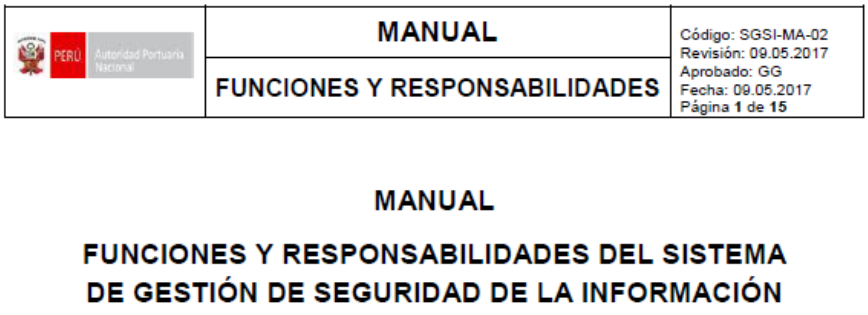


Figura 17. Portada del de Funciones y Responsabilidades del SGSI. Documento interno de la institución.

En la Figura 17, de acuerdo a las funciones del Bachiller, el desarrollo del mencionado Manual se realizó de acuerdo a la modificación del artículo N° 5 de la Resolución Ministerial N° 004-2016-PCM, donde indican las funciones específicas del Comité de Seguridad de la Información, de igual forma, con ayuda de la Norma se desarrollaron las funciones para los integrantes del mencionado comité.

Figura 18. Procedimiento de Control de Documentos del SGSI. Documento interno de la institución.

En la Figura 18, El bachiller participó en la elaboración del mencionado documento con ayuda de la Norma y del consultor de acuerdo al requisito 7.5.3 “Cuando se crea y actualiza información documentada, la organización debe asegurarse que esté disponible y sea conveniente para uso y que esté protegida adecuadamente”, funciones que fueron delegadas por el jefe del proyecto, para luego pasar a revisión y aprobación por parte del Comité de Gestión de Seguridad de la Información.

Figura 19. Plan de Comunicaciones interno del SGSI. Documento interno de la institución.

En la Figura 19, el presente Formato fue desarrollado en su totalidad por el bachiller, interpretando lo que indica la Norma en su requisito 7.4 “La organización debe determinar la necesidad de comunicaciones internas y externas relevantes al SGSI”, al término de la elaboración fue revisado por el jefe de proyecto y así mismo, aprobado por el Comité del SGSI e implementado para la obtención de evidencias.

Se estructura de la siguiente manera:

- Tipo de comunicación: Se identifica si la comunicación será interna o externa.
- Qué comunica: Se identifica si se comunica una política, procedimientos, directivas. Etc.
- Quién comunica: Se identifica al usuario que realiza la comunicación.
- Cómo comunica: Se identifica el medio de comunicación, correo, teléfono, resolución, etc.
- A quién comunica: Se identifica a quien va dirigido, comité del SGSI, jefe de área, presidencia, etc.
- Cuando comunica: Se coloca la fecha en la que se realiza la comunicación.

Este formato es importante ya que, en las auditorías, el auditor líder lo solicitará para identificar cómo se están comunicando los documentos del SGSI.

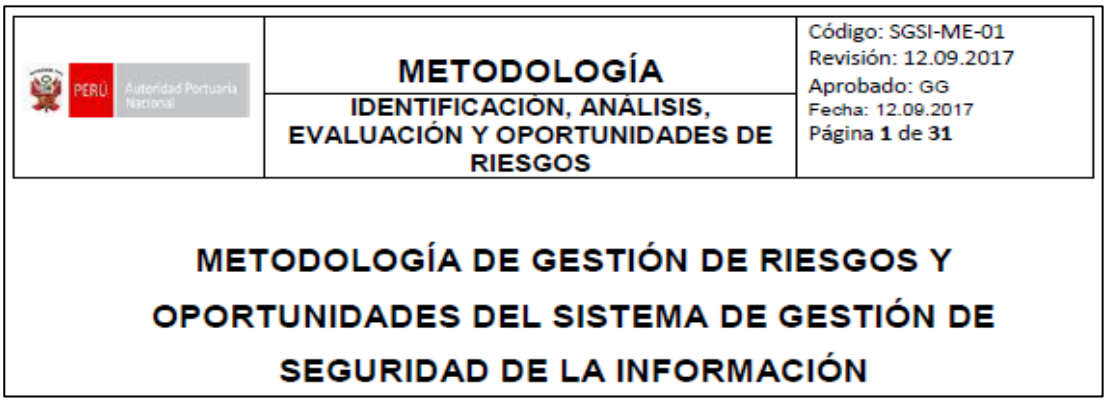


Figura 20. Metodología de Gestión de Riesgos y Oportunidades del Sistema de Gestión de Seguridad de la Información. Documento interno de la institución.

En la Figura 20, la metodología de Gestión de Riesgos y Oportunidades se desarrolló con la asesoría del consultor en seguridad de la información, ya que para definir los lineamientos de seguridad en la gestión de riesgos, se necesitaba conocer cómo se gestionan los riesgos a nivel de SGSI, luego de realizar la asesoría, se realizaron reuniones con los responsables de los procesos para realizarles inducción

del funcionamiento del manual, el bachiller participó en la inducción y la generación de evidencias.

		IDENTIFICACION DE RIESGOS								ANALISIS DE RIESGO		
Código Riesgo	Descripción del Riesgo	Activos Comprometidos	Amenaza	Vulnerabilidad	Fuente del Riesgo	Descripción de las Causas	Consecuencias	Dueño de Riesgo	Áreas de Impacto	Probabilidad	Impacto	
										Tipo	Tipo	Nivel de Riesgo
R01	Acceso no autorizado a información digital reservada por personal	Documentación de fiscalización	Divulgación	Deficiencia en el control de fuga de información / Incumplimiento de control de accesos	Humanas	Falta de controles de seguridad de acceso a información	Demandas judiciales. Perdidas de imagen	Director de Fiscalización	Toda la organización	Posible	Alto	Medio

Figura 21. Formato de Gestión de Riesgos y Oportunidades. Documento interno de la institución.

En la Figura 21, de acuerdo a las funciones del bachiller delegadas por el jefe del proyecto, el bachiller elaboró el Formato, siguiendo los lineamientos de la Metodología de Gestión de Riesgos, así mismo, se tuvo reuniones con los responsables de los procesos para asesorarlos en la identificación, análisis y tratamiento de riesgos de Seguridad de la Información. El formato se divide en 2 partes, las cuales son:

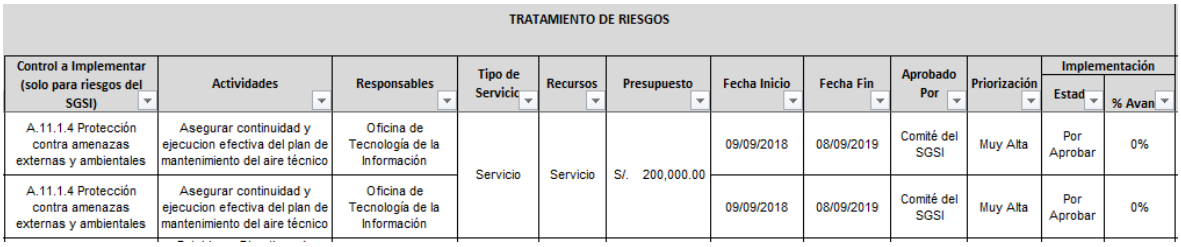
- Identificación de riesgos.
- Análisis de riesgo.

En la primera parte (identificación de riesgo), se identifica los riesgos y se le da una breve descripción.

Se identifican los activos comprometido, así mismo, la amenaza, la vulnerabilidad, la fuente del riesgo, se describen las causas si el riesgo se materializa, las consecuencias que traería la materialización del riesgo, quien es el dueño del riesgo y a que áreas impactaría ese riesgo.

En la segunda parte (análisis del riesgo), se valoriza el riesgo de acuerdo a la probabilidad y a su impacto y el resultado de esa multiplicación define el nivel de riesgo.

Este Formato es de suma importancia ya que los usuarios lo utilizarán cada vez que identifiquen nuevos riesgos y de esa forma sean evaluados y para luego darles tratamiento y puedan ser mitigados.



TRATAMIENTO DE RIESGOS

Control a Implementar (solo para riesgos del SGSI)	Actividades	Responsables	Tipo de Servicio	Recursos	Presupuesto	Fecha Inicio	Fecha Fin	Aprobado Por	Priorización	Implementación	
										Estado	% Avan
A.11.1.4 Protección contra amenazas externas y ambientales	Asegurar continuidad y ejecucion efectiva del plan de mantenimiento del aire técnico	Oficina de Tecnología de la Información	Servicio	Servicio	S/. 200,000.00	09/09/2018	08/09/2019	Comité del SGSI	Muy Alta	Por Aprobar	0%
A.11.1.4 Protección contra amenazas externas y ambientales	Asegurar continuidad y ejecucion efectiva del plan de mantenimiento del aire técnico	Oficina de Tecnología de la Información				09/09/2018	08/09/2019	Comité del SGSI	Muy Alta	Por Aprobar	0%

Figura 22. Formato de Plan de Tratamiento de riesgos. Documento interno de la institución.

En la Figura 22, de acuerdo a las funciones del bachiller delegadas por el jefe del proyecto, el bachiller elaboró el Formato siguiendo los lineamientos de la Metodología de Gestión de Riesgos, así mismo, se tuvo reuniones con los responsables de los procesos para asesorarlos en el tratamiento de riesgos de Seguridad de la Información, el Formato tiene la siguiente estructura:

- Control a implementar: Se identifica el control del Anexo A de la Norma que será implementado para que el riesgo sea mitigado.
- Actividades: Se describen las actividades que se realizarán para mitigar los riesgos identificados.
- Responsable: Se identifica al responsable del proceso que será el encargado de efectuar las actividades para mitigar los riesgos.
- Tipo de servicio: Si el riesgo requiere de una compra, un servicio o una capacitación.
- Presupuesto: Se le asigna un presupuesto de acuerdo al tipo de servicio que se contratará para mitigar los riesgos.
- Fecha inicio, Fecha fin: Se estiman las fechas de ejecución de las actividades para mitigar los riesgos.
- Aprobado por: Se identifica a los responsables de la aprobación del tratamiento de riesgos para que supervisen la ejecución de las actividades.
- Priorización: Se identifica la prioridad de acuerdo al nivel del riesgo identificado.
- Implementación: Se identifica y supervisa la aprobación de las actividades, así mismo, se le asigna un porcentaje de implementación.

Su uso es importante ya que deberá ser aprobado por los dueños del riesgo y el comité de seguridad para que se puedan ejecutar.

Dentro de los requisitos de la Norma se desarrollaron documentos los cuales sirven de apoyo para la generación de evidencia, se participó en la elaboración de dichos documentos. Los documentos desarrollados en esta etapa del proyecto son los siguientes:

- SGSI-FO-Lista Maestra de Documentos. (Ver Fig. 23)
- SGSI-FO-Solicitud de Acción Correctiva. (Ver Fig. 24)
- SGSI-FO-Acta de Reunión. (Ver Fig. 25)
- SGSI-FO-Acta de Revisión por la Dirección. (Ver Fig. 26)

PERÚ Autoridad Portuaria Nacional

FORMATO
LISTA MAESTRA DE DOCUMENTOS INTERNOS DEL SGSI

Fecha de Actualización: 13/09/2017

N°	Norma	PROCESO	Tipo	Título	Código del Documento	N° de Versión	Aplican	Estado	Fecha de Aprobación	Ubicación
1	ISO 27001	SGSI	Política	Seguridad de la Información	SGSI-PO-01	3	TODOS	APROBADO	12.09.2017	Carpeta SGSI APN dentro de la unidad Comun de la red
2	ISO 27001	SGSI	Política	Seguridad Física y del Ambiente	SGSI-PO-02	3	TODOS	APROBADO	12.09.2017	Carpeta SGSI APN dentro de la unidad Comun de la red

Figura 23. Lista Maestra de documentos Internos del SGSI. Documento interno de la institución.

En la Figura 23, el desarrollo del Formato se realizó de acuerdo a buenas prácticas en la implementación de la Norma, el bachiller tuvo como función elaborar el formato y realizar el llenado del mismo de acuerdo a los documentos desarrollados, agrupándolos por tipo y de esa forma sean accesibles por los responsables de los procesos.

