FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

"IMPLEMENTACIÓN DE LA NTP/ISO 27001 PARA MEJORAR EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL DEPARTAMENTO TELEMÁTICA DE LA OFICINA DE ECONOMÍA DEL EJÉRCITO DEL PERÚ"

PARA OBTENER EL TÍTULO DE

INGENIERO DE SISTEMAS

AUTORES

GUSTAVO FELIPE SARMIENTO ASTUDILLO
RICHARD GEAMPIERRE GONZALES AYBAR

ASESOR

MG. JOSÉ LUIS HERRERA SALAZAR

LIMA, PERÚ, ENERO DE 2019

DEDICATORIA

Dedico la presente tesis a mis seres queridos que me apoyaron en todo momento y me dieron la fuerza para seguir adelante y no rendirme ante la adversidad. Rosendo, Rosi, Belén, Karla y equipo SIGMA.

Gustavo Felipe Sarmiento Astudillo

Dedico el presente trabajo de investigación a mis padres, amigos, compañeros de trabajo y de estudio que me dieron su apoyo incondicional en todo momento, a lo largo de mi formación profesional y personal.

Richard Geampierre Gonzales Aybar

AGRADECIMIENTOS

Agradezco a las personas que nos apoyaron para que el presente trabajo de investigación se lleve a cabo y así poder culminar nuestros estudios superiores y obtener el tan ansiado título de ingeniero de sistemas.

Gustavo Felipe Sarmiento Astudillo

Agradecimiento a la institución ejército del Perú por brindarnos la información necesaria para poder culminar nuestro estudio con éxito.

Richard Geampierre Gonzales Aybar

RESUMEN

El presente trabajo de investigación tiene como propósito determinar en qué medida la implementación de la NTP/ISO 27001 mejora el proceso de seguridad de la información en el departamento de telemática de la oficina de economía del ejército del Perú. La investigación realizada es de tipo aplicada porque busca dar solución al problema planteado, el nivel es explicativo, ya que busca establecer la relación causa y efecto de la solución sobre el problema, su diseño es Pre-Experimental. La población seleccionada para la investigación fueron todos procesos del departamento de telemática y su muestra fue el proceso de seguridad de la información, la técnica de muestreo utilizada fue probabilística aleatoria simple. Para el desarrollo de la investigación se utilizó la norma técnica peruana ISO 27001:2014. El resultado principal obtenido en la investigación fue la mejora significativa en el proceso de seguridad de la información en el departamento de telemática. Se realizaron 15 entregables estandarizados y normados para mejorar el proceso de seguridad de la información. La implementación de la NTP/ISO 27001 mejoró significativamente el proceso de seguridad de la información en el departamento de telemática de la oficina de economía del ejército.

Palabras clave: Sistema de gestión de la seguridad de la información (SGSI), seguridad de la Información (SI), norma técnica peruana (NTP), ISO 27001.

ABSTRACT

The purpose of this research work is to determine to what extent the implementation of NTP / ISO 27001 improves the process of information security in the telematics department of the office of economy of the army of Peru. The research carried out is of an applied type because it seeks to solve the problem, the level is explanatory since it seeks to establish the cause and effect relationship of the solution on the problem, its design is pre-experimental. The population selected for the research were all processes of the telematics department and its sample was the process of information security, the sampling technique used was simple random probabilistic. For the development of the research, the peruvian technical standard ISO 27001: 2014 was used. The main result obtained in the investigation was the significant improvement in the process of information security in the telematics department. 15 standardized and standardized deliverables were made to improve the process of information security. The implementation of the NTP / ISO 27001 significantly improved the information security process in the telematics department of the army economy office.

Keywords: Information security management system (ISMS), Information security (SI), peruvian technical standard (NTP), ISO 27001.

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

En el presente trabajo de investigación tiene como objetivo principal la propuesta de implementación de un sistema de gestión de seguridad de la información para mejorar el proceso de seguridad, del departamento de telemática de la oficina de economía del ejército. Para la propuesta de implementación del sistema de gestión de seguridad de la información se utilizó la norma NTP/ISO 27001:2014, este estándar nos permite tener un nivel de seguridad de la información conforme a una norma reconocida internacionalmente y alineada para la aplicación de esta a nivel nacional.

Capítulo I, planteamiento metodológico: Se detalla todo referente a la definición del problema, justificación, nivel de investigación, objetivos, hipótesis, variables e indicadores, diseño de investigación y los métodos de recolección de datos.

Capítulo II, marco referencial: Se detalla los antecedentes, teniendo como referencias tesis, libros y artículos científicos, y la parte teórica de la tesis, la validación del marco teórico relacionado con las metodologías y modelos que se están usando para el desarrollo de la tesis.

Capítulo III, implementación: Se describe la propuesta de implementación de un sistema de gestión de seguridad de la información, basado en la norma NTP/ISO 27001:2014 y definidas en el marco teórico.

Capítulo IV, análisis e interpretación de los resultados: Se realiza la prueba empírica para la recopilación, análisis e interpretación de los resultados obtenidos. En primer lugar, se describe la población y muestra, seguidamente el tipo de muestra. También se muestra el análisis de los datos Pre-Prueba y post prueba. Los datos se muestran en tablas las cuales al término de este capítulo serán analizadas y seguidamente se realizará la contratación de la hipótesis.

Capítulo V, conclusiones y recomendaciones: Se muestran las conclusiones y recomendaciones.

CAPÍTULO I

PLANTEAMIENTO METODOLÓGICO

1.1. El problema

1.1.1. Descripción de la realidad problemática

Realidad mundial

Gutzmer (2017) señala:

> El 7 de septiembre del 2017 se reportó un evento catastrófico para millones de personas del país vecino del Norte. Una de las principales entidades de crédito de los Estados Unidos (Equifax) reportó que la información de más de 143 millones de ciudadanos (incluyendo residentes del Reino Unido y Canadá) se había visto comprometida en un ataque, que según las últimas investigaciones, duró más de dos meses en ser detectada y tardó otros dos meses en ser reportada al público. Este incidente expuso información muy importante de las personas, tales como: Nombre completo, fecha de nacimiento, dirección postal y divulgación de números de seguridad social. En los Estados Unidos, el número de seguridad social es crítico para la vida de las personas, también se le conoce como social security number (SSN) y este es utilizado no solo como referencia, sino como un token para todo tipo de procesos tales como: apertura de créditos bancarios, atención médica, declaraciones de impuestos, sentencias criminales. (p. 2)**.**

Realidad nacional

Los sistemas de información de las organizaciones se enfrentan día a día con riesgos e inseguridades que se enfocan en explotar vulnerabilidades de sus activos de información poniendo en riesgo la continuidad del negocio.

Huamán (2014) señala:

> Un estudio realizado por Huamán en el 2014 da a conocer que en mayo del 2012 se publicó en el diario el peruano la aprobación del uso obligatorio de la NTPISO/IEC 27001:2008 en las entidades del estado, esto nos demuestra la intención del gobierno peruano en establecer un modelo integral para el desarrollo de los planes de seguridad de la información en la administración pública. (p. 6).

Realidad empresarial

Las instituciones públicas a pesar que tuvieron la exigencia por parte del estado peruano en aplicar la NTP/ISO 27001:2008 con la finalidad de salvaguardar la información ante cualquier riesgo o amenaza; sin embargo las entidades siempre

están vulnerables ante la pérdida y fuga de información relevante, debido a que los cyber delincuentes encuentran nuevas formas y maneras de apropiarse de nuestra información, es por ello que las medidas de seguridad de las entidades deben estar en constante actualización. Por lo general las empresas hacen un estudio de sus riesgos y amenazas una sola vez en la vida y no las vuelven analizar, este factor se puede deber a dos causas, la falta de conocimiento o interés ya que es un proceso bastante pesado y delicado de realizar. Es por ello que las empresas deben tomar conciencia de lo importante que son las actualizaciones en los procesos de seguridad.

Ubicación

El presente trabajo de investigación se desarrolla en el departamento de telemática de la oficina de economía del ejército del Perú (OEE), que se encuentra ubicado en la Av. Paseo del bosque N° 740 - San Borja - Lima - Perú.

Figura 1. Mapa de ubicación de la oficina de economía del ejército del Perú. Fuente: Google maps (2018).

1.1.2. Definición del problema

Actualmente la información que se transmite, procesa y almacena en los sistemas de información se encuentra en todas las instituciones de diferentes rubros; los sistemas de información han alcanzado un nivel de complejidad alto debido a que la distancia ya no es un impedimento, de esta manera a aumentado el porcentaje de personas que tienen acceso a la información de las instituciones.

La institución no cuenta con políticas de seguridad actualizada, manuales de procedimientos estructurados y completamente probados, normas de control de acceso, acta de confidencialidad, cámaras de seguridad y acceso biométrico.

La información esta almacenada y a la vez es procesada en computadoras que no brindan las condiciones de seguridad para resguardar la integridad y confiabilidad de esta, debido a que no hay un estricto control y monitoreo. Es por ello que la información pueda ser mal utilizada o modificada, también puede estar vulnerable a fraude, sabotaje y robo.

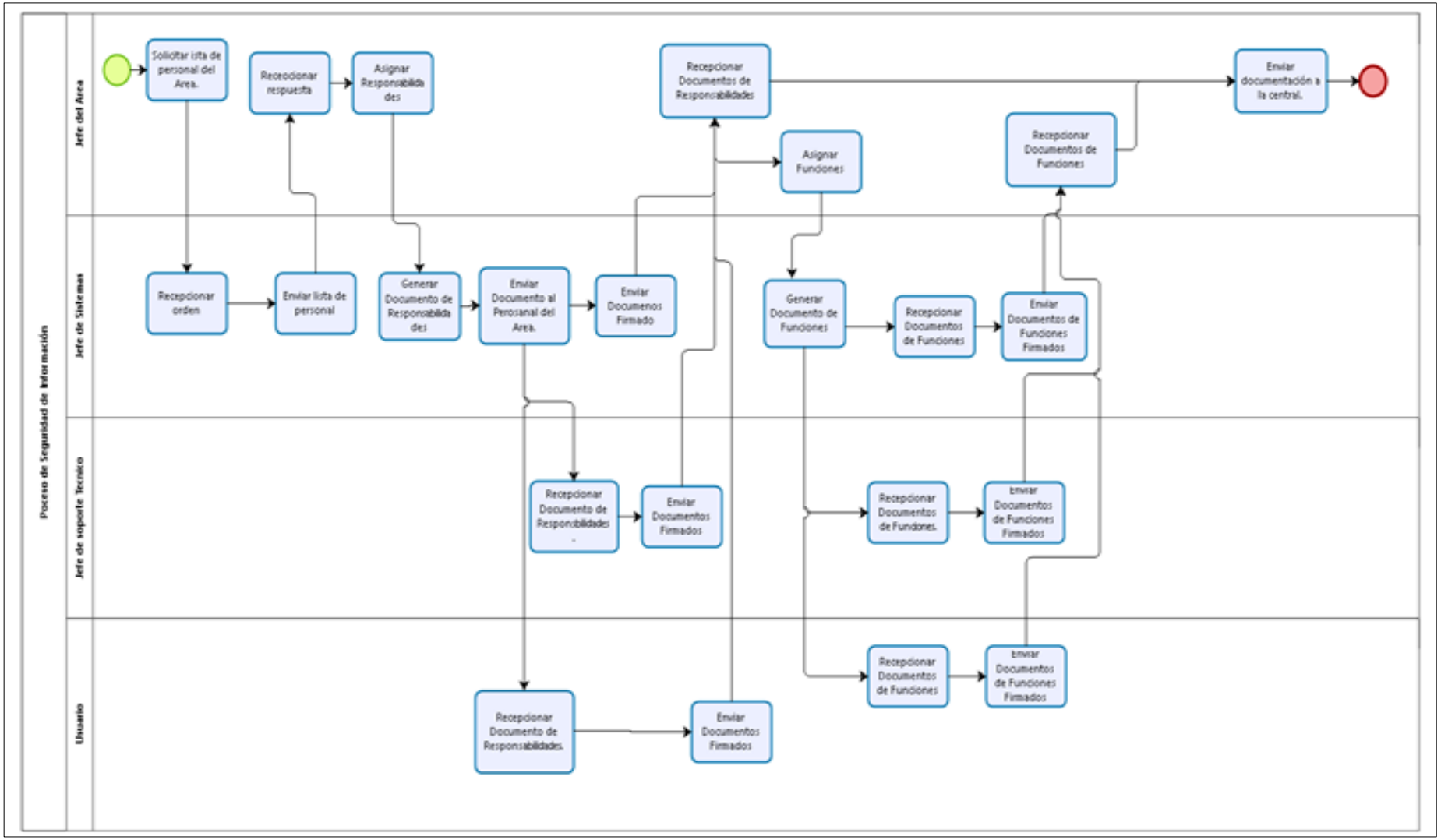


Figura 2. Flujograma del proceso de seguridad de la información del ejército del Perú (AS-IS).

El proceso de seguridad mostrado anteriormente en la figura 2 describe los problemas de:

- ✓ Bajo promedio de reportes sobre las incidencias referidas a la seguridad de la información.
- ✓ Falta de controles para el acceso a la información.
- ✓ Falta de documentación de compromiso de confiabilidad.
- ✓ No existe roles establecidos para la solución de incidencias.
- ✓ Insatisfacción del usuario sobre ciertos procedimientos al realizarse el proceso de seguridad de la información.