El formato se estructura de la siguiente manera:

- Tipo: Si es una política, procedimiento, formato, metodología, resolución, directiva o manual.
- Código del documento: Se le asigna un código a los documentos de acuerdo a los controles de la norma.
- N° de versión: Se identifica en qué versión se encuentra el documento.
- Aplicación: Se define si el documento será aplicado a toda la organización o a solo unos procesos.
- Estado: Se identifica si está en proceso de desarrollo, aprobación o difusión.
- Fecha de aprobación: Una vez que los documentos fueron revisados pasan al comité para que sean aprobados formalmente.

- Ubicación: Se identifica la ubicación del documento.

PERÚ Autoridad Portuaria Nacional	FORMATO	Código	P03_02-DI07_R01
	SOLICITUD DE ACCIÓN DE MEJORA	Versión	01

Reporte N°: 001	Fecha del Reporte: 28/11/2017
Proceso: Recursos Humanos	Reportado por: Jose Luis Sandoval
Normativa Aplicable: NTP ISO/IEC 27001:2014	Requisito: 7 Soporte (A.7.2.2, 7.2 C)
Hallazgo: Cuando ingresa un nuevo colaborador a APN, no siempre se registra la inducción del SGSI. En el registro SGSI-FO-27 Inducción del Personal al SGSI no se ha registrado inducción a Fernando Soriano y sólo hay registros de personal de la OTI y no de las otras áreas. Además, no siempre APN se asegura que el conocimiento necesario llegue de forma adecuada a los participantes.	
Tipo de Solicitud: Acción Correctiva [X]	Acción Preventiva [ ]
Aceptado por: Mariela Gutarra	Responsable de Tratamiento: Mariela Gutarra
Requiere Análisis de Riesgo: SI [ ]	NO [ ]
Análisis de causa: 1. Se consideró las capacitaciones que se venían realizando en forma presencial, ya que, se escogían al azar a los usuarios de todas las áreas. 2. Algunos usuarios que salían desaprobados no asistían a la clase, se retiraban o estaban de comisión, por lo que volvían a desaprobar.	

Descripción de Acciones:				
Tipo	Actividad	Riesgo	Responsable	Fecha de cumplimiento
Cumplimiento de las Actividades:				
Seguimiento de la eficacia de las Actividades:				
Fecha:	Responsable de Cierre:	Firma:		

Figura 24. Solicitud de Acción Correctiva. Documento interno de la institución.

En la Figura 24, de acuerdo a las funciones desarrolladas por el bachiller, el Formato fue desarrollado tomando como ejemplo, el que se usó en el Sistema de Gestión de la Calidad, ajustándolo al Sistema de Gestión de Seguridad de la Información, el formato es importante ya que cuando se realizó la auditoría interna, sirvió para identificar las no conformidades y/o acciones de mejora del SGSI, el formato se encuentra dividido en 3 partes:

- En la primera parte se identifica el proceso que fue objeto de la auditoría, se le asigna un número de solicitud, se coloca la fecha, el nombre del responsable

de la auditoría, el requisito de la norma que aplica al proceso auditado y se realiza una breve del hallazgo identificado en la auditoría.

- En la segunda parte: se identifica el tipo de solicitud, si es una acción correctiva o una acción preventiva, de acuerdo al tipo de solicitud se identifica si se requiere análisis de riesgo o no, y por último se identifica el análisis de causa que son las actividades que se realizaron para cumplir con el control de la norma.
- En la tercera parte: se describen las acciones que se van a realizar para poder mitigar el hallazgo encontrado, así mismo, se verifica el cumplimiento de dichas actividades y por último se verifica la eficacia de las actividades implementadas.

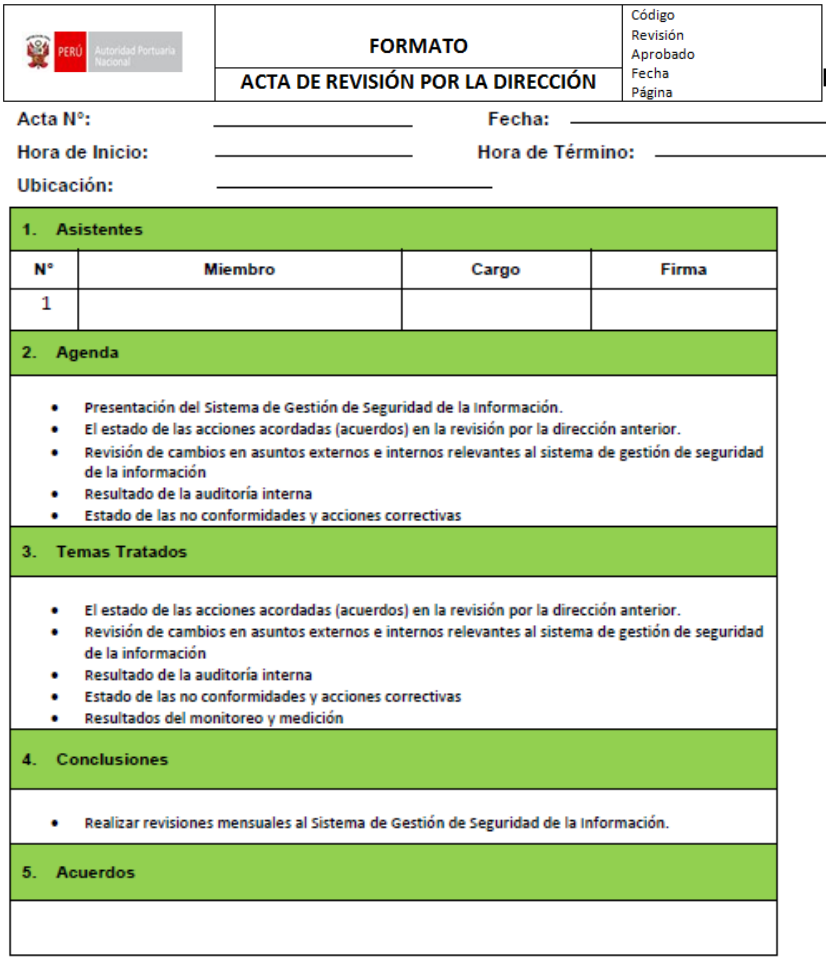
	FORMATO	Código: SGSI-FO-13 Revisión: 12-09-2017 Aprobado: GG Fecha: 12-09-2017 Página 1 de 1
	ACTA DE REUNIÓN	

N° de Acta	00xx	
Tema de Convocatoria		
Dirección y/o Jefatura		
Lugar de reunión		
Fecha		
Hora de inicio	xx : xx horas	
Hora de finalización	xx : xx horas	
ASISTENTES	**ÁREA ó ENTIDAD**	**FIRMA**
AGENDA *(Temas a tratar)*		
DESARROLLO DE LA AGENDA		
ACUERDOS ADOPTADOS		
Se acordó próxima reunión de _____, para el día _____ de fecha ___.___.2017 a las xx:xx hrs. (Sólo si se acuerda)		
PLAZOS *(de requerirse)*		
OTROS / OBSERVACIONES / RECOMENDACIONES		

Figura 25. Acta de reunión. Documento interno de la institución.

En la Figura 25, de acuerdo a las buenas prácticas de la Norma, el bachiller participó en la elaboración del Formato, ya que sirvió como evidencia de las reuniones con la alta dirección acerca del avance de implementación de la Norma. El formato consta de 2 partes:

- La primera parte: Se le asigna un número de reunión, se indica el tema de la convocatoria, se identifica que jefatura está realizando la reunión, donde se realizará la reunión, la fecha de la reunión y la hora de inicio y fin de la reunión.
- La segunda parte: Se colocan los nombres de los asistentes, el área y su firma, así mismo, se identifican los temas que serán tratados en dicha reunión, los acuerdos a los cuales llegaron, los plazos de ejecución de los acuerdos y por último se colocan observaciones si las hubiera.



PERÚ Autoridad Portuaria Nacional	FORMATO	Código Revisión Aprobado Fecha Página
	ACTA DE REVISIÓN POR LA DIRECCIÓN	

Acta N°: _____ **Fecha:** _____

Hora de Inicio: _____ **Hora de Término:** _____

Ubicación: _____

1. Asistentes

N°	Miembro	Cargo	Firma
1			

2. Agenda

- Presentación del Sistema de Gestión de Seguridad de la Información.
- El estado de las acciones acordadas (acuerdos) en la revisión por la dirección anterior.
- Revisión de cambios en asuntos externos e internos relevantes al sistema de gestión de seguridad de la información
- Resultado de la auditoría interna
- Estado de las no conformidades y acciones correctivas

3. Temas Tratados

- El estado de las acciones acordadas (acuerdos) en la revisión por la dirección anterior.
- Revisión de cambios en asuntos externos e internos relevantes al sistema de gestión de seguridad de la información
- Resultado de la auditoría interna
- Estado de las no conformidades y acciones correctivas
- Resultados del monitoreo y medición

4. Conclusiones

- Realizar revisiones mensuales al Sistema de Gestión de Seguridad de la Información.

5. Acuerdos

Figura 26. Acta de Revisión por la Dirección. Documento interno de la institución.

En la Figura 26, el bachiller elaboró el Formato de acuerdo a lo indicado por la Norma en el cual de específica cómo debe hacer la revisión por la dirección, luego se pasó a revisión por parte del jefe de proyecto, para luego ser llevado a Comité y se realice su aprobación. El Formato de Acta de Revisión por la Dirección, consta de 3 partes, las cuales son.

- La primera parte: se le asigna un número de acta, fecha de la revisión, hora de inicio y término y la ubicación donde se realizará la revisión.
- La segunda parte: Se colocan los nombres de los asistentes, su cargo y su firma, se desarrollan los temas preestablecidos en la agenda y los temas que se trataran, luego cómo conclusión se define la periodicidad de las revisiones al SGSI, se escriben los acuerdos y por último firman los integrantes que pertenecen al comité de seguridad.

Al término de la fase II del proyecto, se obtuvieron las siguientes conclusiones:

- Se realizaron los talleres para la identificación de riesgos y oportunidades de seguridad de la información.
- Es de suma importancia que los propietarios de los activos participen en los talleres de trabajo.
- Uno de los aspectos críticos del Plan de Comunicación interna del SGSI es su aprobación, por lo que debe asegurarse la participación de los altos funcionarios de la institución.
- Se desarrolló el alcance que se encuentra en el Manual del Sistema de Gestión de Seguridad de la Información.

De acuerdo a las etapas del proyecto, la fase de Planificación del proyecto culminó con los documentos anteriormente mencionados los cuales fueron revisados y puestos en marcha para la generación de evidencia mientras se oficializaba su aprobación.

3.3 Fase III: Despliegue

En esta fase del proyecto se desplegaron las actividades de implementación del SGSI y se realizaron las siguientes actividades:

- Se definió y desarrolló el formato a utilizar para la Declaración de Aplicabilidad (SOA), el cual contiene los controles de seguridad de la información.
- Se desarrollaron los controles de Seguridad de la Información que se encuentran en el Anexo A de la Norma.

- Se definieron indicadores que permitan obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles a nivel operativo y de gestión. (Ver Anexo 7 – Indicadores del SGS.

PERÚ Autoridad Portuaria Nacional	**Declaración de Aplicabilidad**	Código: SGSI-FO-46 Revisión: 11.04.2017 Aprobado: GG Fecha: 11.04.2017

Cláusula N°	Objetivos de Control	Control		Aplica SI/NO	Justificación de la Exclusión o Inclusión	Documento Relacionado o Justificación de la Exclusión
A.5	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**					
	A.5.1 Dirección de Gestión para la Seguridad de Información	A.5.1.1 Políticas de seguridad de información	Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la gerencia, publicado y comunicado a los empleados y a las partes externas relevantes.	**SI**		
		A.5.1.2 Revisión de las políticas de seguridad de información	Las políticas para la seguridad de la información deben ser revisadas a intervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y efectividad continua.	**SI**		
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**					
		A.6.1.1 Funciones de seguridad de información y responsabilidades	Todas las responsabilidades de seguridad de la información deben ser definidas y asignadas.	SI		

Figura 27. Formato de Declaración de Aplicabilidad SOA. Documentación interna de la institución.