Tabla 1

As – Is y To – Be

AS – IS	TO BE
Reportar incidencias de seguridad de la información.	Disminuir el tiempo para reportar incidencias de seguridad de la información.
Porcentaje de disponibilidad de la Información.	Aumentar el porcentaje de disponibilidad de la información dentro de la empresa.
Porcentaje de confiabilidad de la información	Aumentar el porcentaje de confiabilidad de la información dentro de la empresa.
Solucionar incidencias de seguridad de la información.	Disminuir el tiempo de respuesta a una incidencia de seguridad de la información.
Insatisfacción del usuario.	Aumentar el nivel de satisfacción del usuario.

Tabla 2

Datos actuales de los indicadores

Indicador	Datos de Pre-Prueba (promedio)
Tiempo para reportar incidencia de seguridad de la información.	37 min
Porcentaje de disponibilidad de la Información.	47%
Porcentaje de confiabilidad de la información	24 %
Tiempo para dar respuesta a una incidencia de seguridad de la información.	25 min
Nivel de satisfacción del usuario	Regular

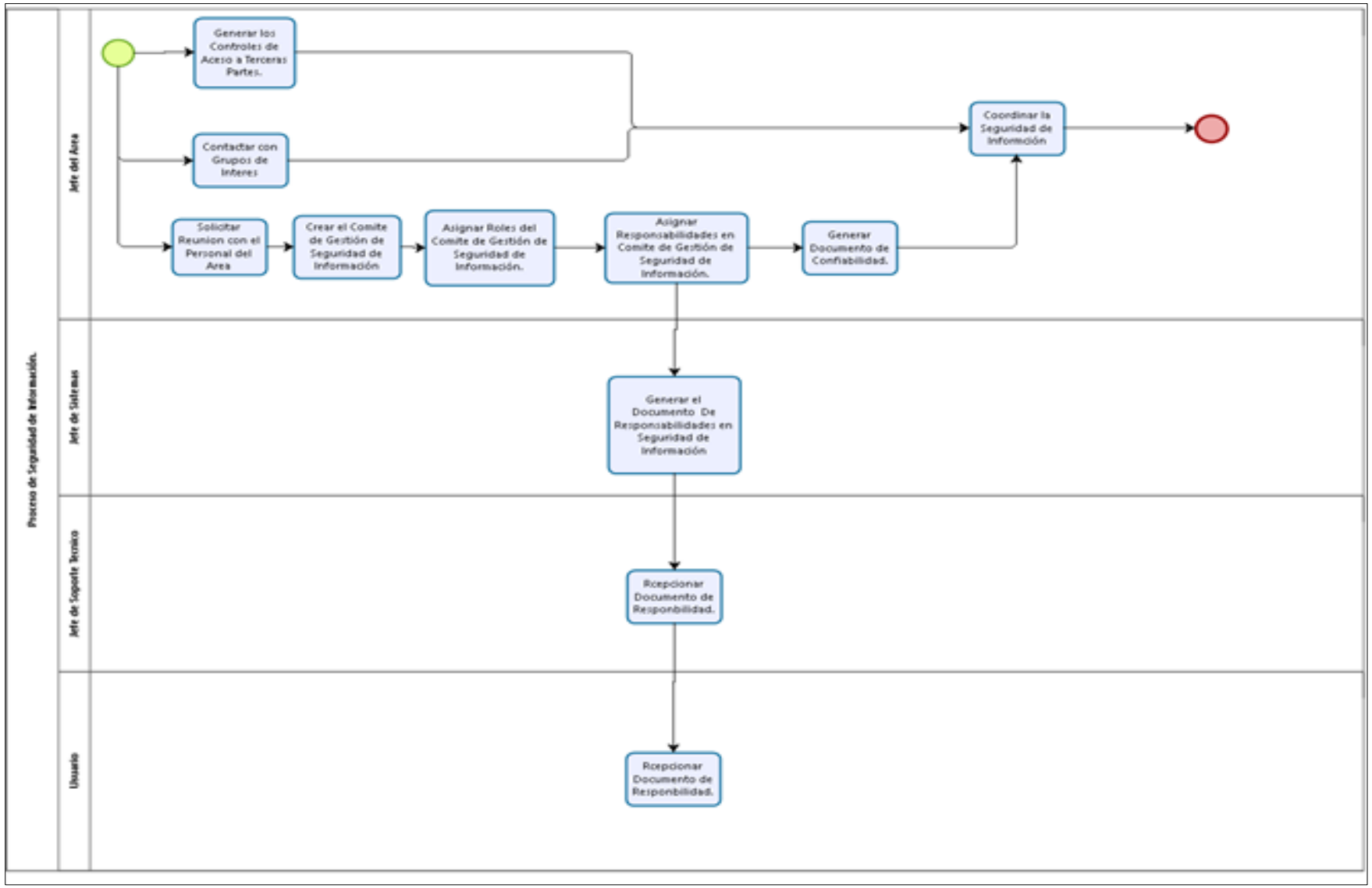


Figura 3. Proceso de seguridad de la información de la oficina de economía.

1.1.3. Enunciado del problema

¿En qué medida la implementación de la norma técnica peruana/ISO 27001 mejorará el proceso de seguridad de información en el departamento de telemática de la oficina de economía del ejército del Perú?

1.2. Tipo y nivel de la investigación

1.2.1. Tipo de investigación

Aplicada: Para dar solución al problema planteado en el proceso de seguridad de información, qué apoyado con la norma técnica peruana/ISO 27001 sean útiles y eficaces para la mejora de este proceso.

1.2.2. Nivel de investigación

Nivel explicativo:

Relación causa efecto de la solución sobre el problema.

1.3. Justificación de la investigación

1.3.1. Teórica

Guzmán (2016) señala:

> En su investigación publicada en el año 2016 nos dice que el diseño de un sistema de gestión de seguridad de la Información basado en un modelo de buenas prácticas de seguridad conocido a nivel mundial como la norma ISO/IEC 27001:2013, nos proveerá las condiciones de gobernabilidad, oportunidad y viabilidad necesaria, para que la seguridad de la información se apoye y extienda a los objetivos estratégicos del negocio, mediante la protección y aseguramiento de la información. Debido a que la información es fundamental para garantizar la correcta gestión financiera, administrativa y operativa. Con ello la entidad asegura el cumplimiento de su misión. (p. 15).

1.3.2. Social

Villegas y Gaviria (2013) afirman:

> Para establecer el SGSI, este se define en términos del negocio, la organización, la localización, activos y tecnologías. También hay que tener en cuenta que las políticas de

> seguridad deben estar relacionadas con los objetivos de seguridad de la información y que se debe definir la metodología adecuada para el análisis de riesgos de la información. (p. 7).

1.3.3. Metodológica

Aguirre y Aristizábal (2013) enfatizan:

> Un sistema de gestión de seguridad de la información contribuye a estar a la altura de las grandes organizaciones que buscan en las certificaciones de seguridad de la información, una de las mayores ventajas competitivas para lanzarse al mercado ya explorado o a los mercados que aún se encuentran disponibles, los cuales por el crecimiento global se han tornado exigentes, por lo que es indispensable realizar transacciones electrónicas y acogerse a ellas mediante distintos canales de pago para la sostenibilidad y manejo de los clientes a nivel nacional e internacional. (p. 10).

1.3.4. Institucional

Actualmente las empresas carecen de un proceso de seguridad eficiente con respecto a los estándares establecidos por la norma técnica peruana (NTP) ISO 27001. Es por ello que las instituciones tienen que anticiparse y no deben permitir que se produzcan incidentes de seguridad contra su información por no tener los controles suficientes para salvaguardarla. Por lo tanto, una correcta aplicación de los estándares de seguridad de la información, ayudan a mitigar el riesgo de sufrir algún atentado contra los activos más importantes de la organización.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Determinar en qué medida la implementación de la norma técnica peruana/ISO 27001 mejora el proceso de seguridad de información en el departamento de telemática de la oficina de economía del ejército del Perú.

1.4.2. Objetivos específicos

- ✓ Determinar en qué medida se reduce el tiempo para reportar incidencias de seguridad de la información.
- ✓ Determinar en qué medida se incrementa la disponibilidad de la información dentro de la institución.
- ✓ Determinar en qué medida aumenta el porcentaje de confidencialidad de la información dentro de la institución.
- ✓ Determinar en qué medida se reduce el tiempo para dar respuesta a una incidencia de seguridad de la información.

1.5. Hipótesis

Si se implementa la NTP/ISO 27001 entonces mejora significativamente el proceso de seguridad de la información en el departamento de telemática de la oficina de economía del ejército del Perú.

1.6. Variables e indicadores

1.6.1. Variable independiente

a) Norma técnica peruana ISO 27001

Tabla 3

Conceptualización de indicador de presencia y ausencia

Indicador: Presencia – Ausencia
Descripción: Cuando indique “No”, es porque no se ha implementado la NTP/ISO 27001 en el departamento de telemática de la oficina de economía del ejército del Perú y aún se encuentra en la situación actual del problema. Cuando indique “Si”, es cuando ya se implementó la NTP/ISO 27001 en el departamento de telemática de la oficina de economía del ejército del Perú, esperando obtener mejores resultados.

Tabla 4

Operacionalización del indicador de la variable independiente

Indicador	**Índice**
Presencia – Ausencia	Sí, No

1.6.2. Variable dependiente

b) Proceso de seguridad de la información

Tabla 5

Conceptualización de indicadores de la variable dependiente

Indicadores	Descripción
Tiempo para reportar una incidencia de seguridad de la información.	Es el tiempo promedio que toma para reportar incidencias que afectan la continuidad de la institución.
Porcentaje de disponibilidad de la información dentro de la institución.	Es el porcentaje de disponibilidad de la información que se maneja dentro de la institución.
Porcentaje de confidencialidad de la información dentro de la institución.	Es el porcentaje de confidencialidad de la información que se maneja dentro de la institución.
Tiempo para dar respuesta a una incidencia de seguridad de la información.	Es el tiempo promedio que toma para solucionar una incidencia de seguridad de la información que afecta a la continuidad de la institución.
Nivel de satisfacción del usuario.	Es el nivel cualitativo de satisfacción que puede tener un usuario con respecto al desarrollo del proceso.

Tabla 6

Operacionalización de indicadores de variable dependiente

Indicadores	Índice	Unidad de Medida	Unidad de Observación
Tiempo para reportar una incidencia de seguridad de la información.	[10 - 37]	Minutos	Jefa de área
Porcentaje de disponibilidad de la información dentro de la institución.	[47-89]	%(Porcentaje)	Jefa de área
Porcentaje de confidencialidad de la información dentro de la institución.	[24-68]	%(Porcentaje)	Jefa de área
Tiempo para dar respuesta a una incidencia de seguridad de la información.	[8- 25]	Minutos	Jefa de área
Nivel de satisfacción del usuario.	[Excelente, bueno, regular, malo]	Nivel de satisfacción	Usuario encuesta

1.7. Limitaciones de la investigación

La presente investigación se desarrollará durante los meses de agosto a diciembre del año 2018, se llevará a cabo en el departamento de telemática de la oficina de economía del ejército del Perú y tiene como delimitación conceptual la norma técnica peruana (NTP/ISO27001:2014) para mejorar la seguridad de la información en el departamento de telemática de la oficina de economía del ejército del Perú.

1.8. Diseño de la investigación

Diseño experimental de pre prueba y post prueba con un solo grupo.

Tabla 7

Diseño de la investigación

G_e	O_1	X	O_2
Primero, se asigna a los participantes al azar al Grupo experimental.	Pre-Prueba o medición previa al estímulo o tratamiento experimental.	Administrar el estímulo o tratamiento experimental.	Post-Prueba o medición posterior al estímulo o tratamiento experimental.

El diseño se diagrama de la siguiente manera:

$$G_e \quad 0_1 \quad X \quad 0_2$$

Dónde:

- **Ge:** Grupo experimental, conformado por procesos de seguridad del departamento de telemática del ejército del Perú.
- **O_1:** Son los valores de los indicadores de la variable dependiente en la Pre-Prueba.
- **X:** Tratamiento, estímulo o condición experimental. (NTP/ISO 27001).
- **O_2:** Son los valores de los indicadores de la variable dependiente en la Post-Prueba (Después de implementar la solución).

1.9. Técnicas e instrumentos para la recolección de información

Tabla 8

Técnicas e instrumentos de la investigación experimental

Técnicas	Instrumentos
Seguimiento del tiempo de generación de documento de confiabilidad. Seguimiento de la exactitud de la información que se muestra a los usuarios. Seguimiento de la satisfacción del cliente.	Ficha de observación. Reportes generados.