En la Figura 27, el bachiller de acuerdo al curso de certificación llevado, por buenas prácticas se recomienda realizar una Declaración de Aplicabilidad (SoA), para visualizar los controles que serán implementados o que impacten de forma relevante a la institución, para realizar la identificación de los controles a implementar, se tuvo reuniones con alta dirección, una vez identificados los controles, pasó a aprobación por parte del Comité para ser entregado cuando se realicen las auditorías.

De acuerdo a las actividades en esta etapa del proyecto, se desarrollaron las siguientes políticas y procedimientos con la finalidad de cumplir con los lineamientos que dicta la NTP ISO/IEC 27001:2014:

- Política de Organización de Seguridad de la Información.
- Política de Seguridad en Recursos Humanos.
- Política de Gestión de Activos.
- Política de Gestión de Accesos.
- Política de Criptografía.
- Política de Seguridad Física y del Ambiente.
- Política de Gestión de Telecomunicaciones.
- Política de Seguridad de Operaciones.
- Política de Adquisición, Desarrollo y Mantenimiento de Software.
- Política de Seguridad con proveedores.
- Política de Gestión de Incidentes de Seguridad de la Información.
- Política de Cumplimiento.

Así mismo, se desarrollaron los siguientes procedimientos que apoyan a ciertas políticas ayudando a cumplir con los lineamientos de la NTP ISO/IEC 27001:2014:

- Procedimiento de Seguridad y Correcto uso de las Instalaciones de Procesamiento de Información. (Apoya a Política de Seguridad Física y Ambiental).
- Procedimiento de Gestión de Cambios. (Apoya a Política de Adquisición, Desarrollo y Mantenimiento de Software).

- Procedimiento de Gestión de Incidentes de Seguridad de la Información. (Apoya a Política de Gestión de Incidentes de Seguridad de la Información.)
- Procedimiento de Mantenimiento Preventivo y Correctivo de Equipos. (Apoya a Política de Seguridad de Operaciones).
- Procedimiento de Respaldo de Información. (Apoya a Política de Seguridad de Operaciones)

De igual manera se desarrollaron los siguientes formatos que apoyan a los procedimientos para la generación de evidencias:

- Formato de Declaración de Aplicabilidad SOA.
- Formato de Inducción al Personal.
- Formato de Planificación de Capacitaciones.
- Formato de Registro de Cambios.
- Formato de Registro de Incidente de Seguridad de la Información.
- Formato de Ficha de Mantenimiento Preventivo y Correctivo de Equipos.
- Formato de Lista de Contacto con Proveedores.
- Formato de Control de Respaldo de la Información (Backup).
- Formato de Prueba de Recuperación de Copias de Respaldo.
- Formato de Indicadores de Seguridad de la Información.
- Formato de Bitácora de Incidentes de Seguridad de la Información.
- Formato de Inventario de Activos.
- Formato Lista de Procedimientos Operacionales.
- Formato de Control de Envío de Copias de Respaldo a Proveedor.
- Formato de Criterios de Seguridad de Dispositivos de Red.
- Formato de Registro de Entidades de Transferencia de Información.
- Formato de Checklist de Seguridad de la Información.
- Formato de Listado de Personal Proveedor.
- Formato de Evaluación de Requisitos Legales y otros Requisitos.

A continuación, se detalla las políticas, procedimientos y formatos antes mencionados:

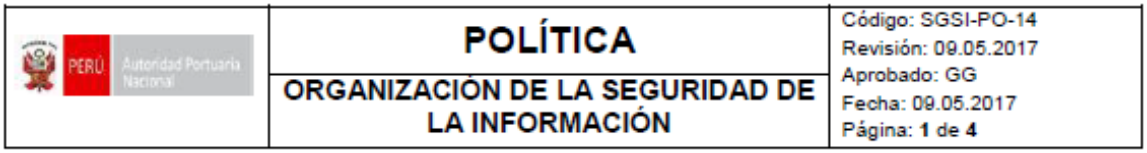


Figura 28. Política de Organización de la Seguridad de la Información. Documento interno de la Institución.

En la Figura 28, el Bachiller de acuerdo a las funciones delegadas por el jefe del Proyecto, participó en la elaboración de la mencionada Política, reuniéndose con los responsables del Comité de Seguridad de la Información para definir cuáles serán sus funciones en la implementación del SGSI de acuerdo a lo que indica la Norma y a la modificación del artículo N° 5 de la Resolución Ministerial N° 004-2016-PCM.

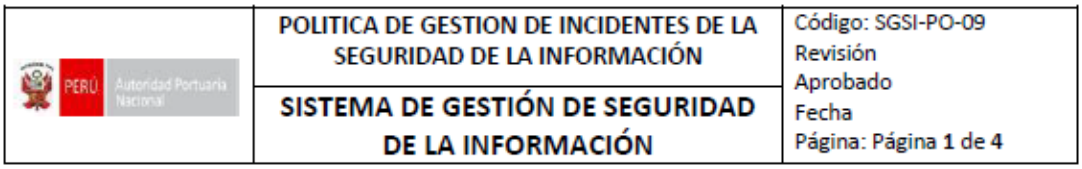


Figura 29. Política de Gestión de Incidentes. Documento interno de la institución.

En la Figura 29, el Bachiller junto con el consultor de Seguridad de la Información, se realizó reuniones con los responsables de Mesa de Ayuda para identificar el ciclo de los incidentes de Seguridad de la Información, partiendo desde su identificación hasta su solución, de acuerdo a lo que indica la Norma, luego de las reuniones, la Política fue aprobada por el Comité del SGSI y puesta en funcionamiento para la generación de evidencias.

La presente Política se apoya del Procedimiento de Gestión de Incidentes de Seguridad de la Información que se describe en la Figura 30.

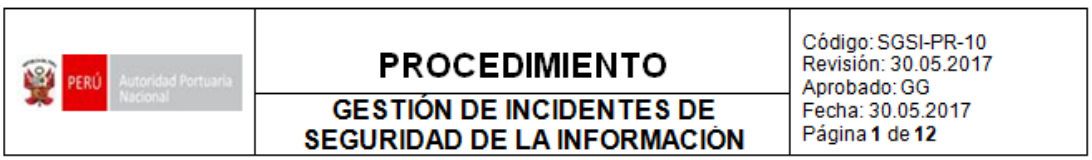


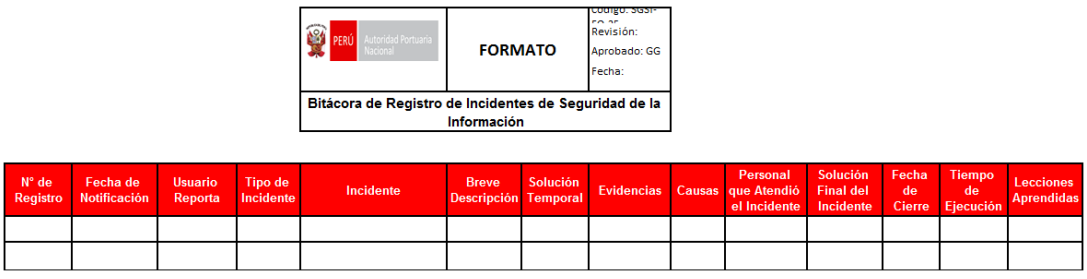
Figura 30. Procedimiento de Incidentes de Seguridad de la Información. Documento interno de la institución.

La Figura 30, el Bachiller participó en la elaboración total del documento guiándose de lo que indica la Norma y de acuerdo a las reuniones que se realizaron

con los responsables de Mesa de Ayuda, para luego ser revisado por el jefe del Proyecto y aprobado por el Comité del SGSI.

La evaluación del evento se realizará en base a los siguientes tipos indicados:

- Pérdida de servicio, equipos o instalaciones (disponibilidad del servicio de TI).
- Incumplimientos de políticas, normas y/o procedimientos sobre seguridad de la Información.
- Cambios no controlados en los sistemas (software y hardware) y servicios.
- Violaciones de acceso a los sistemas.
- Ataques por software de tipo malicioso (malware).
- Correos fraudulentos (phishing) solicitando información del usuario.
- Pérdida o fuga de Información.
- Mal uso y abuso del correo electrónico.
- Detección de vulnerabilidades de la seguridad.
- Identificación de protocolos en el tráfico de la red que sobrecargan el servicio.
- Sobrecarga de software/hardware.



PERÚ Autoridad Portuaria Nacional	FORMATO	Código: SGSI-RG-05 Revisión: Aprobado: GG Fecha:
Bitácora de Registro de Incidentes de Seguridad de la Información		

N° de Registro	Fecha de Notificación	Usuario Reporta	Tipo de Incidente	Incidente	Breve Descripción	Solución Temporal	Evidencias	Causas	Personal que Atendió el Incidente	Solución Final del Incidente	Fecha de Cierre	Tiempo de Ejecución	Lecciones Aprendidas

Figura 31. Registro de Incidentes de Seguridad de la Información. Documento interno de la institución.

En la Figura 31, de acuerdo a las funciones indicadas por el jefe del Proyecto, el Bachiller elaboró la totalidad del Formato interpretando lo indicado por la Norma, luego, se realizó una inducción a los responsables de Mesa de Ayuda para la generación de evidencias de acuerdo a lo desarrollado en el formato. El formato consta de 3 partes fundamentales:

Primera parte:

- Número de registro: Número asignado al incidente reportado.
- Fecha de notificación: Fecha en la que se produzco el incidente.
- Quien reporta: Datos del usuario que reporta el incidente.
- Tipo de incidente: Se identifica el tipo de incidente y se clasifica de acuerdo a la lista de eventos antes mencionada.
- Incidente: Se coloca el nombre del incidente identificado.

Segunda parte:

- Breve descripción: Se describe el incidente.
- Solución temporal: Se escribe la solución temporal hasta que se realice la investigación del incidente.
- Evidencias: Se escribe cómo y a través de qué fue reportado el incidente.
- Causas: Se describe cómo pasó el incidente.

Tercera parte:

- Personal que atendió el incidente: Se escribe el nombre de la persona que atendió el incidente.
- Solución final del incidente: Se describe la solución final.
- Fecha de cierre: Se indica la fecha en la que el incidente fue cerrado.
- Tiempo de ejecución: Se describe cuánto tiempo duró el incidente.
- Lecciones aprendidas: Se coloca la solución que se identificó y se almacena para futuros incidentes.

El formato es muy importante ya que cuando se realizan auditorías, se debe mostrar como evidencia la lista de incidentes de seguridad de la información reportados y cerrados. El formato pertenece al control A.16 Gestión de Incidentes de Seguridad de la Información.

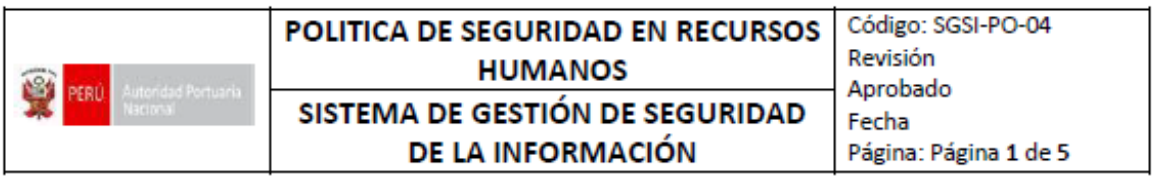
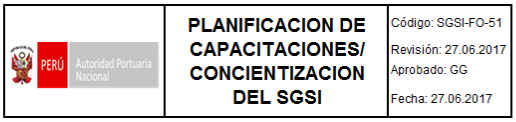


Figura 32. Política de Seguridad en Recursos Humanos. Documento interno de la institución.

En la Figura 32, el Bachiller de acuerdo a acuerdo a sus funciones participó en la totalidad de la Política, guiándose de lo indicado por la Norma, realizando reuniones con el director del proceso para identificar los lineamientos de Seguridad de la Información, respecto a Recursos Humanos, luego fue revisado por el jefe del Proyecto y aprobado por el Comité del SGSI para la generación de evidencias.

La mencionada Política se apoya en dos formatos: Planificación de Capacitaciones e Inducción al personal y proveedores que se detallan a continuación, los cuales responden a control A.7.2.2 de la norma referente a concientización, educación y capacitación en seguridad de la información.