Tabla 9

Técnicas e instrumentos de investigación de campo

Técnicas	Instrumentos
Observación directa (estructurada)	Fichas de observación. Registro manual en Excel.
Entrevista estructurada.	Formato de entrevistas.
Aplicación de cuestionario (cerrado)	Cuestionario, anexo 12 “Encuesta al usuario”

CAPÍTULO II

MARCO REFERENCIAL

2.1. Antecedentes de la investigación

a) Autor: Fernández Peñaloza, David Aurelio
Pacheco Vargas, Oscar Alexis

Título: Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/ISO 27001:2008.
Año: 2015
Tipo: Tesis de pregrado

Correlación: Desarrollaron el análisis y diseño de un plan de sistema de gestión de seguridad de la Información, basado en las mejores prácticas de la NTP-ISO/IEC 27001:2008 para gestionar los procesos de seguridad de la empresa y lograr una gestión de operaciones más rápida, como puntos clave a tomar serán desde la recolección de datos y/o levantamiento de la información, análisis de riesgos, evaluación selectiva hasta el diseño del plan de gestión de la seguridad de la información.

b) Autor: Hans Ryan Espinoza Aguinaga

Título: Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo.
Año: 2013
Tipo: Tesis de pregrado

Correlación: Realizó la implementación del SGSI, basado en la norma ISO/IEC 27001:2005 que está dirigida a procesos, activos, riesgos y demás consideraciones de una empresa del rubro de producción y comercialización de productos de consumo masivo.

Espinoza (2013) señala:

> Cubre todos aquellos aspectos que se deben de tener en cuenta en relación a estándares, procedimientos, normas y medidas que empleen tecnología que permiten asegurar las principales características que debe tener la información; las cuales son: Integridad, disponibilidad y confidencialidad. (p. 9).

c) Autor: David Arturo Aguirre Mollehuanca

Título: Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.
Año: 2014
Tipo: Tesis de pregrado

Correlación: Desarrolló el proyecto que busca el diseño e implementación de un sistema de gestión de seguridad de información para resguardar la confidencialidad, disponibilidad e integridad de los activos de información involucrados en los procesos institucionales críticos.

"Posteriormente se realizó una serie de entrevistas que permitieron identificar y valorar los activos críticos de la empresa, también se identificaron y evaluaron los riesgos que afectaba a la continuidad del negocio" (Aguirre, 2014, p. 10).

d) Autor: Henry Iván Condori Alejo

Título: Un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información para determinar su influencia en la intención del usuario.
Año: 2012
Tipo: Tesis de maestría

Correlación: Desarrollaron un modelo que servirá como referencia para la evaluación de los factores críticos de éxito para garantizar la implementación de la seguridad de información en las organizaciones, con lo particular que su enfoque principal es la actitud del usuario.

Tal es así, que para lograr un nivel adecuado de protección de información en las organizaciones se tiene que identificar sus principales amenazas pues es la necesidad principal y más urgente. Cuando el valor de los sistemas de información y la información son vitales para la organización, esto hace que la necesidad de protección sea más exigente.

e) Autor: Paula Andrea Maya Arango

Título: Plan de implementación del SGSI basado en la norma ISO 27001:2013.
Año: 2014
Tipo: Tesis de maestría

Correlación: Desarrolló la creación del modelo de seguridad de la información para la organización "Textil S.A", basado en la norma ISO 27001:2013; iniciando desde el entendimiento de la organización, la óptica de los procesos críticos, la ejecución del diagnóstico de seguridad de la información, la identificación de las principales vulnerabilidades y amenazas, aplicando la metodología de gestión de riesgos para la seguridad de la información, para el tratamiento de riesgos y generación del marco documental del sistema de gestión de seguridad de la información.

El principal objetivo es sentar las bases del proceso de mejora continua y plantear las acciones necesarias para minimizar el impacto de los riesgos potenciales.

Maya (2016) señala:

> El proyecto plantea el establecimiento de las bases para la implementación de un SGSI. Para ello se abordarán las siguientes fases:
> - ✓ Documentación normativa sobre las mejores prácticas en seguridad de la información.
> - ✓ Definición clara de la situación actual y de los objetivos del SGSI.
> - ✓ Análisis de riesgos o Identificación y valoración de los activos corporativos como un punto de partida para el análisis de riesgos.

- ✓ Identificación y valoración de los activos corporativos como punto de partida a un análisis de riesgos.
- ✓ Identificación de amenazas, evaluación y clasificación de las mismas.
- ✓ Evaluación del nivel de cumplimiento de la ISO/IEC 27002:2013 en la organización.
- ✓ Propuestas de proyectos de cara a conseguir una adecuada gestión de la seguridad.
- ✓ Esquema documental del sistema de gestión de seguridad de la información. (p. 5).

f) Autor: Hugo Daniel Olaza Aliano

Título: Implementación de la NTP ISO/IEC 27001 para la seguridad de la información en el área de configuración y activos del ministerio de educación – sede Centromin.
Año: 2017
Tipo: Tesis de pregrado

Correlación: Realizó la implementación de la NTP ISO/IEC 27001 para la seguridad de la información en el área de configuración y activos del ministerio de educación - Sede Centromin.

Olaza (2017) señalan:

> Los resultados de esta investigación confirman que la implementación de la norma técnica peruana ISO/IEC 27001 tuvo un efecto positivo para la seguridad de la información. En cuanto al número de información confidencial divulgada antes se registraban 182 casos, después de la implementación se registró 50 casos, para el número o porcentaje de accesos y/o cambios no autorizados a los datos de producción antes se registraba 322 casos, después de la implementación disminuyó a 47 casos, para el porcentaje de tiempo durante el cual un sistema está disponible para el usuario se registró un porcentaje de 70.36%, después de la implementación aumentó a 98.22% respectivamente. (p. 8).

g) Autor: Edward Jean Carlos Llanos Paredes

Título: Modelo de procesos para la implementación de la norma ISO 27001 en la concesionaria terrapuerto, Trujillo.
Año: 2017
Tipo: Tesis de pregrado

Correlación: Desarrolló un modelo de procesos para la implementación de la norma ISO 27001 en la concesionaria terrapuerto Trujillo, al verse comprometida de forma indirecta con la normativa publicada en el año 2016, donde se indica que se tiene que resguardar y administrar de forma correcta la información de la empresa bajo la normativa ISO 27001. Para ello se aplica las etapas basadas en el framework Spark, las cuales serán tomadas para la creación de dicho modelo de procesos para la empresa concesionaria terrapuerto Trujillo S.A.

Demostrando que las etapas que presenta este framework y la realización del modelo de procesos para la implementación se dará en un mayor porcentaje de noventa por ciento de los requerimientos, políticas y controles que exige la norma técnica peruana para que se cumpla en la empresa con respecto al sistema de gestión de seguridad de la información.

h) Autor: Mercedes Ccesa Quincho

Título: Diseño de un sistema de gestión de seguridad de la información bajo la NTP/IEC 27001:2014 para la municipalidad provincial de Huamanga.
Año: 2017
Tipo: Tesis de pregrado

Correlación: Desarrolló su investigación en tres fases: En la primera fase se realizó el diagnóstico inicial de la entidad con respecto a la NTP ISO/IEC 27001:2014 y su posibilidad de aceptación. En la segunda fase se estudió a la organización y su contexto; se identificó el proceso crítico; se definió la política de seguridad, el alcance y se identificó al comité de seguridad de la información de la organización. En la tercera fase, siguiendo la metodología de análisis y gestión de riesgos adoptada, se identificó y valoró los activos de información, se identificó las amenazas, se realizó el cálculo del impacto del riesgo y se identificaron las medidas de control necesarias para mitigar los riesgos a un nivel aceptable.

i) Autor: Vasco Rodrigo Talavera Álvarez

Título: Diseño de un sistema de gestión de seguridad de la información para una entidad estatal de salud de acuerdo con la ISO/IEC 27001:2013.
Año: 2015
Tipo: Tesis de pregrado

Correlación: Desarrolló el análisis y diseño de un sistema de gestión de seguridad de la información para una entidad pública del sector salud. En la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de instituciones de diferentes rubros y funciones.

Talavera (2015) enfatiza:

> Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no sean un obstáculo. En respuesta a este nuevo escenario, las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un sistema de gestión de seguridad de la información a través de diferentes normas, entre ellas la NTP ISO/IEC 27001, que tiene como finalidad asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna. (p. 10).

j) Autor: Enrique Efraín Maldonado Estrada

Título: Norma ISO 27001 para la seguridad de información del área de registros académicos del colegio “Nuestra Señora del Carmen”
Año. 2016
Tipo: Tesis de pregrado

Correlación: Investigó sobre el efecto de la aplicación de la norma ISO 27001 para la seguridad de información del área de registros académicos del colegio “Nuestra Señora del Carmen”.

Maldonado (2016) sostiene:

> Los resultados de esta investigación confirman que la aplicación de la norma ISO 27001 tuvo un efecto positivo para los registros académicos del colegio Nuestra Señora del Carmen, en cuanto a los cambios autorizados se redujo al 80.8% de la etapa de pre prueba con respecto a la post prueba y con respecto a los riesgos fueron mitigados hasta en un 19%. (p. 6).

k) Autor: Julio Cesar Alcantára Flores

Título: Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte PNP en la ciudad de Chiclayo
Año. 2015
Tipo: Tesis de pregrado

Correlación: En su investigación se enfoca en la elaboración de una guía de implementación de la seguridad basada en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas de información en la institución policial (Comisaria del norte – Chiclayo).

Alcantára (2015) señala:

> Los resultados obtenidos permitieron determinar de forma real que al incorporar la norma ISO/IEC 27001 basada en una guía de implementación se logró incrementar los procedimientos utilizados en favor de la institución, permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla. (p. 6).

l) Autor: Paul Omar Cueva Araujo
Juan Antonio Ríos Mercado

Título: Gestión de la historia clínica y la seguridad de la información del hospital II Cajamarca – Essalud bajo la NTP-ISO/IEC 27001:2014

Año: 2018
Tipo: Tesis de maestría

Correlación: De la investigación con respecto a los servicios de salud dicen que el activo principal del centro de salud es la información de la historia clínica que al ser un documento médico legal y que tiene que ver con los procesos de atención de los pacientes y el seguro social de salud cuenta con una norma a nivel nacional para el cumplimiento de la gestión de la historia clínica.

"El resultado encontrado se observa que en el hospital II Cajamarca existe un cumplimiento del 60% de las buenas prácticas y recomendaciones sobre la norma de gestión de las historias clínicas de los pacientes en los centros de salud" (Cueva y Ríos, 2018, p. 2).

m) Autor: Fressia Lisset Ariasca Suma
Sheny Katerine Quispe Borda

Título: Desarrollo de una propuesta de implementación de la NTP-ISO/IEC 27001:2014, sistema de gestión de seguridad de la información, para la oficina funcional de informática del gobierno regional del Cusco
Año: 2016
Tipo: Tesis de pregrado

Correlación: Elaboraron una propuesta de implementación, los requisitos se especifican del capítulo 4 al 10 de la NTP-ISO/IEC 27001:2014 que exigen para la conformidad de un sistema de gestión de seguridad de la Información.

Ariasca y Quispe (2016) señalan:

> Inicialmente se realiza un diagnóstico de la situación actual de la oficina funcional de informática en relación con el cumplimiento de los requisitos de la norma, logrando así identificar las debilidades y falencias en temas de seguridad de la información relacionados al cumplimiento de la norma. (p. 4).

n) Autor: Javier Alfonso Seclén Arana

Título: Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo con la NTP-ISO/IEC 27001
Año: 2016
Tipo: Tesis de maestría

Correlación: En su investigación de tipo cualitativa da a conocer que utilizar una estrategia de recopilación de información de una manera organizada y estructurada, ayudan en la identificación de las restricciones que hay para la implementación de un sistema de gestión de seguridad de la información. Es por ello que realizar un correcto levantamiento de las necesidades y requerimientos de la empresa, ayudará a tener el éxito en la implementación de las políticas de seguridad de la información en las entidades que integran el sistema nacional de informática.

o) Autor: Daniel Elías Santos Llanos

Título: Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software
Año: 2016
Tipo: Tesis de pregrado

Correlación: La solución planteada para este problema es un sistema de gestión de seguridad de información (SGSI), el cual cuenta con el estándar ISO 27001:2013 como marco formal de requisitos a cumplir.

2.2. Marco teórico

A. Sistema de gestión de seguridad de la información

El sistema de Gestión de Seguridad de la Información o también llamado SGSI o en inglés ISMS, siglas equivalentes a information security management

system, es el principal concepto de lo que está conformada la ISO 27001, esta se debe realizar mediante un proceso sistémico, documentado y conocido por toda la empresa. Según ISO 27001, el SGSI, consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la organización.

Fundamentos: Para garantizar que el sistema de gestión de seguridad de la información gestionado de forma correcta se tiene que identificar el ciclo de vida y los aspectos relevantes adoptados para garantizar su:

- ✓ **Confidencialidad:** La información no se pone a disposición de nadie, ni se revela a individuos o entidades no autorizados.
- ✓ **Integridad:** Mantener de forma completa y exacta la información y los métodos de proceso.
- ✓ **Disponibilidad:** Acceder y utilizar la información y los sistemas de tratamiento de la misma parte de los individuos, entidades o proceso autorizados cuando lo requieran.