PERÚ Autoridad Portuaria Nacional	PLANIFICACION DE CAPACITACIONES/ CONCIENTIZACION DEL SGSI	Código: SGSI-FO-51 Revisión: 27.06.2017 Aprobado: GG Fecha: 27.06.2017

Tipo de Actividad	Nombre de Actividad	Presencial / Online	¿Interna / externa?	Empresa Externa	Perfil de la audiencia objetivo	Fechas de Actividad	Horas efectivas	Costo (S/.)	Estado	Responsable de la Actividad	Comentarios / Bitácora

Figura 33. Formato de Planificación de Capacitaciones. Documento interno de la institución.

En la Figura 33, el Bachiller participó en el desarrollo del Formato de acuerdo a lo indicado por la Norma, guiándose de la Política mencionada anteriormente, en la cual se detalla la planificación y capacitación en temas de seguridad de la información al personal interno y externo.

PERÚ Autoridad Portuaria Nacional	POLÍTICA GESTIÓN DE ACTIVOS	Código: SGSI-PO-12 Revisión: 04.07.2017 Aprobado: GG Fecha: 04.07.2017 Página: 1 de 9

Figura 34. Política de Gestión de Activos. Documento interno de la institución.

En la Figura 34, de acuerdo a las funciones del Bachiller delegadas por el jefe del Proyecto, participó en la totalidad de la Política interpretando lo indicado por la Norma, así mismo, se realizó una inducción con los responsables de los procesos para implementación de la Política, luego fue revisado por el Comité del SGSI para su aprobación.

Dicha Política se apoya en el Procedimiento de Gestión de activos, el cual se detalla a continuación:

Figura 35. Procedimiento de Gestión de Activos. Documento interno de la institución.

En la Figura 35, el Bachiller participó en la elaboración del procedimiento, siguiendo las indicaciones del consultor de Seguridad de la Información e interpretando lo indicado por la Norma.

De igual manera, este procedimiento se apoya en el Formato de Inventario de Activos que se describe en la Figura 41.

Sec.	Proceso	Tipo de Activo	Categoria de Activo	Nombre del Activo	Descripción del Activo	Propietario	Ubicación (Física o lógica	Aspecto de			Valor CID	Frecuencia de uso	Estado
								C	I	D			
1								Interna	Alta	Alta	Muy Critico	Alta	Activo
2								Interna	Baja	Media	Moderado	Media	Activo

Figura 36. Formato de Inventario de Activos. Documento interno de la institución.

En la Figura 36, el Bachiller participó en la elaboración guiándose de lo desarrollado por el Procedimiento y realizando la inducción a los responsables de los procesos para ayudarlos a identificar sus activos de información, los cuales, una vez identificados se evaluaron sus riesgos.

Figura 37. Política de Control de Accesos. Documento interno de la institución.

En la Figura 37, el Bachiller de acuerdo a sus funciones, participó en la elaboración total del documento guiándose de lo indicado por la Norma y realizando reuniones con los responsables del área de Infraestructura de TI, para elaborar de

acuerdo a sus funciones la Política mencionada, una vez desarrollado la Política, fue revisada por los responsables, el jefe del Proyecto para su posterior aprobación por el Comité del SGSI.

Figura 38. Política de Criptografía. Documento interno de la organización.

En la Figura 38, para la elaboración de la Política el Bachiller tuvo que adquirir conocimientos acerca de controles criptográficos para poder interpretar lo indicado por la Norma, el mismo que fue revisado por los especialistas en cifrado para su aprobación por parte del Comité del SGSI.

Figura 39. Política de Seguridad Física y del Ambiente. Documento interno de la organización.

En la Figura 39, de acuerdo a las funciones del Bachiller, se tuvo reuniones con los especialistas en Infraestructura y Soporte para alinear lo indicado por la Norma y las responsabilidades de los mismos, dicha Política fue revisada por los especialistas para luego ser llevada al Comité del SGSI para su aprobación.

Dicha Política se apoya en el Procedimiento de Seguridad y Correcto Uso de las Instalaciones, que se detalla en la Figura 40.

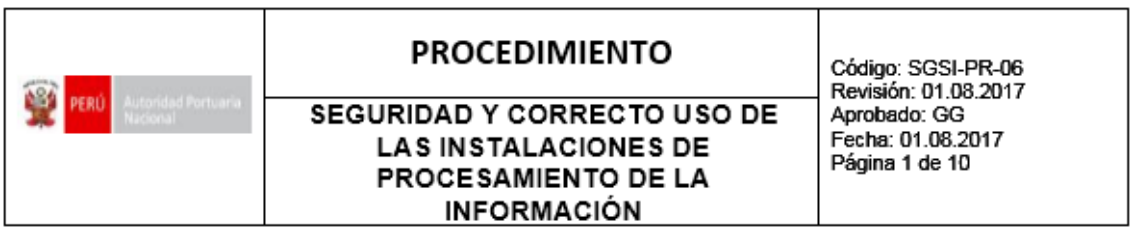


Figura 40. Procedimiento de Seguridad y Correcto Uso de las Instalaciones. Documento interno de la institución.

El Bachiller participó en la elaboración total del Procedimiento realizando reuniones con los responsables de las áreas de Almacén, Infraestructura, Soporte Técnico para alinear sus funciones y responsabilidad a lo indicado por la Norma y de esa forma sea implementado para la generación de evidencias.

Así mismo, la Política de Seguridad Física y del Ambiente también se apoya en el Procedimiento de Mantenimiento Preventivo y Correctivo de Equipos que se detalla en la Figura 41.

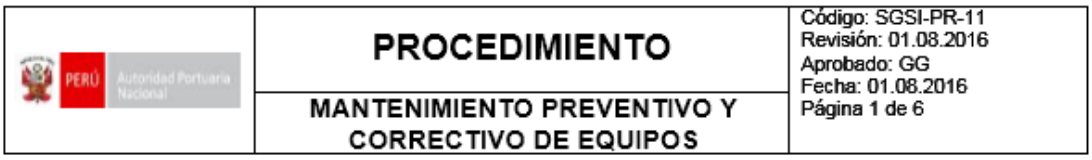


Figura 41. Procedimiento de Mantenimiento Preventivo y Correctivo de Equipos. Documento interno de la institución.

El Bachiller, de acuerdo a sus funciones delegadas por el Jefe del Proyecto, elaboró la totalidad del Procedimiento guiándose a los lineamientos de indica la Norma, el Procedimiento fue revisado por el especialista de Soporte Técnico y llevado al Comité del SGSI para su aprobación.

El procedimiento mencionado se apoya en el Formato Ficha de Mantenimiento Preventivo y Correctivo, que se detalla en la Figura 42.

	FORMATO	Código: SGSI-FO-08 Revisión: 01-08-2017 Aprobado: GG Fecha: 01-08-2017 Página 1 de 1
	FICHA DE MANTENIMIENTO	

N° de Ficha:		**Fecha de Mantenimiento:**	
Código del Equipo:			
Nombre del Personal o la Empresa que realizó el mantenimiento:			
Tipo de Mantenimiento:			
	Mantenimiento Preventivo		Mantenimiento Correctivo
Tipo de Equipo:			
	Servidor	PC	Laptop
	Scanner	Multifuncional	UPS
	Equipo de Refrigeración	Switch	Router
	Cableado de Datos del Centro de Cómputo	Cableado de Datos de Oficinas	
Características del Equipo:			
Número de Serie del Equipo:			
Detalle del Mantenimiento:			
Piezas Actualizadas:			

Nombres y Apellidos del Jefe de la OTI	**Nombres y Apellidos del Personal de Mantenimiento**
Firma del Jefe de la OTI	**Firma del Personal de Mantenimiento**

Figura 42. Formato Ficha de Mantenimiento Preventivo y Correctivo. Documento interno de la institución.

En la Figura 42, el Bachiller elaboró el Formato de acuerdo a lo indicado en el Procedimiento antes mencionado y de acuerdo a lo indicado por el especialista de Soporte Técnico, el formato de divide en 3 partes:

Primera parte:

- N° de ficha: Número asignado al mantenimiento de los equipos.
- Fecha de mantenimiento: se identifica la fecha en la se realiza el mantenimiento.
- Código del equipo: se identifica el código del equipo al que se le realizará el mantenimiento.
- Nombre del personal o la empresa que lo realiza: Se identifica a la persona o proveedor que será responsable del mantenimiento a los equipos.

- Tipo de mantenimiento: Se identifica el tipo de mantenimiento que se le realizará al equipo, ya se preventivo o correctivo.

Segunda parte:

- Tipo de equipo: Se identifica el equipo al cual se le realizará el mantenimiento.
- Características del equipo: Se identifican las características principales del equipo y se procede a llenar el espacio correspondiente.
- N° de serie: Se identifica el número de serie del equipo de acuerdo al inventario de equipos.
- Detalle del mantenimiento: Se describe todo lo realizado en el mantenimiento preventivo o correctivo.
- Piezas actualizadas: Se identifican las piezas que deben ser reemplazadas de acuerdo al diagnóstico del mantenimiento.

Tercera parte:

- Nombres y apellidos del jefe de OTI: Se coloca el nombre y firma del jefe de la OTI.
- Nombre del personal de mantenimiento: Se coloca el nombre de la persona quien realizó el mantenimiento y su firma.

Figura 43. Política de Gestión de Operaciones. Documento interno de la institución.

En la Figura 43, el Bachiller de acuerdo a sus funciones realizó reuniones junto con el consultor en Seguridad de la Información y el responsable del área de Operaciones de TI para alinear sus funciones de acuerdo a lo indicado por la Norma, para ser llevado al Comité del SGSI para su aprobación.

La política antes mencionada se apoya en el siguiente formato:

PERÚ Autoridad Portuaria Nacional	**LISTA DE PROCEDIMIENTOS OPERACIONALES**	Código: SGSI-FO-39 Revisión: 22.08.2017 Aprobado: GG Fecha: 22.08.2017

TIPO DE DOCUMENTO	NOMBRE DE DOCUMENTO	RUTA

Figura 44. Formato de Procedimientos Operacionales. Documento interno de la institución.

En la Figura 44, el Bachiller elaboró el Formato guiándose de lo indicado por la Norma, para luego ser implementado en el área de Operaciones de TI y se generen evidencias que ayudaron al realizarse la auditoría interna.

La Política mencionada se apoya en el Procedimiento de Respaldo y Recuperación de la Información que se detalla en la Figura 45.

PERÚ Autoridad Portuaria Nacional	**PROCEDIMIENTO** RESPALDO Y RECUPERACION DE LA INFORMACION	Código: SGSI-PR-09 Revisión: 22.08.2017 Aprobado: GG Fecha: 22.08.2017 Página 1 de 12

Figura 45. Procedimiento de Respaldo y Recuperación de la Información. Documento interno de la Institución.

Para la elaboración del siguiente Procedimiento el Bachiller realizó reuniones con los especialistas de Infraestructura, Soporte Técnico y Operaciones de TI, para alienar sus funciones y responsabilidades de acuerdo a lo indicado por la Norma, así mismo, se les capacitó para poder evidenciar el uso del mismo.

Dicho Procedimiento se apoya en los siguientes formatos:

PERÚ Autoridad Portuaria Nacional	**FORMATO** CONTROL DE RESPALDO DE LA INFORMACIÓN (BACKUP)	Código: SGSI-FO-06 Revisión: 22-08-2018 Aprobado: GG Fecha: 22-08-2018 Página 1 de 1

Fecha	Medios Utilizados	Recursos respaldados (Archivos, Aplicación o Sistema)	Tipo de Copia de Respaldo	Coordinador de Soporte Técnico	Firma	Observaciones

Figura 46. Formato de Control de Respaldo de la Información. Documento interno de la institución.

En la Figura 46, el Bachiller participó en la elaboración del Formato, guiándose de las responsabilidades de los especialistas, luego se realizó una asesoría para el uso del formato.

El formato se detalle de la siguiente forma:

- Fecha: Se escribe el día en el cual fue se realizó el Backup.
- Medios utilizados: A través de qué se realizó el Backup (cintas, discos duros, discos externos, etc.).
- Recursos respaldados: Qué recurso se respaldó, aplicaciones, base de datos, sistemas, códigos fuentes, etc.
- Tipo de copia de respaldo: Si se realizó un Backup completo, medio, etc.
- Coordinador de soporte técnico: Se coloca el nombre de la personal responsable del área de soporte técnico.
- Firma: La firma del responsable.
- Observaciones: Si las hubiera.

PERÚ Autoridad Portuaria Nacional	FORMATO CONTROL DE ENVIO DE COPIAS DE RESPALDO (BACKUP) A PROVEEDOR	Código: SGSI-FO-16 Revisión: 22-08-2018 Aprobado: GG Fecha: 22-08-2018 Página: Página 1 de 1

Fecha de envió a custodia	Número de Caja	Datos del Personal de la APN Remitente	Firma	Datos del Personal del Proveedor que recibe	Firma	Observaciones

Figura 47. Control de Envío de Copias de Respaldo a Proveedor. Documento interno de la institución.

En la Figura 47, el Bachiller participó en la elaboración del Formato, guiándose de las responsabilidades de los especialistas, luego se realizó una asesoría para el uso del formato.

El formato se detalla de la siguiente forma:

- Fecha de envío a custodia: Se escribe la fecha en el cual se envió el Backup.

- Número de caja: Se indica el número de la caja en el cual se envía el Backup.
- Datos del personal remitente: Se coloca el nombre del responsable que está enviando el Backup.
- Firma: Firma el responsable.
- Datos del proveedor que recibe: Se coloca el nombre de la personal que custodia el Backup.
- Firma: Firma el proveedor.
- Observaciones: Si las hubiera.

Figura 48. Política de Seguridad en Comunicaciones. Documento interno de la institución.

En la Figura 48, el Bachiller se reunió con el especialista de Infraestructura de TI para alienar sus funciones con lo indicado por la Norma, lo cual llevó a realizar un pequeño taller para explicar el control referido a Seguridad en las Comunicaciones.

La Política antes mencionada se apoya en el Procedimiento que se describe a continuación:

Figura 49. Procedimiento de Seguridad en Comunicaciones. Documento interno de la institución.

En la Figura 49, el Bachiller en conjunto con el consultor en Seguridad de la Información se elaboró el procedimiento mencionado de acuerdo a las funciones y responsabilidades de los especialistas, para luego realizar una asesoría para el uso del Procedimiento.

El procedimiento antes mencionado se apoya de los siguientes formatos:

PERÚ Autoridad Portuaria Nacional	**CRITERIOS DE SEGURIDAD DE DISPOSITIVOS DE RED**	Código: SGSI-FO-22 Revisión: 12.09.2017 Aprobado: GG Fecha: 12.09.2017

		Relación de equipos de comunicaciones			
Item	riterio de la Seguridad de los dipositivos de RE	Equipo 1	Equipo 2	Equipo 3	Equipo 4
1	Tiene filtro de acceso al switch por IP				
2	El acceso esta centralizado a traves de un				
3	Las contraseñas estan encriptadas				
4	El acceso es a traves de un protocolo encriptado (Ej. SSH, HTTPS)				
5	Las interfaces que estan desconectadas, se encuentran en shutdown				
6	Tiene el equipo de comunicaciones				

Figura 50. Formato de Criterios de Seguridad de Dispositivos de Red. Documento interno de la institución.

En la Figura 50, el Bachiller elaboró el Formato de acuerdo a los criterios mínimos de seguridad que deben cumplir los equipos de comunicación, luego se asesoró al responsable de Infraestructura de TI para su uso.

PERÚ Autoridad Portuaria Nacional	**Registro de Entidades de Transferencia de Información**	Código: SGSI-FO-31 Revisión:12.09.2017 Aprobado: GG Fecha: 12.09.2017

Item	Empresa/Entidad	IP pública con la que se conecta	Existe acuerdo firmado?	Fecha
1				
2				
3				
4				
5				

Figura 51. Formato de Registro de Entidades de Transferencia de Información. Documento interno de la Institución.

En la Figura 51, el Bachiller elaboró el Formato de acuerdo a lo indicado por la Norma en el control referido a Seguridad en las Comunicaciones, así mismo, realizó asesorías al responsable de Infraestructura para su uso.

PERÚ Autoridad Portuaria Nacional	**POLÍTICA** **ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**	Código: SGSI-PO-05 Revisión: 26.09.2017 Aprobado: GG Fecha: 26.09.2017 Página: 1 de 7

Figura 52. Política de Adquisición, Desarrollo y Mantenimiento de Software. Documento interno de la institución.

En la Figura 52, el Bachiller tuvo que capacitarse en temas relacionados al desarrollo de software y de esa forma, realizar reuniones con los especialistas del área de Sistemas de Información para alinear sus funciones de acuerdo a lo indicado por la Norma, la Política fue revisada por los especialistas para luego ser llevada al Comité del SGSI para su aprobación.

La Política mencionada se apoya en el siguiente formato que se describe a continuación:

PERÚ Autoridad Portuaria Nacional	**CHECKLIST- Requerimientos de seguridad de la Información**	Código: SGSI-FO-21 Revisión: 26-09-2018 Aprobado: GG Fecha: 26-09-2018

Aplicativo:	
Fecha:	
Área:	
Evaluador:	
Hora Inicio:	
Hora Fin:	

	Si Cumple	No Cumple
1.- Análisis		
Evaluar requerimientos/especificaciones acorde a los procedimientos y procesos de la organización.		
Evaluar riesgos de seguridad de la información.		
2.- Diseño		
Cumplir con los estandares de programación.		
Cumplir con los estandares de Base de Datos		

Figura 53. Formato de Checklist de Seguridad de la Información. Documento interno de la institución.

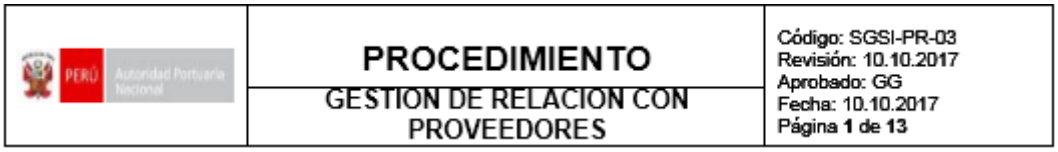
En la Figura 53, el Bachiller desarrolló el Formato de acuerdo a los lineamientos del control de Desarrollo de Sistemas de Información, guiándose de lo indicado por la Norma, realizando asesorías a los especialistas para su uso.

	POLÍTICA	Código: SGSI-PO-06 Revisión: 10.10.2017 Aprobado: GG Fecha: 10.10.2017 Página **1** de **10**
PERÚ Autoridad Portuaria Nacional	RELACIONES CON LOS PROVEEDORES	

Figura 54. Política de Relación con Proveedores. Documento interno de la institución.

En la Figura 54, el Bachiller realizó reuniones con los responsables del área de Administración para verificar como se realizan con contratos con los proveedores, luego, se alineó sus funciones de acuerdo a lo indicado por la Norma, se revisó el documento desarrollado por el director del área y fue llevado al Comité del SGSI para su aprobación.

La Política antes mencionada se apoya del siguiente procedimiento:



	PROCEDIMIENTO	Código: SGSI-PR-03 Revisión: 10.10.2017 Aprobado: GG Fecha: 10.10.2017 Página **1** de **13**
PERÚ Autoridad Portuaria Nacional	GESTION DE RELACION CON PROVEEDORES	

Figura 55. Procedimiento de Relación con los Proveedores. Documento interno de la institución.

En la Figura 55, el Bachiller elaboró en su totalidad el Procedimiento mencionado, guiándose de las responsabilidades del área de Administración, luego fue revisado por el director del área el mismo que fue llevado al Comité del SGSI para su aprobación e implementación.

El procedimiento antes mencionado se apoya del siguiente formato:

	LISTA PERSONAL PROVEEDOR	Código: SGSI-FO-28 Revisión: 12.09.2017 Aprobado: GG Fecha: 12.09.2017
PERÚ Autoridad Portuaria Nacional		

Nombre Completo	*Apellido Paterno*	*Apellido Materno*	*Fecha Fin de contrato*	*Perfil*	*Tipo de Documento*	*N° de documento*	*FotocheckK*	*Constancia de recepción y de aceptación de la política*

Figura 56. Formato de Listado de Personal Proveedor. Documento interno de la Institución.

En la Figura 56, el Bachiller elaboró el Formato guiándose de lo indicado por Norma y de esa forma cumplir con el Control alineado a Seguridad con Proveedores.

PERÚ Autoridad Portuaria Nacional	**POLÍTICA** CUMPLIMIENTO	Código: SGSI-PO-08 Revisión: 26.09.2017 Aprobado: GG Fecha: 26.09.2017 Página **1** de **4**

Figura 57. Política de Cumplimiento. Documento interno de la institución.

En la Figura 57, el Bachiller tuvo que recibir asesorías legales respecto a Seguridad de la Información y de esa forma, reunirse con los especialistas legales y alinear sus funciones de acuerdo a lo indicado por la Norma, la Política fue revisada por el director de área Legal y llevada al Comité para su aprobación e implementación.

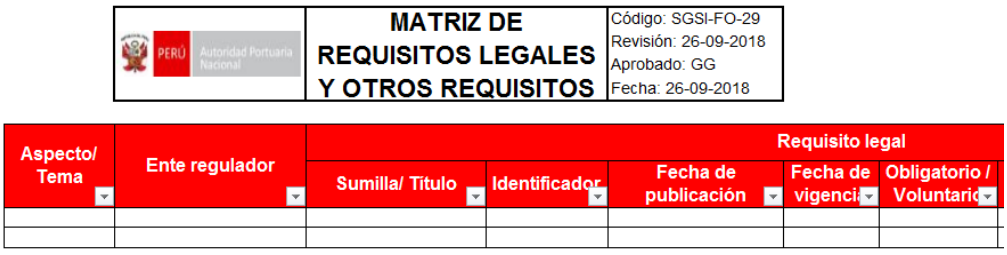
La Política antes mencionada se apoya del procedimiento que se detalla a continuación:

PERÚ Autoridad Portuaria Nacional	**PROCEDIMIENTO** GESTION DE CUMPLIMIENTO	Código: SGSI-PR-02 Revisión: 26.09.2017 Aprobado: GG Fecha: 26.09.2017 Página **1** de **10**

Figura 58. Procedimiento de Cumplimiento. Documento interno de la institución.

En la Figura 58, el Bachiller en conjunto con el consultor de Seguridad de la Información se elaboró el Procedimiento antes mencionado de acuerdo a lo indicado por la Norma, con la finalidad de cumplir el Control referido a Cumplimiento Legal.

El procedimiento antes mencionado se apoya del siguiente formato que se describe a continuación:



PERÚ Autoridad Portuaria Nacional	**MATRIZ DE REQUISITOS LEGALES Y OTROS REQUISITOS**	Código: SGSI-FO-29 Revisión: 26-09-2018 Aprobado: GG Fecha: 26-09-2018

Aspecto/ Tema	Ente regulador	Requisito legal				
		Sumilla/ Título	Identificador	Fecha de publicación	Fecha de vigenci	Obligatorio / Voluntario

Figura 59. Formato de Evaluación de Requisitos Legales y otros Requisitos. Documento interno de la institución.

En la Figura 59, el Bachiller elaboró el Formato de acuerdo a los lineamientos del Control de Cumplimiento y se realizaron asesorías a los especialistas para su uso y generación de evidencias para las auditorías.

PERÚ Autoridad Portuaria Nacional

SEGUIMIENTO Y MEDICION DE INDICADORES DEL SGSI

			Resultado Medición							
Objetivos de Control y Controles	Indicador - Meta	Frecuenci	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto
A.5 Políticas de seguridad de la información										
A.5.1 Gestión de la Gerencia para la seguridad de la información										
A.5.1.1 - Políticas de la seguridad de la información		Anual								
A.6 Organización de la seguridad de la información										
A.6.1 Organización interna										
A.6.1.5 - Seguridad de la información en la gestión del proyecto		Semestral								
A.7 Seguridad de los recursos humanos										
A.7.1. Antes de reclutarlo										
A.7.1.1 - Filtración		Mensual								
A.7.1.2 - Términos y condiciones del empleo		Mensual								

Figura 60. Formato de Métricas del SGSI. Documento interno de la organización.

En la Figura 60, el Bachiller elaboró el Formato de Indicadores guiándose de lo indicado por la Norma, de igual manera, elaboró los indicadores para los controles seleccionados de acuerdo a la reunión que se sostuvo con Alta Dirección.