Según el conocimiento que se tiene del ciclo de vida de la información relevante se puede adoptar la utilización de un proceso sistemático, documentado y conocido por toda la empresa, desde un enfoque de riesgos empresarial. El proceso es el que constituye un SGSI. (ISO 27000.es, s.f.-a)

ISO 27000.es (s.f.-b) señala:

> **¿Para qué sirve un SGSI?**
>
> La información, junto a los procesos y los sistemas que hacen uso de ella, son activos demasiado importantes para la empresa. La confidencialidad, integridad y disponibilidad de dicha información puede ser esencial para mantener los niveles de competitividad, conformidad, rentabilidad e imagen de la empresa necesarios para conseguir los objetivos de la empresa y asegurase de que haya beneficios económicos.
>
> Las organizaciones y los sistemas de información se encuentran expuestos a un número cada vez más elevado de amenazas que aprovechan cualquier tipo de vulnerabilidad para

someter a los activos críticos de información a ataques, espionajes, vandalismo, etc. Los virus informáticos o los ataques son ejemplos muy comunes y conocidos, pero también se deben asumir los riesgos de sufrir incidentes de seguridad que pueden ser causados voluntariamente o involuntariamente desde dentro de la propia empresa o los que son provocados de forma accidental por catástrofes naturales.

El cumplimiento de la legalidad, la adaptación dinámica y de forma puntual de todas las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar que se obtiene el máximo beneficio son algunos de los aspectos fundamentales en los que un **SGSI** es una herramienta de gran utilidad y de importante ayuda para la gestión de las empresas.

El nivel de seguridad que se alcanza gracias a los medios técnicos es limitado e insuficiente por sí mismo. Durante la gestión efectiva de la seguridad debe tomar parte activa toda la empresa, con la gerencia al frente, tomando en consideración a los clientes y a los proveedores de la organización.

El modelo de gestión de la seguridad tiene que contemplar unos procedimientos adecuados y planificar e implementar controles de seguridad que se basan en una evaluación de riesgos y en una medición de la eficiencia de los mismos. (p. 13-16).

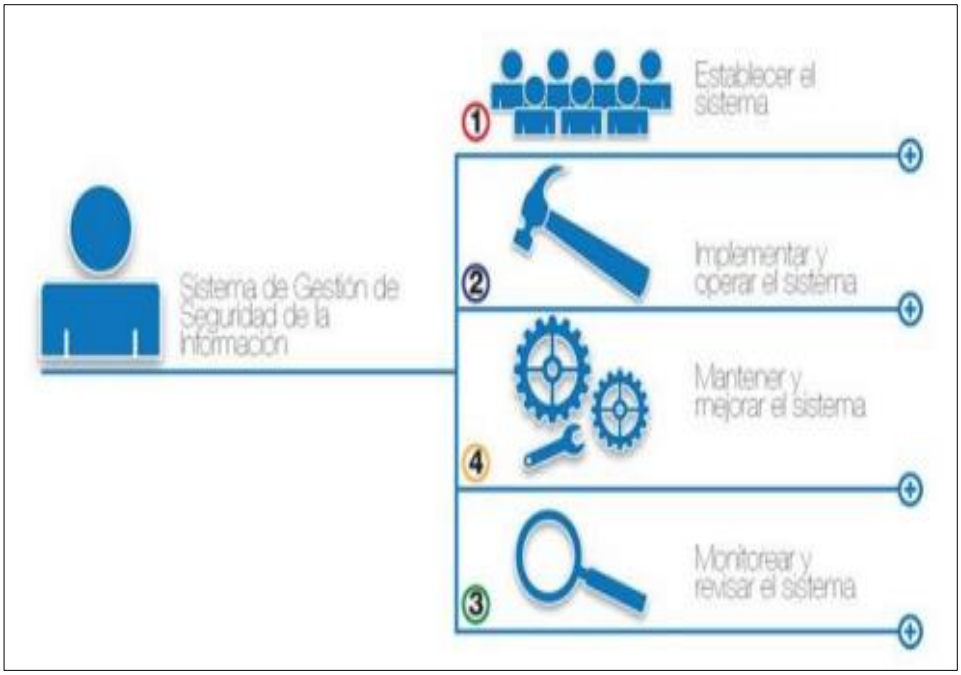


Figura 4. Actividades de la ISO 27001. Fuente: Picón (2016).

¿Qué es lo que Incluye el SGSI?

Figura 5. Pirámide SGSI. Fuente: www.iso27000.es (2016).

ISO 27000.es (s.f.-b) señala:

Documentos de nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería 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.

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.

Documentos de nivel 3

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

Documentos 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.

De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

- ✓ **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 (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- ✓ **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.
- ✓ **Procedimientos y mecanismos de control que soportan al SGSI:** aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- ✓ **Enfoque de evaluación de riesgos:** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- ✓ **Informe de evaluación de riesgos:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- ✓ **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, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- ✓ **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.
- ✓ **Registros:** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- ✓ **Declaración de aplicabilidad:** (SOA-Statement of applicability-, en sus siglas inglesas); 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.

Control de la documentación

Para los documentos generados se debe establecer, documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- ✓ **Aprobar documentos** apropiados antes de su emisión.
- ✓ **Revisar y actualizar documentos** cuando sea necesario y renovar su validez.
- ✓ Garantizar que los **cambios y el estado actual de revisión** de los documentos están identificados.
- ✓ Garantizar que las versiones relevantes de **documentos vigentes están disponibles** en los lugares de empleo.
- ✓ Garantizar que los documentos se mantienen **legibles y fácilmente identificables**.
- ✓ Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son **transmitidos, almacenados y finalmente destruidos acorde con los procedimientos** aplicables según su clasificación.
- ✓ Garantizar que los **documentos procedentes del exterior** están identificados.

- ✓ Garantizar que la **distribución de documentos** está controlada.
- ✓ Prevenir la utilización de **documentos obsoletos**.
- ✓ Aplicar la identificación apropiada a **documentos que son retenidos** con algún propósito.

Implementar un SGSI:

Segùn la ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad:

- ✓ **Plan (planificar):** establecer el SGSI.
- ✓ **Do (hacer):** implementar y utilizar el SGSI.
- ✓ **Check (verificar):** monitorizar y revisar el SGSI.
- ✓ **Act (actuar):** mantener y mejorar el SGSI.

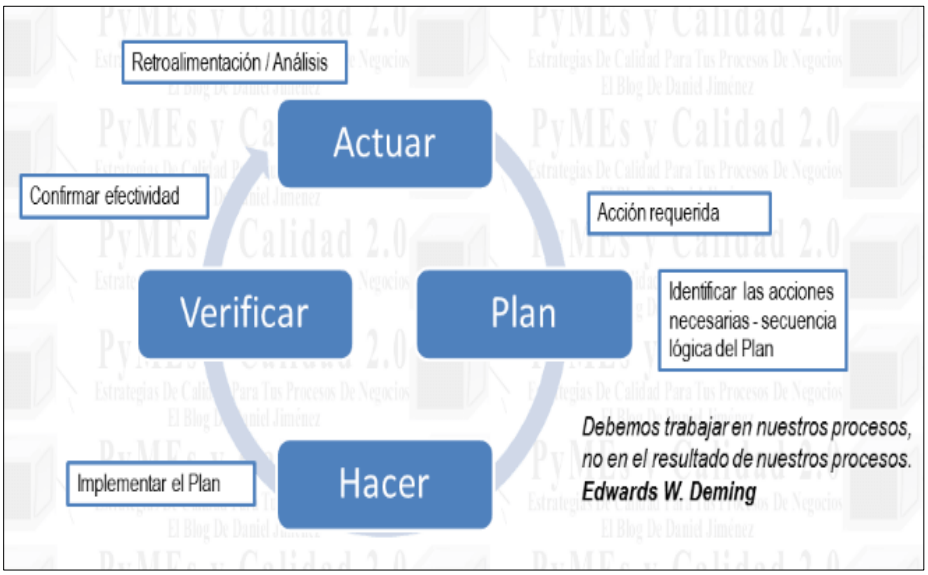


Figura 6. Ciclo PDCA. Fuente: Jiménez (2013).

Plan: Establecer el SGSI

- Definir el **alcance** del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una **política de seguridad** que:

  – incluya el marco general y los objetivos de seguridad de la información de la organización;

  – considere requerimientos legales o contractuales relativos a la seguridad de la información;

  – esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;

  – establezca los criterios con los que se va a evaluar el riesgo;

  – esté aprobada por la dirección.

- Definir una **metodología de evaluación del riesgo** apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- **Identificar los riesgos:**

  – identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

  – identificar las amenazas en relación a los activos;

  – identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;

  – identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- **Analizar y evaluar los riesgos:**

  – evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;

  – evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación con las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;

  – estimar los niveles de riesgo;

  – determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de **tratamiento de los riesgos** para:

  – aplicar controles adecuados;

  – aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;

  – evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;

  – transferir el riesgo a terceros, p. ej., compañías aseguradoras o proveedores de outsourcing.
- Seleccionar los **objetivos de control** y los **controles** del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los **riesgos residuales** como la **implantación y uso del SGSI**.
- Definir una **declaración de aplicabilidad** que incluya: – los objetivos de control y controles seleccionados y los motivos para su elección; – los objetivos de control y controles que actualmente ya están implantados; – los objetivos de control y controles del anexo a excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias. En relación con los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en

11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de “documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades particulares.

Do: Implementar y utilizar el SGSI

- **Definir un plan de tratamiento de riesgos** que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- **Implantar el plan de tratamiento de riesgos**, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- **Implementar los controles** anteriormente seleccionados que lleven a los objetivos de control.
- Definir **un sistema de métricas** que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de **formación y concienciación** en relación con la seguridad de la información a todo el personal.
- **Gestionar las operaciones del SGSI**.
- **Gestionar los recursos** necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida **detección y respuesta a los incidentes de seguridad**.

Check: monitorizar y revisar el SGSI

- Ejecutar procedimientos de **monitorización y revisión** para:

  – detectar a tiempo los errores en los resultados generados por el procesamiento de la información;

  – identificar brechas e incidentes de seguridad;

  – ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación con lo previsto;

  – detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;

  – determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la **efectividad del SGSI**, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

- Medir la **efectividad de los controles** para verificar que se cumple con los requisitos de seguridad.
- Revisar regularmente en intervalos planificados **las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables**, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Realizar periódicamente **auditorías internas** del SGSI en intervalos planificados.
- **Revisar el SGSI por parte de la dirección** periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- **Actualizar los planes de seguridad** en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- **Registrar acciones y eventos** que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act: Mantener y mejorar el SGSI

- Implantar en el SGSI las **mejoras identificadas**.
- Realizar las acciones preventivas y correctivas adecuadas a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- Asegurarse que las mejoras introducidas alcanzan los objetivos previstos. (p. 20-113).

B. La información

Aguirre (2014) señala:

La información es un activo que brinda valor al negocio; por ello, se necesita tener una adecuada protección frente a la constante exposición a distintas amenazas y vulnerabilidades. Esta puede adoptar distintas formas, de ahí surge la importancia de conocerlas para poder protegerla adecuadamente, estas formas son:

- ✓ Impresa o escrita en papel
- ✓ Almacenada electrónicamente
- ✓ Transmitida vía correo o e-mail
- ✓ Mostrada en videos
- ✓ Hablada en conversaciones [NTP ISO/IEC 177999] (p. 28).

Amorín (2016) enfatiza:

> **¿Por qué la información es el activo más importante en una empresa?**
> Se calcula que en 2014 la generación de información en internet superó los 4,4 zettabytes. La mayor parte de estos datos fueron generados por usuarios finales, pero se estima que cerca del 25% de la información gestionada en internet corresponde a entornos empresariales y corporativos. (p 1).

Amorín (2016) enfatiza:

> **La información es poder**
> Actualmente la información es probablemente el recurso intangible más importante que existe en el entorno empresarial. Diferentes encuestas muestran cómo sólo el 7% de las empresas que sufre una incidencia con pérdidas de información significativas sigue con su actividad empresarial 2 años después del suceso. (p. 3).

Figura 7. Pérdida de información. Fuente: Amorín (2016).

Amorín (2016) enfatiza:

> **¿Cuáles son las principales causas de la perdida de información?**
> Cada año se actualizan informes y aparecen nuevos rankings sobre las principales causas relacionadas con las pérdidas de información y las caídas de los sistemas IT en diferentes corporaciones, pero el top 4 de las principales causas siempre se repite:
> - **Errores operacionales:** Problemas de conectividad, anomalías en el software o el hardware, corte en suministro eléctrico.
> - **Errores humanos:** Borrado de Información, falta de control en la gestión de versiones, golpes en equipos, robo.
> - **Desastres naturales:** Incendios de Oficinas o Inundaciones.
> - **Ciberataques y malware:** El 7% de los ciberataques se centran en empresas con menos de 250 empleados. (p. 5).

C. ISO 27001

¿Qué es y para qué sirve?

Es una norma internacional de buenas prácticas, que se emplea para la certificación de los sistemas de gestión de seguridad de la información en las organizaciones empresariales.

Con esta certificación ISO 27001, la empresa, puede demostrar a sus clientes actuales y potenciales, así como a sus proveedores y accionistas, la integridad en el manejo de la seguridad de la información. También le posibilita reforzar la seguridad de la información y disminuir los riesgos de fraude, pérdida o filtración de información.

Basado anteriormente en el estándar BS 7799, el cual fue sustituido por esta norma, esta ha sido reorganizada para alinearse con otras normas internacionales. Fueron incorporados nuevos controles, poniendo énfasis en las métricas para la seguridad de la información y la gestión de incidentes. (Universidad ESAN, 2016)

Entre sus aspectos más importantes, la implementación de la norma ISO 27001 tiene como resultados:

- ✓ El énfasis en la mejora continua de procesos del sistema de gestión de seguridad de la información.
- ✓ La claridad en los requisitos de documentación y registros.
- ✓ Procesos de evaluación y gestión de los riesgos involucrados mediante el modelo del proceso planificar, hacer, verificar, actuar (PDCA sus siglas en inglés).
- ✓ La protección de los activos de la empresa, desde la información digital, los documentos y activos físicos (computadoras y redes) hasta los conocimientos de los empleados. (Universidad ESAN, 2016)

Fernández y Pacheco (2014) señalan:

> Esta norma adopta el modelo planificar, Hacer, verificar, actuar - PDCA en inglés, el cual se aplica para estructurar todos los procesos del SGSI, y tiene por objeto: Establecer, gestionar y documentar el SGSI, responsabilizando a la dirección, incluso en el monitoreo, auditoria y mejoramiento continuo.
>
> Para cumplir con este objetivo, la norma ISO 27001 ha sido estructurada de forma metodológica con cláusulas y anexos, que incluyen objetivos de control y controles, así como también su relación con otras normas ISO. Como punto de partida, la norma en referencia presenta un prefacio, de manera seguida se presentan las cláusulas y anexos. (p. 50).

En la tabla siguiente se muestra esta estructura:

Tabla 10

Estructura de la norma ISO 27001

Cláusula	**Nº**	**Sección**	**Subsección**
Introducción	0		
Objeto	1		
Referencias normativas	2		
Términos y definiciones	3		

Cláusula	Nº	Sección	Subsección
Sistema de gestión de seguridad de la información	4	4.1 Requisitos generales	
		4.2 Establecer y gestionar el SGSI	4.2.1 Establecer el SGSI
			4.2.2 Implementar y operar el SGSI
			4.2.3 Monitorear y revisar el SGSI
			4.2.4 Mantener y mejorar el SGSI
		4.3 Documentar el SGSI	4.3.1 Generalidades
			4.3.2 Controlar documentos
			4.3.3 Controlar los registros
Responsabilidad de la dirección	5	5.1 Compromiso de la dirección	
		5.2 Gestionar los recursos	5.2.1 Provisión de recursos
			5.2.2 Capacitación y entrenamiento
Auditorías internas del SGSI	6		
Revisión por la dirección del SGSI	7	7.1 Generalidades	
		7.2 Elementos de entrada para revisión	
		7.3 Resultados de la revisión	
Mejora del SGSI	8	8.1 Mejoramiento continuo	
		8.2 Acción correctiva	
		8.3 Acción preventiva	
Anexos		A. Normativo	
		B. Informativo	
		C. Informativo	

Fernández y Pacheco (2014) señalan:

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

- ✓ Política de seguridad
- ✓ Organización de la seguridad de la información
- ✓ Gestión de activos
- ✓ Seguridad de los recursos humanos
- ✓ Seguridad física y del entorno
- ✓ Gestión de las comunicaciones y 53 operaciones
- ✓ Control de accesos
- ✓ Adquisición, desarrollo y mantenimiento de sistemas de información
- ✓ Gestión de los incidentes de seguridad
- ✓ Gestión de la continuidad del negocio
- ✓ Cumplimiento normativo - legales, de estándares, técnicas y auditorias

Como objetivo final la norma ISO 27001 tiene como función principal, preservar la disponibilidad, la confidencialidad, la integridad de la información como el activo principal en una organización, entonces en este gráfico se vería la relación de todos los controladores para un mismo fin. (p. 52-53).

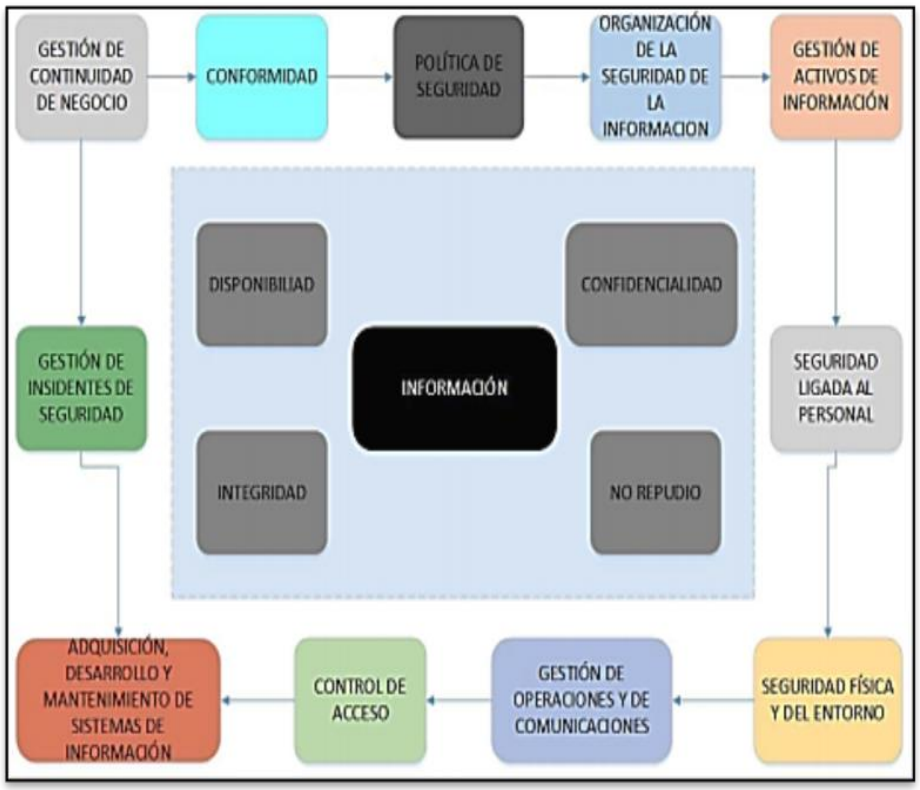


Figura 8. Enfoque de los controles de la norma ISO 27001. Fuente: *Fernández y Pacheco (2016).*

Fernández y Pacheco (2014) señalan:

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

- ✓ **Política de seguridad.**
  Se necesita una política que refleje las expectativas de la organización en materia de seguridad con el fin de suministrar administración con dirección y soporte, la cual también se puede utilizar como base para el estudio y evaluación en curso.
- ✓ **Organización de la seguridad de la información.**
  Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes**.**
- ✓ **Gestión de activos.**
  Muestra la necesidad de un inventario de los recursos de información de la organización y con base en este conocimiento, asegurar que se brinde un nivel adecuado de protección.
- ✓ **Seguridad de los recursos humanos.**
  Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad 55 y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la CAC o se debe implementar un plan para reportar los incidentes.
- ✓ **Seguridad física y del entorno.**
  Responde a la necesidad de proteger las áreas, el equipo y los controles generales.
- ✓ **Gestión de las comunicaciones y operaciones.**
  Los objetivos de esta sección son:
  - Asegurar el funcionamiento correcto y seguro de las instalaciones del procesamiento de información. Minimizar el riesgo de falla de los sistemas.
  - Proteger la integridad del software y la información.
  - Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.
  - Garantizar la protección de la información en las redes y de la infraestructura de soporte.
  - Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.
  - Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.
- ✓ **Control de accesos.**
  Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos. Adquisición,

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

- ✓ **Gestión de incidentes de seguridad.**

  Asegura que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.
- ✓ **Gestión de continuidad del negocio.**

  Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes, en caso de una falla grave o desastre. Cumplimiento normativo - legales, de estándares, técnicas y auditorías - Imparte instrucciones para que se verifique si el cumplimiento con la norma técnica ISO 27001 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de 57 auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio. (p. 54-56).

Universidad Autónoma de Tamaulipas (s.f.) define:

Conceptos básicos de la SI

La Seguridad de la Información consiste en mantener:

- ✓ **Confidencialidad:** Información disponible exclusivamente a personas autorizadas.
- ✓ **Integridad:** Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas. Contra la integridad la información puede parecer manipulada, corrupta o incompleta.
- ✓ **Disponibilidad:** Acceso y utilización de los servicios sólo y en el momento de ser solicitado por una persona autorizada. (p. 5).

CAPÍTULO III
IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. Fase 0: estudio de factibilidad

3.1.1. Factibilidad técnica

Esta tesis es viable técnicamente, ya que se cuenta con los recursos necesarios y básicos para poner en marcha el proyecto en la Institución Oficina de Economía del Ejército, se detalla las herramientas para el desarrollo del proyecto de tesis.

3.1.2. Factibilidad operativa

Esta tesis es factible operativamente, porque los investigadores tienen el conocimiento necesario y tendrá un gran impacto en la institución, ya que permitirá proteger los activos de información a través de lineamientos y medidas de seguridad. El proyecto es de responsabilidad de los alumnos de la Universidad Autónoma del Perú en donde se aplicará los conocimientos adquiridos en el transcurso de la formación profesional de la carrera de ingeniería de sistemas.

3.1.3. Factibilidad económica

Esta tesis es viable económicamente, ya que el departamento de telemática de la oficina de economía del ejército está dispuesto a mejorar el proceso de seguridad de información. De tal manera, se muestra los recursos necesarios:

Tabla 11

Cuadro de factibilidad técnica.

Categoría	Descripción	Unidad de medida	Precio Unitario	Cantidad	Total
Software	Microsoft Office 2013	Global	135	2	270
	Bizagi Modeler	Global	Versión gratuita	1	0
	Windows 2010	Global	390	2	780
	Antivirus	Global	83	2	166

Categoría	Descripción	Unidad de medida	Precio Unitario	Cantidad	Total
Hardware	Impresora multifuncional	Unidad	610	1	610
	Computador personal	Unidad	2374	2	4748
	USB	Unidad	60	1	60
Recurso humano	Especialista en la ISO 27001	Persona	5000	1	5000
	Gonzales Aybar, Richard	Persona	2500	1	2500
	Sarmiento Astudillo, Gustavo	Persona	2500	1	2500
Materiales	NTP-ISO27001:2014	Global	67	1	67
	Hojas bond	Millar	13	3	39
	Internet	Servicio Mensual	100	12	1200
	Folder	Unidad	0.5	20	10
	Engrapador	Unidad	12	1	12
	Perforador	Unidad	5	1	5
	Cd	Unidad	1.5	7	10.5
Recursos técnicos	Viáticos	Unidad	1000	1	1000
					18977.5
					1897.75
					20875.25

3.2. Fase i: contexto de la organización

3.2.1. Descripción de la institución diversificada:

La empresa

Institución responsable de ejecutar la fase de gasto del ejército dentro de las normativas y lineamientos establecidos por el ente rector (ministerio de economía y finanzas) Y en cumplimiento del calendario presupuestal del presente año.

Misión

Ser el órgano rector del sistema de administración económico financiero del ejército que se encarga de la ejecución presupuestal, la contabilidad y tesorería, así como de los fondos de seguros de retiro, cesación y préstamos. Actúa con un elevado nivel de profesionalismo y un ideal de servicio, fundamentado en la ética, los valores institucionales y en el cumplimiento de la normativa de los sistemas administrativos del estado.

Visión

Órgano de apoyo tecnológicamente moderno, conformado por personal altamente capacitado, para estar en condiciones de presentar los informes financieros y presupuestarios al ministerio de economía y finanzas.

Valores empresariales

- Tenacidad
- Disciplina
- Coordinación
- Planificación
- Racionalización
- Prioridad

Figura 9. Organigrama de la empresa oficina de economía del ejército.

Figura 10. Ubicación de la empresa oficina de economía del ejército.
Fuente: Google maps (2018).

3.2.2. Cartera de negocio

LUGAR	UEN	DIRECCIÓN	LOCAL
LIMA	ASESORAMIENTO AL JEFE DE LA OEE EN EL DESARROLLO DE SISTEMAS	Av. Paseo del Bosque 740 – San Borja	
	OPTIMIZACIÓN DEL FUNCIONAMIENTO DEL SISTEMA INFORMÁTICO DE LA OEE.		
	EVALUACIÓN DE LA SITUACIÓN DE LOS SISTEMAS DE LA OEE PARA DETERMINAR SUS NECESIDADES.		
	ANÁLISIS Y DIFUSIÓN DE LAS NUEVAS TECNOLOGÍAS EMERGENTES DE INTERÉS PARA EL SISTEMA		
	GESTIÓN DE LOS MEDIOS Y RECURSOS HUMANOS, PARA REALIZAR EL MANTENIMIENTO AUTORIZADO DE LOS SISTEMAS DE INFORMACIÓN EN ACTUAL PRODUCCIÓN		
	GESTIÓN INFORMÁTICA DE REMUNERACIONES		
	APROBACIÓN DE LAS FASES DE GASTO		
	OPERATIVIDAD DEL HARDWARE Y SOFTWARE QUE SE EMPLEA		
	FUNCIONALIDAD DEL SERVICIO DE CORREO ELECTRÓNICO "CHASQUI" Y DEL SISTEMA DE MENSAJERÍA Y COLABORACIÓN "OLAYA", INTRANET E INTERNET QUE BRINDA LA DITELE.		
	SOPORTE TÉCNICO ESPECIALIZADO		
	INFORMES TÉCNICOS A LOS EQUIPOS INFORMÁTICOS.		
	ASESORAMIENTO SOBRE LA ADQUISICIÓN DE NUEVOS RECURSOS INFORMÁTICOS		
	COORDINACIÓN CON LA DITELE, PARA MANTENER LA OPERATIVIDAD DEL SISTEMA DE TELEMÁTICA DEL EJÉRCITO.		
	RECOLECCIÓN DE INFORMACIÓN PARA LOS PROCESOS ESTADÍSTICOS EN LA OEE Y PREPARAR INFORMES ESTADÍSTICOS (BOLETINES, COMPENDIOS, ETC.) EN BASE A ELLOS.		
	DETERMINACIÓN DE LAS NECESIDADES DE INFORMACIÓN ESTADÍSTICA, VARIABLES E INDICADORES NECESARIOS PARA EL CUMPLIMIENTO DE LAS FUNCIONES DEL DETELE.		
	ELABORACIÓN DE ESTADÍSTICAS A FIN DE RECOMENDAR ACCIONES PARA INCREMENTAR LA EFICIENCIA DEL FUNCIONAMIENTO DE LA OEE.		
	PROPOSICIÓN DE ACCIONES RELACIONADAS AL ÁMBITO DE ESTADÍSTICA QUE PERMITA A LA OEE EJERCER LA SUPERVISIÓN NORMATIVA, EFECTUANDO LAS RECOMENDACIONES A QUE HUBIERA LUGAR		
	DESARROLLO DE ACTIVIDADES ORIENTADAS A LA CAPACITACIÓN DEL PERSONAL COMPROMETIDO EN LAS ACTIVIDADES ESTADÍSTICAS.		
	REMISIÓN DE INFORMACIÓN ESTADÍSTICA QUE SOLICITE LA DITELE		
	SEGURIDAD DE INFORMACIÓN		

Figura 11. Cartera de negocio.