3.4 Control y Seguimiento

De acuerdo a lo indicado por la Norma en el requisito 9.2 (Auditoría interna), indica lo siguiente:

La organización de acuerdo al requisito de mejora continua de la norma debe planificar, establecer, implementar y mantener uno o varios programas de auditoría, de esa forma asegurarse que el Sistema de Gestión de Seguridad de la Información ha sido implementado de forma correcta respecto a los controles seleccionados e implementados. La organización debe considerar las auditorías previas para definir el alcance, la selección de auditores y conducir al SGSI hacia los objetivos definidos y de esa forma reportar a la alta gerencia los resultados obtenidos de los programas de auditorías. A continuación, se adjunta el plan de auditoría:

PLAN DE AUDITORÍA INTERNA

ORGANIZACION	AUTORIDAD PORTUARIA NACIONAL		
AUDITORÍA INTERNA N°	2	**FECHA DE EJECUCIÓN**	10, 12 y 16 de Octubre de 2017
OBJETIVO	Verificar la implementación, cumplimiento y eficacia del Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001:2013, los requisitos legales aplicables y el logro de los objetivos propuestos para identificar oportunidades que permitan mejorar el sistema.		
ALCANCE	Sistema de Gestión de Seguridad de la Información comprende los siguientes procesos: "Gestión de Licencias, Gestión de Recepción y Despacho de Naves" y "Gestión de Sistemas de Información"		
CRITERIO DE AUDITORIA	- Norma ISO/IEC 27001:2013. - Documentación del Sistema de Gestión de Seguridad de la Información		
LUGAR DE AUDITORÍA	Av. Santa Rosa 135, La Perla, Callao	**IDIOMA DE AUDITORÍA**	Español

EQUIPO AUDITOR	**NOMBRE Y APELLIDO**	**FUNCIÓN**	**ABREVIATURA**
	José Luis Sandoval	Auditor Líder	JLS

EXCLUSIONES	A.10.1.2 Gestión de claves A.18.1.5 Regulación de controles criptográficos A.6.1 Teletrabajo

PROGRAMACIÓN DE ACTIVIDADES

FECHA	HORARIO	AUDITOR	UNIDAD / PROCESO DE LA ORGANIZACIÓN	REQUISITO	ENTREVISTADO
10/10/2017	09:00 - 09:30	JLS	Reunión de Apertura		
	09:30 - 10:30	JLS		Liderazgo y compromiso (5.1) Política (5.2.) Objetivos (6.2) Políticas de Seguridad de la Información (A.5)	
	10:30 -11:00	JLS		Entendimiento de la Organización y su contexto (4.1)	
	11:00 - 11:30	JLS		Entendimiento de las Necesidades y Expectativas de las Partes Interesadas (4.2)	
	11:30 - 12:00	JLS		Determinación del Alcance (4.3)	
	12:00 - 13:00	JLS		Roles Organizacionales, Responsabilidades y Autoridades (5.3), Organización de la Seguridad de la Información (A.6)	
	13:00 - 14:00	Almuerzo			
	14:00 - 15:00	JLS		Acciones para Atender Riesgos y Oportunidades (6.1) Objetivos de la Seguridad de la Información (6.2) Planificación y control operacional (8.1)	
	15:00 - 16:00	JLS		Apreciación de Riesgos de Seguridad de la Información (6.1.2) Apreciación de los riesgos de Seguridad de la Información(8.2)	
16/10/2017	10:00 - 11:30	JLS		Gestión de Eventos e Incidentes (A.16)	
	11:30 - 13:00	JLS		Control de Acceso (A.9)	
	13:00 - 14:00	Almuerzo			
	14:00 - 15:00	JLS		Gestión de Activos (A.8)	
	15:00 - 15:30	JLS		Revisión Gerencial (9.3) Mejora Continua (10.2)	
	15:30 - 16:30	JLS		Recursos (7.1)	
	16:30 - 17:00	JLS		Seguimiento, medición, análisis y evaluación (9.1)	
	17:00 - 17:30	JLS	Preparación del Informe final		
	17:30 - 18:00	JLS	Reunión de cierre de auditoría		

CONSIDERACIONES:
1. La puntualidad y el cumplimiento de la agenda es imprescindible, por lo cual los responsables de los subprocesos deberán disponer del tiempo necesario según agenda.
2. Los auditores internos en entrenamiento, en caso se estime, deberán acompañar como auditores observadores por lo menos 3 horas, según agenda adicional de auditores observadores.

Figura 61. Plan de auditoría interna. Documentación interna de la institución.

3.5 Cierre

3.5.1 Introducción

En esta etapa del proyecto se detallan las actividades realizadas durante la implementación de la NTP ISO/IEC 27001:2014 en la Autoridad Portuaria Nacional en cumplimiento a la Resolución Ministerial N° 004-2016-PCM.

Esta resolución obliga a todas las entidades integrantes del Sistema Nacional de Información a implementar la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos”. En la cual se definen las actividades de implementación del Sistema de Gestión de Seguridad de la Información en base a la NTP ISO/IEC 27001:2014 que permite mantener la confidencialidad, integridad y disponibilidad de la información y la de los activos de información de los servicios que son críticos para la ejecución y entrega de los mismos que son prestados por la APN a los ciudadanos y entidades del estado y/o privadas.

3.5.2 Resumen

El presente proyecto tuvo una duración de 8 meses, en la cual se realizaron las actividades definidas en las bases del proyecto, las cuales fueron dispuestas en 3 fases:

- Fase I – Organización.
- Fase II – Planificación.
- Fase III – Despliegue.

Al inicio del proyecto se identificó que no existía un SGSI y que solo existía algunos controles relacionados a seguridad, que habían sido desarrollados por el área de OTI, por lo tanto, se realizaron las siguientes actividades a manera general:

- Realizar el diseño del SGSI, el cual incluía determinar el alcance y la política del SGSI y a partir de allí, desarrollar los documentos que gestionen el SGSI.
- Realizar talleres de sensibilización al personal.
- Capacitar al equipo responsable del proyecto.

- Definir la metodología para la gestión de riesgos y oportunidades de seguridad de la información.
- Desarrollar controles de seguridad de la información.

Como resultado de estas actividades se desarrollaron documentos los cuales fueron revisados, aprobados y difundidos en la institución, de tal forma que sean aplicados por los usuarios.

Luego de realizar la difusión y aplicación, se debe realizar la medición de los controles implementados, el cual permitirán verificar su efectividad.
Cuando se cumplan con las actividades mencionadas se realizarán auditorías internas al SGSI, así como también la revisión del SGSI por parte de la alta dirección y proceder a realizar la mejora continua del SGSI, tal como lo define la propia norma.

3.5.3 Actividades del proyecto

Se realizaron las siguientes actividades para la implementación del SGSI:

Fase I

- Se realizó un diagnóstico inicial para verificar el estado del SGSI en la APN.
- Se desarrolló el taller de sensibilización del SGSI con el objetivo de presentar al personal interno de la organización la importancia y beneficios que brinda una adecuada gestión de riesgos mediante la implementación de un sistema de gestión de seguridad de la información para poder obtener el apoyo institucional.

Fase II

- Se desarrolló la Política de Seguridad de la Información y objetivos.
- Se definió la comprensión de la institución y su contexto.
- Se identificaron las partes interesadas internas y externas de la institución.
- Se determinó el alcance del SGSI, el cual se encuentra en el Manual del SGSI.
- Se desarrollaron las funciones y responsabilidades del comité del SGSI.

- Se definió los formatos para las políticas, procedimientos, manuales, directivas.
- Se verificación las capacidades, competencias y concientización en seguridad de la información.
- Se definió el plan de comunicaciones.
- Se definió la Metodología de Gestión de Riesgos y Oportunidades.
- Se diseñó la Matriz de Riesgos.
- Se identificó, clasificó activos de información.
- Se identificaron, clasificaron y evaluaron riesgos de seguridad de la información.
- Se desarrolló el Plan de Tratamiento de Riesgos.

Fase III

- Se definió y desarrolló el formato a utilizar para la Declaración de Aplicabilidad (SOA), el cual contiene los objetivos de control y controles de seguridad de la información.
- Se desarrollaron los controles de Seguridad de la Información que se encuentran en el Anexo A.
- Se definieron métricas que permitan obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles a nivel operativo y de gestión.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 CONCLUSIONES

1. Se estableció el marco de gestión de la seguridad de la información de acuerdo a los requerimientos de la NTP ISO/IEC 27001:2014 el cual se encuentra documentado en el Manual del SGSI el cual es claro porque cuenta con un lenguaje no técnico y puede ser entendido por cualquier usuario, y estructurado porque sigue los lineamientos que indica la norma. (Ver Fig. 16)
2. Al implementar el SGSI se dio cumplimiento a la Resolución Ministerial N° 004-2016-PCM, implantando controles de seguridad que ayudarán a la organización a tener una ventaja competitiva y reducir costos asociados a los riesgos. (Ver anexo 3).
3. Se desarrolló la metodología de análisis de riesgos y oportunidades, la cual permitió cumplir con lo siguiente: (Ver Fig. 20)

   3.1 Identificar los riesgos y oportunidades de seguridad de la información a los que se encuentran expuestos los procesos que forman parte del alcance de la APN.

   3.2 Evitar impactos de pérdidas por fuga, corrupción, acceso no autorizado o indisponibilidad de la información, que afecta la confidencialidad, integridad y disponibilidad de la información.

   3.3 Establecer actividades para gestionar y mejorar de forma continua los riesgos y sus controles, a través del tratamiento de riesgos del SGSI.

4 Se realizó una auditoría interna al SGSI, la cual permite con su ejecución identificar cíclicamente las debilidades de seguridad y las áreas a mejorar. (Ver Fig. 61)

5 Se desarrollaron talleres de capacitación, que permitieron que el personal a cargo de la gestión del SGSI incremente su capacidad y habilidad para la Gestión de la Seguridad de la Información y sus mejores prácticas. (Ver Fig. 11, anexo 4)

Finalmente, como resultado del proyecto, se concluye en tres aspectos importantes:

- El cumplimiento de la Resolución Ministerial obligatoria para todas las entidades del sector informático del estado.

- La implantación de una cultura de seguridad de la información desde la alta dirección hacia los usuarios.

- El desarrollo de este proyecto puede ser usado como modelo para que sea aplicado en otras organizaciones.

4.2 RECOMENDACIONES

De la ejecución este proyecto, se toman algunas lecciones aprendidas, que se sugieren tener en cuenta en proyectos futuros:

1. Se recomienda mantener formalmente un Comité de Sistema de Gestión de la Seguridad de la Información, de manera permanente, durante la ejecución del proyecto y posterior a su implantación, a fin de asegurar la mejora continua.

2. Implementar tres controles de COBIT referidos a la seguridad de la información y dado que estos se ponen en práctica desde el punto organizacional, siendo un complemento de la seguridad de la información, desde el punto de vista de la ISO 27001, los cuales son: Dominio APO (Alinear, Planificar y Optimizar), Dominio BAI (Construir, Adquirir e Implementar) y Dominio DSS (Entrega, Servicio y Soporte). Con la finalidad de complementar los controles de la Norma. (Ver Fig. 8)

REFERENCIAS BIBLIOGRÁFICAS

WEB

Alvites, E. (2016). Sistemas de Información.

Recuperado de https://www.mindmeister.com/es/801699804/sistemas-de-informacion

Arauzo, M. (s.f.). Metodología de Análisis de riesgos para Iso 2000.

Recuperado de http://www.doitsmart.es/metodologia-analisis-riesgos-iso20000-parte-1.php

Bernal, J. J. (2013). Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua.

Recuperado de https://www.pdcahome.com/5202/ciclo-pdca/

C Seaoane, R. (2010). Seguridad Informática.

Recuperado de https://issuu.com/juanjesustorresvalero/docs/seguridad_inform_tica/4

ESAN. (2016). Los cinco principios de COBIT 5.

Recuperado de https://www.esan.edu.pe/apuntes-empresariales/2016/06/los-cinco-principios-de-cobit-5/

ISO 27000. (2012). El Portal de ISO 27001.

Recuperado de http://www.iso27000.es/glosario.html#section10s

ISO 27000. (2012). ¿Qué es un SGSI?

Recuperado de http://www.iso27000.es/sgsi.html

ISO 27000.es. (2012). Serie 27000.

Recuperado de http://www.iso27000.es/iso27000.html

ISOTools. (2015). ISO 27001: Pilares fundamentales de un SGSI.