3.2.3. Diagrama de contexto

Figura 12. Diagrama de contexto.

3.2.4. Proceso de seguridad de la información.

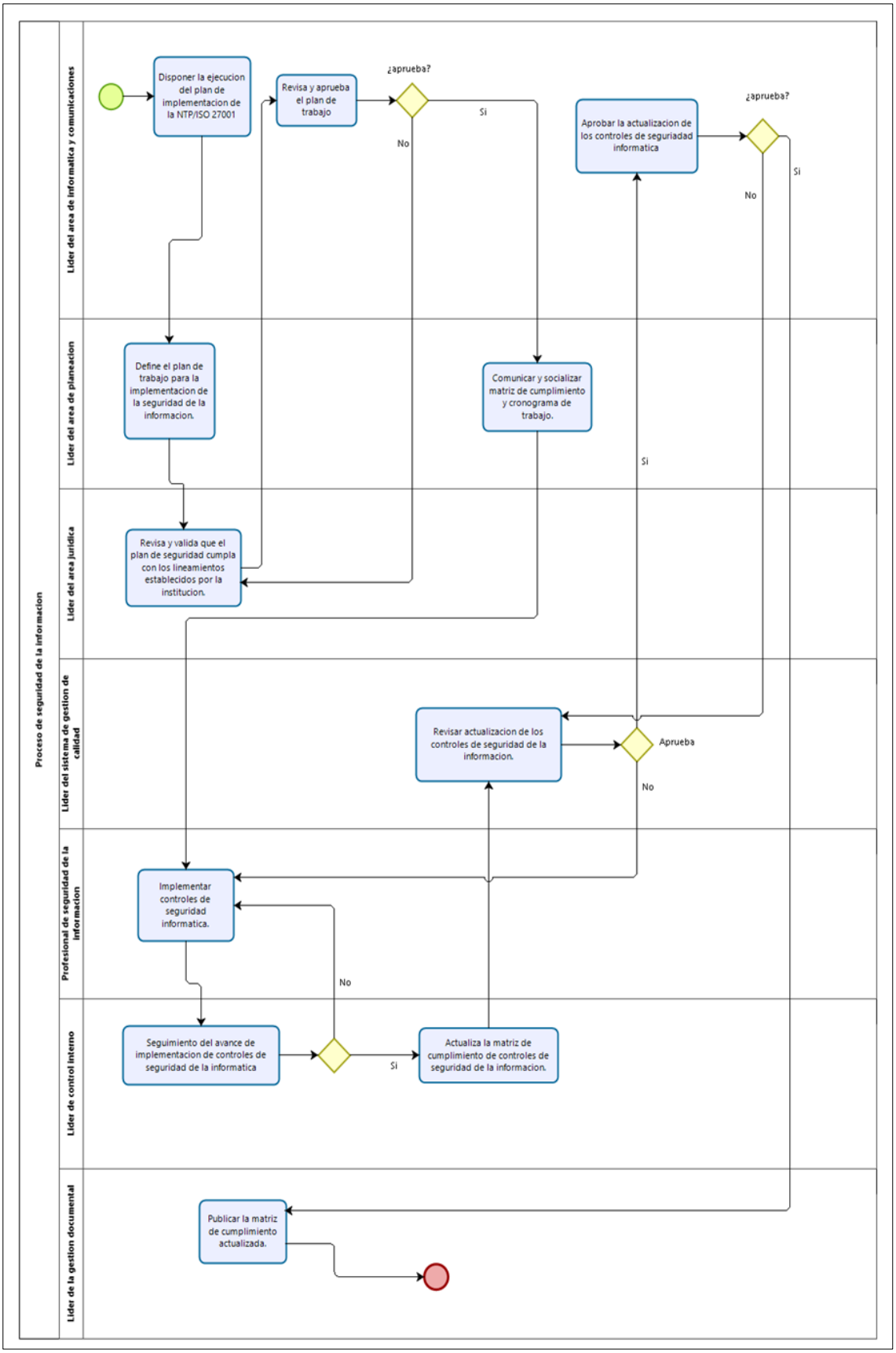


Figura 13. Flujograma del proceso de seguridad de la información del ejército del Perú (TO-BE).

3.2.5. Gestión de alcance

Tabla 12

Gestión del alcance

Gestión del alcance código versión 1. 0					
Proyecto:	Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el departamento telemática de la oficina de economía del ejército.				
Gerente:	Grl.Brig. Luis Enrique Bedoya Perales				
Preparado por:	Richard Gonzales Aybar	Fecha	02	01	19
Revisado por:	Gustavo Sarmiento Astudillo	Fecha	03	01	19
Aprobado por:	Líder del área Informática y comunicaciones.	Fecha	07	01	19

Alineamiento del proyecto

1. Objetivos estratégicos de la organización (a qué objetivo estratégico se alinea el proyecto)	2. Propósito del proyecto (beneficios que tendrá la organización una vez que el producto del proyecto esté operativo o sea entregado)
Nuestro objetivo es ejecutar correctamente la fase de gastos del presupuesto anual del ejército.	Establecer las medidas de seguridad basado en la NTP ISO 27001:2014 para asegurar la integridad, confiablidad y disponibilidad

3. Objetivos del proyecto

(Principalmente en términos de costo, tiempo, alcance, calidad)

Puesta en marcha del sistema de gestión de seguridad de la información para el departamento de telemática de la oficina de economía del ejército a través de la norma técnica peruana iso27001:2014 que facilita la gestión de seguridad de la información y la reducción de riesgos.

1. Criterios de éxito del proyecto

(Componentes o características que deben cumplirse en el proyecto para considerarlo exitoso)

El proyecto debe ser concluido en el horizonte de un año $\pm$ 2 meses.

El presupuesto otorgado de S/ 20,875.25 no debe exceder.

Implementar el plan de seguridad para el aseguramiento de los activos de información.

El proyecto incluye la creación del comité de gestión de seguridad de la información y la asignación de funciones.

El proyecto proporciona los controles de seguridad para el cumplimiento y mejora continua de proceso de seguridad.

Desarrollo de la propuesta

2. Descripción del producto del proyecto (características, funcionalidades, soporte, entre otros)

3. Descripción de los entregables principales del proyecto (características, funcionalidades, soporte, entre otros)

Entregable	Descripción
Inventario de activos	Se hará un inventario detallado de todos los activos del departamento de telemática.
Políticas de seguridad	Se diseñará políticas de seguridad alineadas a la NTP ISO 27001:2014.
Plan de continuidad del negocio	Se establecen los procedimientos necesarios para la continuidad del negocio.
Estructura de comité de gestión de seguridad	Se establecen las partes que conformaran el comité de gestión de seguridad.
Hoja de funciones del comité de gestión de seguridad	Se definen las funciones de cada una de las partes que conforman el comité de gestión de seguridad de información.
Herramientas de medición.	Se diseñarán encuestas y entrevistas para la obtención de información.
Informe de análisis de riesgo	Se elaborará la herramienta para el análisis adecuado de los riesgos.
Lista de controles de seguridad	Se elaborará un catálogo de controles de seguridad alineado a NTP ISO 27001:2014
Evaluación de procesos críticos del negocio.	Se hará un análisis comparativo de todos los procesos de la organización y se elegirá al más crítico.

Tabla 13

Contexto del proyecto

Contexto del proyecto
7. Límites del proyecto (Entregables no considerados como parte del proyecto) El proyecto está limitado a la puesta en marcha de algunos de los planes de seguridad que sean más fáciles y de costos factibles a solventar por la institución, ya que este proyecto se limita específicamente al departamento de telemática de la oficina de economía del ejército que se encuentra en el pentagonito. 8. Restricciones (Estado, calidad o sensación de estar forzado a tomar un determinado curso de acción o inacción. Una restricción o El proyecto debe cumplirse antes de la primera quincena de julio del 2017 El presupuesto máximo disponible es de S/ 20,875.25 Se contará con un capacitador (san Borja - pentagonito) La documentación del SGSI debe ser confidencial. Las disposiciones de los recursos financieros están sujetos a aprobaciones según el rango del importe. Para disponer de personal se debe contar con aprobación del gerente del área de proyectos. El horario de trabajo del personal del proyecto debe ceñirse a lo establecido por la organización. 1. Personal proyecto: lunes a viernes, un turno por día 8 horas. 9. Supuestos (Factores que, para efectos de planificación, se consideran verdaderas, reales o ciertas sin necesidad de pruebas)

3.2.6 Lista de stakeholder

Tabla 14

Leyenda de lista de stakeholders

Índice	**valor**
Poder	P
Interés	I
Alto	A
Bajo	B
Medio	M

Tabla 15

Cabecera de registro de versiones

Registro de interesados versión 1.1					
Proyecto	Implementación de la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el departamento telemática de la oficina de economía del ejército.				
Preparado por:	Sarmiento Astudillo, Gustavo	Fecha	02	01	19
Revisado por:	Gonzales Aybar, Richard	Fecha	02	01	19
Aprobado por:	Bedoya Perales, Luis Enrique	Fecha	07	01	19

Tabla 16

Lista de stakeholders

Apellidos y nombre	**Organización**	**Cargo**	**Matriz poder/Interés**	
			P	**I**
Castro Polo Fidel	Ejercito	Jefe del departamento de telemática	A	A
Sanchez Dávila Abigail Gilberto	Ejercito	Jefe de la sección operaciones y reportes	A	A
Pizango Sangama Carlos Jim	Ejercito	Administrador y soporte técnico SIAF	A	A
Ocas Vásquez Luis Dennis	Ejercito	Jefe de la sección soporte técnico	A	A
Rodríguez Poquioma Jacqueline	Ejercito	Analista de sistemas	B	B
Ninahuaman Hurtado David	Ejercito	Administrador de BD	B	M
Sotelo Flores María Elena	Ejercito	Secretaria	B	B
Villanueva Miriam Noemí	Ejercito	Analista programador	B	B
Torres Seminario Yraida	Ejercito	Analista programador	B	B
Arteaga Rosado Virginia	Ejercito	Analista programador	B	B
Severino Cruz Elvis	Ejercito	Ingeniería de sistemas	B	M
Salazar Valenzuela Carlos	Ejercito	Analista programador	B	B
Tácuna Calderon Luis	Ejercito	Especialista en redes y comunicaciones	A	A
Esteban Chuquimango Johnny	Ejercito	Especialista en redes y comunicaciones	A	A
Trigo Villaca Eduardo	Ejercito	Analista programador	B	M
Gonzales Aybar Richard	Ejercito	Analista programador	B	M
Villegas Yarleque Juan	Ejercito	Analista programador	B	M

3.3. Fase ii: liderazgo

3.3.1. Organigrama del comité de gestión de seguridad de información

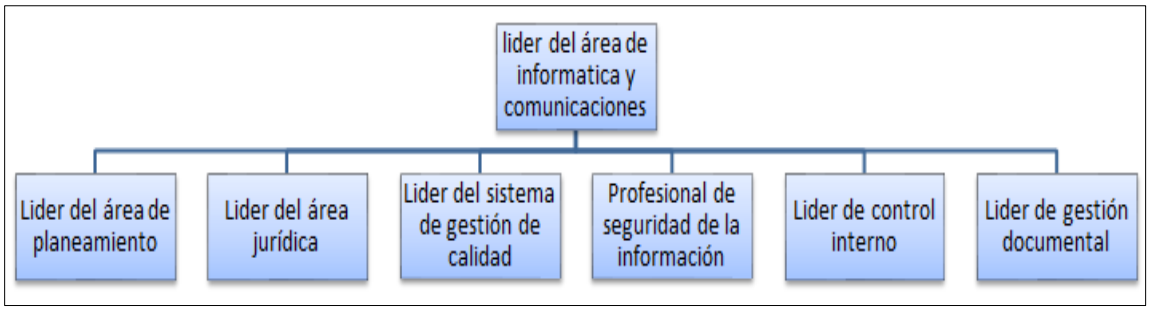


Figura 14. Organigrama del comité de gestión de seguridad de la información.

3.3.2. Funciones de los miembros del comité de gestión de seguridad

Funciones de los miembros del comité de gestión de seguridad de la información del departamento de telemática de la oficina de economía del ejército.

Tabla 17

Líder del área de informática y comunicaciones

Líder	
Nombre del cargo	Líder del área de informática y comunicaciones
Nombre	Castro Polo, Fidel
Personal a cargo	• Ocas Vásquez, Luis Dennis • Sánchez Dávila, Abigail • Rodríguez Paquioma, Jacqueline • Tácuna Calderon, Luis • Esteban Chuquimango, Johnny • Severino Cruz, Elvis
Perfil	
Educación	Superior
Formación	Informática y comunicaciones/ Administración y gestión
Experiencia	Gestión de procesos de seguridad
Responsabilidades generales	• Elaborar periódicamente planes estratégicos y operativos • Administrar los recursos bajo su responsabilidad • Comunicar los planes, objetivos, metas, políticas, normas y procedimientos al personal a su cargo. • Dirige procesos de evaluación y cambios tecnológicos • Evalúa procesos y políticas de seguridad de la información. • Define estrategias para para la gestión de seguridad informática. • Promueve el desarrollo de proyectos tecnológicos que ayuden a mitigar los riesgos de la organización. • Realiza estudios de factibilidad • Gestiona programas de capacitación en seguridad de la información. • Evalúa y monitorea el trabajo del personal a su cargo. • Cumple los lineamientos, normas y procedimientos administrativos y técnicos establecidos en la organización. • Otorga responsabilidades al personal a su cargo.

Tabla 18

Líder del área de planeación

Líder	
Nombre del cargo	Líder del área de planeación
Nombre	Ocas Vásquez, Luis Dennis
Perfil	
Educación	Superior
Formación	Informática y comunicaciones
Experiencia	Gestión de procesos y planeamiento estratégico TI
Responsabilidades generales	
• Planifica en coordinación con el líder de informática y comunicaciones para alcanzar las metas y cumplir con los objetivos de la planificación. • Impulsar planes estratégicos para aumentar la eficiencia del equipo. • Supervisa y coopera en el seguimiento de los planes de seguridad y cumplimiento del mismo.	

Tabla 19

Líder del área jurídica

Líder	
Nombre del cargo	Líder del área jurídica
Nombre	Sánchez Dávila, Abigail
Perfil	
Educación	Superior
Formación	Informática y comunicaciones
Experiencia	Procesos de seguridad.
Responsabilidades generales	
• Establecer las normas del comité de gestión de seguridad de la información. • Establecer las políticas de seguridad de la información. • Aprobar políticas de seguridad de la información. • Crear nuevas políticas de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información.	

Tabla 20

Líder del sistema de gestión de calidad

Líder	
Nombre del cargo	Líder del sistema de gestión de calidad
Nombre	Rodríguez Paquioma, Jacqueline
Perfil	
Formación	Informática y comunicaciones
Experiencia	Gestión de calidad de servicios
Responsabilidades generales	
• Supervisar que se cumplan las políticas establecidas en la organización. • Llevar a cabo auditorías internas para la mejora constante de la seguridad de la información. • Trabajar en conjunto con los auditores, supervisar y analizar resultados. • Realizar reuniones de trabajo con la finalidad de revisar la calidad y eficiencia de los servicios que se ofrecen. • Proponer cambios o ajustes en la documentación y supervisar que estos cambios se den. • Controlar y supervisar que no esté en funcionamiento documentación obsoleta del sistema de gestión de calidad. • Revisar y dar seguimiento al desarrollo del plan de capacitación del personal en lo relacionado con el sistema de gestión de la calidad.	

Tabla 21

Líder de la gestión documental

Líder	
Nombre del cargo	Líder de la gestión documental
Nombre	Severino Cruz, Elvis
Perfil	
Formación	Informática y comunicaciones
Experiencia	Gestión de proyectos
Responsabilidades generales	
• Coordinar y supervisar las actividades técnicas y administrativas de las Unidades de archivo de la institución. • Llevar el control, con evidencias, del desempeño del personal bajo su responsabilidad. • Elaborar Informes de sus actividades en proceso o concluidas. • Verificar y autorizar la digitalización de documentos. • Verificar la aplicación de las normas y políticas en función a la documentación de la organización. • Documentar los procesos de gestión de seguridad de la información. • Exigir documentación de todo lo establecido y acordado por el comité de gestión de seguridad de la información.	

Tabla 22

Líder de control interno

Líder	
Nombre del cargo	Líder de control interno
Nombre	Esteban Chuquimango, Johnny
Perfil	
Formación	Informática y comunicaciones
Experiencia	Implementación de controles de seguridad
Responsabilidades generales	
• Evaluar la ejecución y desarrollo del control en la organización. • Liderar las auditorias de control interno para validar la aplicación del sistema de seguridad de la información. • Coordinar la relación con los organismos de control externo, facilitando los requerimientos de información y la coordinación en los informes de la entidad. • Liderar el fomento de la cultura del control en la institución, que contribuya al mejoramiento continuo en el cumplimiento de la misión institucional. • Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de organización y recomendar los ajustes necesarios. • Comunicar a los directivos las conclusiones de auditoría y formular recomendaciones tendientes a corregir situaciones insatisfactorias.	

Tabla 23

Profesional de seguridad de la información

Líder	
Nombre del cargo	Profesional de seguridad de la información
Nombre	Tácuna Calderón, Luis
Perfil	
Formación	Informática y comunicaciones
Experiencia	Seguridad de la información
Responsabilidades generales	
• Administrar el desarrollo y la aplicación de las políticas de seguridad, normas y procedimientos para garantizar el mantenimiento continuo de la seguridad de la información. • Salvaguardar la información de la empresa. • Definir la arquitectura de la seguridad de red, acceso a la red y las políticas de monitoreo. • Desarrollar e implementar un sistema de gestión de seguridad de la información que permita identificar y dar respuesta a los nuevos riesgos de la organización. • Aprobar las principales iniciativas de para el incremento del nivel de seguridad de la información. • Garantizar que la seguridad sea parte del proceso de planificación de la información y un requisito necesario más de la organización.	

3.3.3. Políticas institucionales

Este proyecto pretende definir las necesidades conforme a la norma ISO 27001:2013 enfocados en los procesos de la organización en cuanto a políticas de seguridad de la información. Creando nuevas políticas necesarias que permitan fortalecer el sistema de información. Modificando políticas existentes de manera que sean claras y abarquen el contenido necesario que permita a la organización crear un sistema de gestión de la información conforme a estándares y leyes.

Objetivo general

Actualizar el documento actual de políticas de seguridad de la información del departamento de telemática de la oficina de economía del ejército. Estableciendo controles y métodos de divulgación de información.

Objetivos específicos

Definir políticas de seguridad de acuerdo con el análisis de la norma ISO 27001:2013 y establecerlas en el documento políticas de seguridad de la información del departamento de telemática de la oficina de economía del ejército.

Establecer controles de seguridad con el fin de velar el cumplimiento de las políticas de seguridad establecidas en el documento “políticas de seguridad de la información”.

Establecer metodologías y estrategias de divulgación de las políticas de seguridad para que todas las personas que tengan acceso a la información la conozcan.

Elaborar un plan de monitoreo para la revisión periódica de las políticas de seguridad de la información.

Políticas institucionales

1.-Mantener la estabilidad macroeconómica y la estabilidad financiera.
2.-Promover el desarrollo de la inversión pública para cerrar brechas.
3.-Mantener el equilibrio fiscal y la eficiencia financiera.
4.-Modernizar la gestión de las finanzas públicas.
5.-Desarrollar el mercado de deuda pública como instrumento sistémico de liquidez.
6.-Desarrollar el sistema financiero con mayor inclusión financiera.
7.-Ampliar facilidades para el desarrollo de la inversión privada.
8.-Fortalecer la colaboración y participación público-privada para impulsar la productividad y la competitividad.
9.-Consolidar la política y estrategia de apertura comercial.
10.-Promover la inversión en ciencia y tecnología.
11.-Promover la calidad del gasto social.
12.-Impulsar la gestión por resultados en las entidades públicas.
13.-Mejorar la transparencia en el uso de los recursos y la rendición de cuentas.
14.-Desarrollar capacidades especializadas en sistemas administrativos de inversión y presupuesto público.
15.-Resguardar la sostenibilidad financiera de los gobiernos subnacionales y distribuir eficientemente los recursos determinados.

3.3.4. Políticas de seguridad

Políticas de seguridad de información

Medidas de seguridad de las informaciones y empleo de la trituradora

- Todos los papeles, borradores y documentos fuera de uso deberán ser destruidos.
- Todo el personal militar y civil, tiene la responsabilidad y compromiso de mantener el secreto de las informaciones que por razones de trabajo y/o función aleguen a su conocimiento, siendo responsables de cualquier indiscreción o infidencia que cometan, haciéndose acreedores a la sanción correspondiente contempladas en el código de justicia militar (OM).
- Se debe restringir al máximo, el acceso de personal a material clasificado.
- Está prohibido arrojar documentos comunes y/o clasificados a cilindros y/o tacos de basura; así como su incineración en lugares no autorizados, como también está totalmente prohibido, evacuar la documentación depurada de los archivos al exterior en vehículos sin la trituración correspondiente.
- Está terminantemente prohibido sacar al exterior CD's y/o diskettes con información común o reservada al exterior. Salvo autorización del general brigada y director general de la OEE.
- Está prohibido, sacar todo tipo de información (común o clasificada) en cualquier medio de almacenamiento llámese diskettes, cd, disk zip; disco duro; tape backups, memoria usb, etc)
- Está prohibido formular documentos clasificados fuera del centro de trabajo en computadoras personales o alquiladas.
- El acceso a los terminales o computadoras será solo exclusivo del personal que labora en dicha Oficina.
- El personal militar y/o civil que tenga correo electrónico (email), no podrá enviar a través de este medio, mensajes relacionado a asuntos militares o información relacionada a la institución.
- Colocar claves de acceso “password", en las computadoras para evitar que el personal no autorizado tenga acceso a los archivos.

Ley n° 30171 ley que modifica la ley 30096, “ley de delitos informáticos”

1. Castiga al que accede ilícitamente a un sistema informático (Art. 02 de 01 a 04 años de cárcel) sin contar con autorización o excediendo de ella vulnerando las medidas de seguridad entendemos por sistema informático todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí para el manejo de datos.
2. Protege la integridad de los datos informáticos contra el tráfico ilegal o interceptación de estos. Según (Art. 03, Art 07 ambos de 03 a 06 años de cárcel) castiga al que introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos. Según (Art. 06 de 03 a 05 años de cárcel) castiga al quien crea, ingresa o utiliza indebidamente una base de datos sobre una persona para comercializar, vender, favorecer o facilitar información relativa a cualquier ámbito, creando o no perjuicio.
3. Protege la integridad de los sistemas informáticos (art 04, de 03 a 05 años de cárcel) castiga al que inutilice, entorpezca, o impida el acceso a un sistema informático.
4. Sanciona la clonación en el fraude informático (Art. 08, de 03 a 08 años de cárcel) el termino clonación está asociada a replica de información de un sistema a otro. Este delito se relaciona con las tarjetas de crédito.
5. Castiga al que suplanta identidad de una persona jurídica (Art. 09, de 03 a 05 años de cárcel) que, mediante una tecnología de información, realiza algún perjuicio material o moral.
6. La ley también sanciona (Art 10 de 01 a 04 años de cárcel) a los responsables de crear, diseñar, desarrollar o vender programas que ayuden a la comisión de delitos descritos.

_____

Post Firma: ……..

DNI: ……....

HUELLA

EJÉRCITO DEL PERÚ
REPÚBLICA DEL PERÚ
OFICINA DE ECONOMÍA DEL EJÉRCITO

O-214591564-O+
LUIS. E. BEDOYA PERALES

3.4. Fase iii: planificación

Histórico de versiones

Tabla 24

Plantilla de historial de versiones

Versión	Fecha	Motivo del Cambio	Modificado por:
0.1	02-01-2019	Creación del documento	Gonzales Aybar, Richard

3.4.1. Plan de gestión de riesgos

A. Información general

Tabla 25

Plantilla para la gestión de riesgos

Código del proyecto	0001
Nombre del proyecto	Implementación de un sistema de gestión de la seguridad de la información basado en la NTP/ISO 27001 para mejorar el proceso de seguridad de información en el departamento telemática de la oficina de economía del ejército.

B. Metodología de gestión de riesgos

Se identifica las acciones a realizar, las herramientas que interviene y las fuentes de información por cada proceso que interviene en la gestión de riesgos.