Recuperado de https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/

ISOTools. (2016). ISO 27001: Evaluación y tratamiento de riesgos en 6 pasos. Recuperado de http://www.isotools.com.co/iso-27001-evaluacion-tratamiento-riesgos-6-pasos/

Izamorar. (2017). Componentes de un Sistema de Información.

Recuperado de https://izamorar.com/componentes-de-un-sistema-de-informacion/

Jimenez, D. (2014). Definición de Riesgo en el DIS ISO 9001:2015 - Un breve Análisis.

Recuperado de https://www.pymesycalidad20.com/definicion-de-riesgo-iso90012015.html

Lujan, U. N. (s.f.). Taller de Gestión de Riesgos.

Recuperado de www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

METODOSS. (2018). Metodología PDCA - Ciclo Deming.

Recuperado de https://metodoss.com/metodologia-pdca-ciclo-shewhart-deming/

Miranda, W. (2012). SISTEMAS DE INFORMACIÓN.

Recuperado de http://es.calameo.com/read/001699373fff605fe8006

Nacional, A. P. (2016). Misión.

Recuperado de https://www.apn.gob.pe/site/nosotros/mision-vision-valores.aspx

Nacional, A. P. (2016). Oficina de Tecnologías de la Información.

Recuperado de https://www.apn.gob.pe/site/nosotros/tecnologias-de-la-informacion.aspx

PAE. (2012). MAGERIT - versión 3.0. Metodología de Ánalisis y Gestión de Riesgos de los Sistemas de Información.

Recuperado de http://administraciónelectronica.gob.es

Pecert. (2014). ISO-IEC-27001-2014.

Recuperado de http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

Peña, J. Á. (2013). Un vistazo general de COBIT for Risk.

Recuperado de https://www.isaca.org/chapters7/Monterrey/Events/Documents/20133110_COBIT_5_for_Risk.pdf

PMG-SSI. (2015). ISO 27001 - El modelo de madurez de la Seguridad de la Información.

Recuperado de https://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de-madurez-de-la-seguridad-de-la-informacion/

PMG-SSI. (2015). ISO 27001: El modelo de madurez de la seguridad de la información.

Recuperado de http://www.pmg-ssi.com/2015/02/iso-27001-el-modelo-de-madurez-de-la-seguridad-de-la-informacion/

Ponce, N. (2017). Confianza, control y seguridad de la información.

Recuperado de http://www.i-parkman.com/es/articulos/derecho-de-la-propiedad-industrial/2261-confianza-control-y-seguridad-de-la-informacion

Welivesecurity. (2015). COBIT para la seguridad en las organizaciones. Recuperado de https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

LIBROS

ISACA. (2012). *COBIT 5 Procesos Catalizadores.*

Recuperado de http://cotana.informatica.edu.bo/downloads/COBIT5-Framework-Spanish.pdf

ANEXOS

Anexo 1: Cronograma del proyecto.

Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
IMPLEMENTACION DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	173 días	mié 01/03/17	vie 27/10/17	
FASE 1: Organización	36 días	mié 01/03/17	mié 19/04/17	
Etapa 1: Diagnóstico Inicial	19 días	mié 01/03/17	lun 27/03/17	
Plan de auditoria	3 días	mié 01/03/17	vie 03/03/17	
Diagnóstico inicial del estado del SGSI en APN	10 días	lun 06/03/17	vie 17/03/17	4
Elaboración de informe	10 días	lun 06/03/17	vie 17/03/17	4
Presentación de Resultado del diagnostico	5 días	lun 20/03/17	vie 24/03/17	6
Entrega del informe	1 día	lun 27/03/17	lun 27/03/17	7
Etapa 2: Capacitación, Sensibilización	17 días	mar 28/03/17	mié 19/04/17	
Sensibilización a la Alta Dirección	5 días	mar 28/03/17	lun 03/04/17	8
Capacitación Interpretación de la NTP ISO/IEC 27001:2014	10 días	mar 04/04/17	lun 17/04/17	10
Entrega del informe parcial de capacitación	1 día	mar 18/04/17	mar 18/04/17	11
Entrega del informe	1 día	mié 19/04/17	mié 19/04/17	12
FASE 2: Planificación	85 días	mar 04/04/17	lun 31/07/17	
Etapa 3: Implementación de los requisitos NTP ISO/IEC 27001:2014	40 días	mar 04/04/17	lun 29/05/17	
Política del SGSI	5 días	mar 04/04/17	lun 10/04/17	10
Objetivos del SGSI	5 días	mar 11/04/17	lun 17/04/17	16
Comprensión de la organización y su contexto	5 días	mar 18/04/17	lun 24/04/17	17
Identificación de partes interesadas, internas y externas	5 días	mar 25/04/17	lun 01/05/17	18
Definición del Alcance	5 días	mar 02/05/17	lun 08/05/17	19
Asignación de Roles y Responsabilidades	5 días	mar 09/05/17	lun 15/05/17	20

Definición de Competencias, Concientización y Comunicación	5 días	mar 16/05/17	lun 22/05/17	21
Definición y creación de la información documentada	5 días	mar 23/05/17	lun 29/05/17	22
Revisión de Competencias, Plan de Comunicación y Documentación	5 días	mar 23/05/17	lun 29/05/17	22
Etapa 4: Implementación de la gestión de riesgos NTP ISO/IEC 27001:2014	45 días	mar 30/05/17	lun 31/07/17	
Definición de Metodología de Gestión de Riegos	5 días	mar 30/05/17	lun 05/06/17	24
Diseño de Matriz de Riesgo	5 días	mar 06/06/17	lun 12/06/17	26
Identificación, Inventario, Clasificación y Tasación de Activos de Información	20 días	mar 13/06/17	lun 10/07/17	27
Identificación de Amenazas y Vulnerabilidades, análisis y evaluación de riesgos	10 días	mar 11/07/17	lun 24/07/17	28
Desarrollo del Plan de Tratamiento de Riesgos	5 días	mar 25/07/17	lun 31/07/17	29
FASE 3: Despliegue	144 días	mar 11/04/17	vie 27/10/17	
Etapa 5: Implementación de controles Anexo A NTP ISO/IEC 27001:2014	135 días	mar 11/04/17	lun 16/10/17	
Desarrollo del SOA	5 días	mar 11/04/17	lun 17/04/17	16
A.5 Políticas de seguridad de la información	15 días	mar 18/04/17	lun 08/05/17	33
A.6 Organización de la seguridad de la información	15 días	mar 09/05/17	lun 29/05/17	34
A.16 Gestión de los incidentes de seguridad de la información	15 días	mar 30/05/17	lun 19/06/17	35
A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio	5 días	mar 20/06/17	lun 26/06/17	36
A.7 Seguridad de los recursos humanos	5 días	mar 27/06/17	lun 03/07/17	37
A.8 Gestión de los Activos	5 días	mar 04/07/17	lun 10/07/17	38
A.9 Control de acceso	10 días	mar 11/07/17	lun 24/07/17	39
A.10 Criptografía	5 días	mar 25/07/17	lun 31/07/17	40
A.11 Seguridad física y medioambiental	15 días	mar 01/08/17	lun 21/08/17	41
A.12 Seguridad de las operaciones	15 días	mar 22/08/17	lun 11/09/17	42
A.13 Seguridad de las comunicaciones	10 días	mar 12/09/17	lun 25/09/17	43

A.14.1Adqusición, desarrollo y mantenimiento del sistema	10 días	mar 26/09/17	lun 09/10/17	44
Desarrollo del Dominio A.15 Relación con los proveedores	5 días	mar 10/10/17	lun 16/10/17	45
Desarrollo del Dominio A.18 Cumplimiento	5 días	mar 26/09/17	lun 02/10/17	44
Manual del SGSI	5 días	mar 03/10/17	lun 09/10/17	47
Etapa 6: Evaluación del SGSI	10 días	mar 10/10/17	lun 23/10/17	
Envío del plan de auditoría interna	5 días	mar 10/10/17	lun 16/10/17	48
Realización de la Auditoría Interna 1	5 días	mar 10/10/17	lun 16/10/17	48
Informe de auditoría interna 1	5 días	mar 17/10/17	lun 23/10/17	50
Definición del plan para las acciones correctivas	5 días	mar 17/10/17	lun 23/10/17	51
Etapa 7: Cierre del proyecto	4 días	mar 24/10/17	vie 27/10/17	
Informe final del proyecto	4 días	mar 24/10/17	vie 27/10/17	53

Anexo 2: Norma Técnica Peruana ISO/IEC 27001:2014.

NORMA TÉCNICA PERUANA

NTP-ISO/IEC 27001 2014

Comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias - INDECOPI
Calle de La Prosa 104, San Borja (Lima 41) Apartado 145 Lima, Perú

TECNOLOGÍA DE LA INFORMACIÓN. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

INFORMATION TECHNOLOGY. Security techniques. Information security management systems — Requirements

(EQV. ISO/IEC 27001:2013+ISO/IEC 27001:2013/COR.1 Information technology -- Security techniques – Information security management systems – Requirements)

2014-11-20
2ª Edición

R.0129-2014/CNB-INDECOPI. Publicada el 2014-12-01 Precio basado en 36 páginas
I.C.S.: 35.040 ESTA NORMA ES RECOMENDABLE
Descriptores: Tecnología, información, técnicas, seguridad, sistema de gestión, requisitos

Anexo 3: Resolución Ministerial N° 004:2016-PCM.

Aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática

RESOLUCIÓN MINISTERIAL
Nº 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2ª. Edición", en todas las entidades del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial Nº 197-2011-PCM, se estableció el plazo para que determinadas entidades de la Administración Pública implementen el Plan de Seguridad de la Información dispuesto en la Norma Técnica Peruana antes señalada; posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008;

Que, la Norma Técnica Peruana "NTP ISO/IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos", aprobada mediante Resolución Nº 42-2008/INDECOPI-CNB, por la Comisión de Normalización y de Fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual (INDECOPI) ha sido reemplazada por la nueva versión de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos.2ª Edición" aprobada por Resolución Nº 129-2014/DNB-INDECOPI;

Que, de acuerdo a lo establecido en el numeral 4.8 del artículo 4 y el artículo 49 del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo Nº 063-2007-PCM, la Presidencia del Consejo de Ministros actúa como ente rector del Sistema Nacional de Informática a través de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), siendo ésta la encargada de implementar la Política Nacional de Gobierno Electrónico e Informática;

Que, el "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0" aprobado mediante Decreto Supremo Nº 066-2011-PCM, establece en su Objetivo Nº 7, la necesidad de promover una Administración Pública de calidad orientada a la población, determinando como parte de su Estrategia Nº 4, la implementación de mecanismos para mejorar la seguridad de la información, la necesidad de contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros;

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo Nº 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

Que, estando a lo indicado en los considerandos precedentes la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros a través del Memorando Nº 152-2015-PCM/ONGEI, recomienda la aplicación y uso de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo;

De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo Nº 063-2007-PCM y sus modificatorias;

SE RESUELVE:

Artículo 1.- De la aprobación
Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Artículo 2.- Publicación
La Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2ª Edición" será publicada en el Portal de la Presidencia del Consejo de Ministros (www.pcm.gob.pe) y en el Portal de la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) (www.ongei.gob.pe) el mismo día de la publicación de la presente resolución en el Diario Oficial El Peruano.

Artículo 3.- De la implementación
Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

La ONGEI brindará asistencia técnica a las entidades que lo requieran. Las entidades públicas que a la fecha cuenten con la certificación ISO 27001, están exoneradas del presente proceso de implementación.

Artículo 4.- De la certificación de la norma
Las entidades que requieran certificarse de acuerdo a lo establecido en la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2 Edición"; podrán realizar dicha certificación de forma opcional y con recursos propios de cada entidad.

Artículo 5.- Del Comité de Gestión de Seguridad de la Información
Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

- El/la titular de la entidad;
- El/la responsable de administración o quien haga sus veces;
- El/la responsable de planificación o quien haga sus veces;
- El/la responsable del área de informática o quien haga sus veces;
- El/la responsable de área legal o quien haga sus veces y
- El/la oficial de seguridad de la información.

Las funciones del Comité de Gestión de Seguridad de la Información, serán establecidas por cada entidad de acuerdo a la norma que se aprueba mediante el Artículo 1º de la presente Resolución Ministerial.

Artículo 6.- De la responsabilidad de la implementación
La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto
Deróguese la Resolución Ministerial Nº 129-2012-PCM.

Regístrese, comuníquese y publíquese.

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1333015-1

AGRICULTURA Y RIEGO

Delegan facultades a diversos funcionarios del Ministerio durante el Ejercicio 2016

RESOLUCIÓN MINISTERIAL
Nº 0006-2016-MINAGRI

Lima, 12 de enero de 2016

CONSIDERANDO:

Que, mediante la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo, se definen las funciones generales y la estructura orgánica de los Ministerios, precisando en el último párrafo de su artículo 25, que los Ministros de Estado pueden delegar, en los funcionarios de su cartera ministerial, las facultades y atribuciones que no sean privativas a su función, siempre que la normatividad lo autorice;

Que, de acuerdo a lo dispuesto en el último párrafo del artículo 9 del Decreto Legislativo N° 997, Decreto Legislativo que aprueba la Ley de Organización y Funciones del Ministerio de Agricultura, modificado por la Ley N° 30048, en adelante la LOF del MINAGRI, el Ministro puede delegar las facultades y atribuciones que no sean privativas a su función;

Que, el tercer párrafo del literal c) del artículo 8 de la Ley N° 30225, Ley de Contrataciones del Estado, señala que el Titular de la Entidad podrá delegar, mediante resolución, la autoridad que dicha Ley le otorga, salvo los casos expresamente previstos en el referido literal;

Que, según el numeral 7.1 del artículo 7 del Texto Único Ordenado de la Ley Nº 28411, Ley General del Sistema Nacional de Presupuesto, aprobado mediante Decreto Supremo Nº 304-2012-EF, el Titular de una Entidad es la más alta Autoridad Ejecutiva y puede delegar sus funciones en materia presupuestal cuando lo establezca expresamente, entre otras, la citada Ley General;

Que, asimismo, el numeral 40.2 del artículo 40 del referido Texto Único Ordenado de la Ley Nº 28411, establece que las modificaciones presupuestarias en el nivel Funcional Programático son aprobadas mediante Resolución del Titular, a propuesta de la Oficina de Presupuesto o de la que haga sus veces en la Entidad, y que el Titular puede delegar dicha facultad de aprobación, a través de disposición expresa, la misma que debe ser publicada en el Diario Oficial El Peruano;

Anexo 4: Taller de sensibilización y capacitación en Seguridad de la Información.

Anexo 5: Auditoria a los requisitos de la NTP ISO/IEC 27001:2014.

Estándar	Sección	% de cumplimiento	Observaciones
4	**Contexto de la organización**	**43%**	
4.1	**Comprender la organización y su contexto**	**100%**	
4.1	La organización debe determinar los asuntos externos e internos que son importantes para su objetivo y que afecte su capacidad para lograr e(los) resultado(s) esperado(s) de su sistema de gestión de la seguridad de la información	Si	Se encuentra en el documento SGSI-IN-01-Contexto Interno y Externo.
4.2	**Comprender las necesidades y expectativas de las partes interesadas**	**0%**	
4.2	La organización debe determinar: a) las partes interesadas que son pertinentes para el sistema de gestión de la seguridad de la información; y	Si	Se encuentra en el Manual del SGSI con código SGSI-MA-01 v3.
4.2	b) los requisitos de estas partes interesadas que sean pertinentes para la seguridad de la información.	Si	Se encuentra en el Manual del SGSI con código SGSI-MA-01 v3.
4.3	**Determinar el alcance del sistema de gestión de la seguridad de la información**	**20%**	
4.3	La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance.	Si	Se encuentra en el Manual del SGSI con código SGSI-MA-01 v3 a los procesos de Gestión de Licencias, Gestión de Recepción y Despacho de Naves y Gestión de Sistemas de Información.
4.3	Al determinar este alcance, la organización debe considerar: a) los asuntos externos e internos tratados en 4.1; Al determinar este alcance, la organización debe considerar:	Si	SGSI de APN de los procesos de Gestión de Recepción y Despacho de Naves y de la Gestión de Sistemas de Información.
4.3	b) los requerimientos tratados en 4.2; y	Si	

Anexo 6: Auditoria a los controles de la NTP ISO/IEC 27001:2014.

Control	Descripción del Control	% de Cumplimiento	Observaciones
A.5	**Políticas de seguridad de la información**	**50%**	
A.5.1	**Orientación de la dirección para la seguridad de la información** **Objetivo: Proporcionar orientación y apoyo de la dirección para la seguridad de la información, de acuerdo con los requisitos del negocio y con las regulaciones y leyes pertinentes.**	**50%**	
A.5.1.1	Políticas para la seguridad de la información Control: La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de políticas para la seguridad de la información.	Si No	Se cuenta con la política del año pasado. La política integrada todavía no se revisa ni aprueba
A.5.1.2	Revisión de las políticas de seguridad de la información Control: Se deben revisar las políticas de seguridad de la información a intervalos planificados, o si se producen cambios significativos, para asegurar su conveniencia, suficiencia, y eficacia continua.	Si No	Se cuenta con la política del año pasado. La política integrada todavía no se revisa ni aprueba
A.6	**Organización de la seguridad de la información**	**50%**	
A.6.1	**Organización interna** **Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.**	**100%**	
A.6.1.1	Roles y responsabilidades de la seguridad de la información Control Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.	Si	Se evidencia el manual de Funciones y Responsabilidades con código SGSI-MA-02

Anexo 7: Indicadores del SGSI.

PERÚ Autoridad Portuaria Nacional

INDICADORES DE CONTROLES AL SGSI

Objetivos de Control y Controles	Indicador - Meta	Frecuencia	Enero	Febrero	Marzo	Abril	Mayo
A.5 Políticas de seguridad de la información							
A.5.1 Gestión de la Gerencia para la seguridad de la información							
A.5.1.1 - Políticas de la seguridad de la información	# de Actualizaciones Aprobadas a la Política >= 1	Anual	N.A	N.A	N.A	N.A	N.A
A.6 Organización de la seguridad de la información							
A.6.1 Organización interna							
A.6.1.5 - Seguridad de la información en la gestión del proyecto	% de proyectos con participación Activa de Seguridad de TI >=70%	Semestral	N.A	N.A	N.A	N.A	N.A
A.7 Seguridad de los recursos humanos							
A.7.1. Antes de reclutarlo							
A.7.1.1 - Filtración	% de personal nuevo en la APN que cuente con certificado de antecedentes policiales >= 80%	Mensual	N.A	100%	100%	S.D	S.D
A.7.1.2 - Términos y condiciones del empleo	% de personal nuevo en la APN con acuerdo confidencial firmado >= 80%	Mensual	N.A	100%	100%	S.D	S.D
A.7.2 Durante el trabajo							
A.7.2.1 - Responsabilidades de la Gerencia	% de cumplimiento del plan de comunicaciones y plan de capacitaciones >= 80%	Mensual	N.A	N.A	N.A	N.A	1
A.7.2.2 - Concientización, educación y capacitación sobre seguridad de la información	% de cumplimiento del plan de comunicaciones y plan de capacitaciones >= 80%	Mensual	100%	100%	100%	100%	100%
A.7.2.3 - Procesos disciplinarios	% de sanciones ejecutadas que hayan sido derivadas por SGSI >=80%	Mensual	N.A	S.D	S.D	S.D	S.D

GLOSARIO DE TÉRMINOS

A

Acción correctiva: Acción para eliminar la causa de una no conformidad y prevenir su repetición. Va más allá de la simple corrección.

Acción preventiva: Medida de tipo pro-activo orientada a prevenir potenciales no conformidades. Es un concepto de ISO 27001:2005. En ISO 27001:2013, ya no se emplea; ha quedado englobada en Riesgos y Oportunidades.

Aceptación del riesgo: Decisión informada de asumir un riesgo concreto.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización.

Alcance: Ámbito de la organización que queda sometido al SGSI.

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.

Análisis de riesgos: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativo: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la gravedad del impacto y la probabilidad de ocurrencia.

Análisis de riesgos cuantitativo: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y evaluarlas objetivamente para determinar el grado en el que se cumplen los criterios de auditoría.

Autenticación: Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad: Propiedad de que una entidad es lo que afirma ser.

B

BS 7799: Norma británica de seguridad de la información, publicada por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera era un conjunto de buenas prácticas para la gestión de la seguridad de la información -no certificable- y la parte segunda especificaba el sistema de gestión de seguridad de la información -certificable-. La parte primera es el origen de ISO 17799 e ISO

27002 y la parte segunda de ISO 27001. Como tal estándar, ha sido derogado ya, por la aparición de éstos últimos.

BSI: British Standards Institution, la entidad de normalización del Reino Unido, responsable en su día de la publicación de la norma BS 7799, origen de ISO 27001. Su función como entidad de normalización es comparable a la de AENOR en España.

C

CIA: CID. Acrónimo inglés de confidentiality, integrity y availability, las dimensiones básicas de la seguridad de la información.

CID: CIA. Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.

CISA: Certified Information Systems Auditor. Es una acreditación ofrecida por ISACA.

CISM: Certified Information Security Manager. Es una acreditación ofrecida por ISACA.

CISSP: Certified Information Systems Security Professional. Es una acreditación ofrecida por ISC2.

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Cliente: Persona que a cambio de un pago recibe servicios de alguien que se los presta.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. La versión de 2013 de ISO 27001 lo engloba bajo la cláusula de Liderazgo.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo

de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas relevantes. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Corrección: Acción para eliminar una no conformidad detectada. Si lo que se elimina es la causa de la no conformidad, véase acción correctiva.

D

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

Directiva o directriz: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

E

Entidad de certificación: Una empresa u organismo acreditado por una entidad de acreditación para auditar y certificar según diversas normas (ISO 27001, ISO 9001, ISO 14000, etc.) a empresas usuarias de sistemas de gestión.

Empresa: Unidad económico – social, integrada por elementos humanos, materiales y técnicos, que tiene el objetivo de obtener utilidades a través de su participación en el mercado de bienes y servicios.

Estimación de riesgos: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.

Evaluación de riesgos: Proceso global de identificación, análisis y estimación de riesgos.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión de seguridad de la información.

F

Factibilidad: Disponibilidad de los recursos necesarios para llevar a cabo los objetivos o metas señaladas.

G

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

normas BS 7799 e ISO 17799 y, por tanto, de ISO 27001 e ISO 27002.

I

Identificación de riesgos: Proceso de encontrar, reconocer y describir riesgos.

Impacto: El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p.ej., pérdida de reputación, implicaciones legales, etc.

Incidente de seguridad de la información: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Integridad: Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de entidades nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares (normas).

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. Dio lugar a ISO 27002, por cambio de nomenclatura, el 1 de Julio de 2007. Ya no está en vigor.

ISO 19011: "Guidelines for auditing management systems". Norma con directrices para la auditoría de sistemas de gestión. Guía de utilidad para el desarrollo, ejecución y mejora del programa de auditoría interna de un SGSI.

ISO/IEC 27001: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI). Primera publicación en 2005; segunda edición en 2013. Es la norma en base a la cual se certifican los SGSI a nivel mundial.

ISO/IEC 27002: Código de buenas prácticas en gestión de la seguridad de la información. Primera publicación en 2005; segunda edición en 2013. No es certificable.

M

Metodología: Grupo de mecanismos o procedimientos racionales, empleados para el logro de un objetivo, o serie de objetivos que dirige una investigación científica.

O

Objetivo: Resultado o sumatoria de una serie de metas y procesos.

P

Parte interesada: Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

PDCA: Plan-Do-Check-Act. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el

SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). La actual versión de ISO 27001 ya no lo menciona directamente, pero sus cláusulas pueden verse como alineadas con él.

Plan de continuidad del negocio: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado: La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Problema: Cuestión que se debe solucionar o aclarar, una contradicción o un conflicto entre lo que es y lo que debe ser.

Proceso: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del riesgo: Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

S

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: de Gestión de la Seguridad de la Información.

Sistema: Conjunto de partes o elementos organizados y relacionadas que interactúan entre sí para lograr un objetivo.

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza

una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

SoA: Acrónimo inglés de Statement of Applicability. Véase: Declaración de aplicabilidad.

T

Tecnología: Conjunto de técnicas, conocimientos y procesos, que sirven para el diseño y construcción de objetos para satisfacer necesidades humanas.

Tratamiento de riesgos: Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

V

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