Tabla 26

Lista de procesos para la gestión de riesgos

Proceso	Descripción	Herramientas	Fuentes de información
Planificación de gestión de los riesgos	Elaborar plan de gestión de riesgos	PMBOK	Sponsor y usuarios. PM y equipo de proyecto
Identificación de riesgos	Identificar que riesgos pueden afectar el proyecto y documentar sus características	Checklist de riesgos listado de riesgos de la compañía	Sponsor y usuarios. PM y equipo de proyecto Archivos históricos de proyectos

Proceso	Descripción	Herramientas	Fuentes de información
Análisis cualitativo de riesgos	Elaboración de matriz de riesgos.	ISO 31000	Sponsor, stakeholders y equipo de proyecto.
Planificación de la respuesta a riesgos	Definir acción para la mitigación de riesgos.	ISO 31000	Equipo de proyecto.
Seguimiento y control de riesgos	Elaboración de controles para auditoría interna.	Metodología PDCA	Equipo de proyecto.

C. Roles y responsabilidades de la gestión de riesgos

Se identifican los roles que intervienen en los procesos de la gestión de riesgos, así como sus respectivas responsabilidades.

Tabla 27

Lista de procesos con responsables

Procesos	Roles	Responsabilidades
Planificación de gestión de los riesgos	Líder del área de planeación	Elaboración del plan de gestión de riesgos.
Identificación de riesgos	Líder de sistemas de gestión de Calidad.	Identificación de riesgos.
Análisis cualitativo de riesgos	Líder de sistemas de gestión de Calidad.	Identificación de tipo de riesgos.
Planificación de la respuesta a riesgos	Profesional de seguridad de la información.	Elaboración del plan de continuidad de negocio.
Seguimiento y control de riesgos	Líder de control interno.	Encargado de verificar y supervisar el tratamiento de los riesgos.

D. Calendario de la gestión de riesgos

Se identifica el momento, la frecuencia y la fecha de ejecución de las actividades de cada uno de los procesos involucrados en la gestión de riesgos.

Tabla 28

Lista de procesos con tiempo de ejecución

Proceso	Momento de ejecución	Frecuencia	Fecha ejecución
Planificación de gestión de los riesgos	Al inicio del proyecto	Anual	02-01-2019
Identificación de riesgos	Al inicio del proyecto En cada reunión del equipo del proyecto	Anual	02-01-2019
Análisis cualitativo de riesgos	Al inicio del proyecto En cada reunión del equipo del proyecto	Anual	02-01-2019
Planificación de la respuesta a riesgos	En la ejecución del proyecto.	Anual	02-01-2019
Seguimiento y control de riesgos	En seguimiento y control del proyecto.	Anual	02-01-2019

E. Categorías de riesgo (RBS)

Se debe de identificar las categorías de riesgo que pueden afectar al proyecto. Con el fin de clasificar los riesgos identificados a una categoría en particular

Tabla 29

Lista de riesgos (identificación de riesgos)

Riegos	Tipos		
Descripción	Técnico	Externo	Organizacional
acceso no permitido y/o autorizado			X
Ataques externos / internos (hacking).		X	X
Cambio de privilegios sin coordinación y/o autorización.			X
Desastres naturales.		X	

Riegos	**Tipos**		
Descripción	Técnico	Externo	Organizacional
Divulgación de información.			X
Error de usuario.			X
Instalación de software no autorizado.	X		
Interceptación no autorizada de información en tránsito.			X
Interrupción en los servicios.	X		
Modificación sin autorización.			X
Robo de equipos.		X	X
Robo de información.		X	X
Suplantación de identidad de usuarios.		X	X
Uso inadecuado de sistemas para generar fraudes.		X	X
Uso inadecuado de sistemas que generan interrupción.		X	X
Abuso de privilegios.			X

3.4.2. Matriz de probabilidad e impacto adjunta

Tabla 30

Impacto del riesgo

Nivel	**Valor**	**Descripción**
1	Bajo	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Moderado	Si el hecho llegara a presentarse, tendría bajo impacto sobre la entidad.
3	Alto	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Critico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

Tabla 31

Probabilidad del riesgo

Nivel	Valor	Descripción
1	Improbable	Es muy poco probable que el evento ocurra.
2	Posible	Es poco probable que el evento ocurra.
3	Probable	Es medianamente probable que el evento ocurra.
4	Muy probable	Es altamente probable que el evento ocurra.

Tabla 32

Valoración del riesgo

Nivel	Valor	Descripción
1 - 4	Riesgo bajo	El propietario del activo lo administra con procedimientos rutinarios o decide aceptar el riesgo.
5 - 8	Riesgo medio	El riesgo es administrado por los grupos de incidentes bajo procedimientos normales de interés.
9 – 12	Riesgo alto	Requiere acciones correctivas controladas por grupos de manejo de incidentes en periodos de tiempos razonables.
13 - 16	Riesgo extremo	Requiere fuertes medidas correctivas, planes de tratamiento implementados en corto tiempo, reportados y controlados con atención directa de la alta dirección.

Tabla 33

Matriz de probabilidad vs impacto del riesgo

Riesgo	Descripción de riesgo	Probabilidad	Impacto	PXI	Nivel riesgo
R1	Acceso no permitido y/o autorizado	4	4	16	Riesgo extremo
R2	Ataques externos / internos (hacking).	4	4	16	Riesgo extremo
R3	Cambio de privilegios sin coordinación y/o autorización.	4	3	12	Riesgo alto
R4	Desastres naturales.	1	4	4	Riesgo bajo
R5	Divulgación de información.	4	2	8	Riesgo medio

Riesgo	Descripción de riesgo	Probabilidad	Impacto	PXI	Nivel riesgo
R6	Error de usuario.	4	3	16	Riesgo extremo
R7	Instalación de software no autorizado.	3	2	6	Riesgo medio
R8	Interceptación no autorizada de información en tránsito.	2	3	12	Riesgo medio
R9	Interrupción en los servicios.	3	4	16	Riesgo extremo
R10	Modificación sin autorización.	2	3	6	Riesgo medio
R11	Robo de equipos.	3	2	6	Riesgo medio
R12	Robo de información.	3	4	12	Riesgo alto
R13	Suplantación de identidad de usuarios.	2	3	6	Riesgo medio
R14	Uso inadecuado de sistemas para generar fraudes.	2	4	8	Riesgo medio
R15	Uso inadecuado de sistemas que generan interrupción.	2	4	8	Riesgo medio
R16	Abuso de privilegios.	4	3	12	Riesgo alto

Tabla 34

Tratamiento del riesgo

Riesgo	Desc. de riesgo	Prob.	Desc.	Imp.	Desc.	PXI	Nivel riesgo	Tratamiento del riesgo
R1	Acceso no permitido y/o autorizado	4	Muy probable	4	critico	16	Riesgo extremo	Modificar
R2	Ataques externos / internos (hacking).	4	Muy probable	4	critico	16	Riesgo extremo	Modificar

Riesgo	Desc. de riesgo	Prob.	Desc.	Imp.	Desc.	PXI	Nivel riesgo	Tratamiento del riesgo
R3	Cambio de privilegios sin coordinación y/o autorización.	4	Muy probable	3	alto	12	Riesgo alto	Modificar
R5	Divulgación de información.	4	Muy probable	2	moderado	8	Riesgo medio	Modificar
R6	Error de usuario.	4	Muy probable	4	alto	16	Riesgo extremo	Modificar
R7	Instalación de software no autorizado.	3	probable	2	moderado	6	Riesgo medio	Modificar
R8	Interceptación no autorizada de información en tránsito.	3	Muy probable	2	critico	6	Riesgo medio	Modificar
R9	Interrupción en los servicios.	4	probable	4	moderado	16	Riesgo extremo	Modificar
R10	Modificación sin autorización.	2	posible	3	alto	6	Riesgo medio	Modificar
R11	Robo de equipos.	3	probable	2	moderado	6	Riesgo medio	Modificar
R12	Robo de información.	3	probable	4	critico	12	Riesgo alto	Modificar
R13	Suplantación de identidad de usuarios.	2	posible	3	alto	6	Riesgo medio	Modificar
R14	Uso inadecuado de sistemas para generar fraudes.	2	posible	4	critico	8	Riesgo medio	Modificar
R15	Uso inadecuado de sistemas que generan interrupción.	2	posible	4	critico	8	Riesgo medio	Modificar
R16	Abuso de privilegios.	4	Muy probable	3	critico	12	Riesgo alto	Modificar

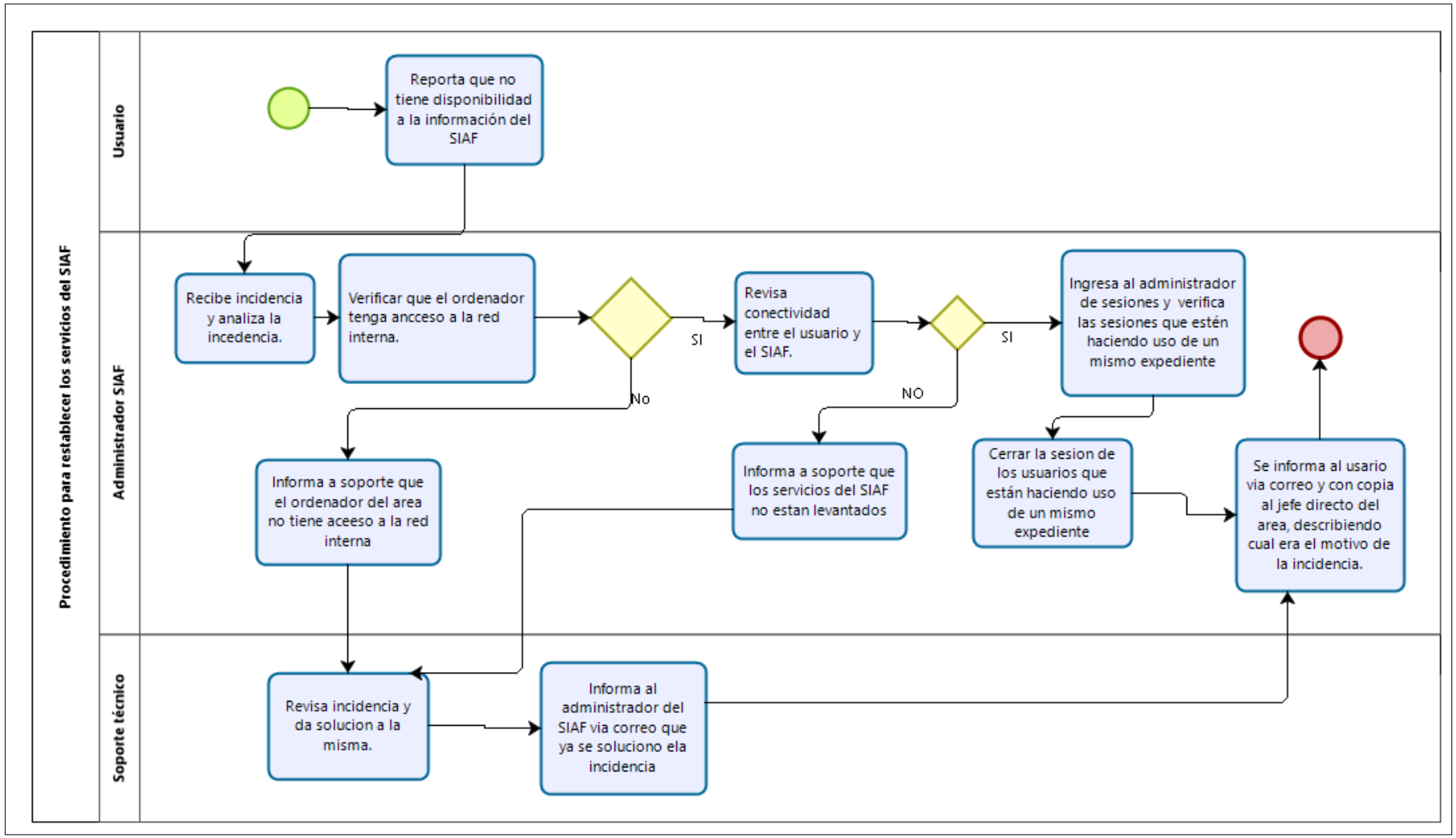


Figura 15. Proceso para restablecer los servicios del SIAF.

Tabla 35

Procedimiento de seguridad para restablecer los servicios del SIAF

Procedimiento de seguridad para restablecer los servicios del SIAF			
Control de versiones del procedimiento de seguridad			
Versión	Fecha	Procedimiento	Creado
1.0	14-01-2019	Restablecer los servicios	Sarmiento Astudillo, Gustavo
Actores del procedimiento de seguridad			
Nº		Responsable	
1		Usuario final	
2		Administrador SIAF	
3		Soporte técnico	

Descripción de actividades (flujo básico)

1. El usuario reporta que no tiene disponibilidad a la información del SIAF.
2. El administrador SIAF recibe y analiza la incidencia.
3. El administrador SIAF verifica que el ordenador tenga acceso a la red interna. Si el ordenador tiene acceso a la red interna sigue el flujo básico en caso no tenga acceso, revisar el flujo alternativo (A1 – A4)
4. El administrador del SIAF revisa conectividad entre el usuario y el servicio SIAF. Si el usuario tiene conectividad con el servicio SIAF, sigue el flujo básico en caso no tenga conectividad revisar el flujo alternativo (B1 – B4)
5. El administrador SIAF ingresa al administrador de sesiones e identifica cuales son los usuarios que están haciendo uso de un mismo expediente.
6. El administrador SIAF cierra la sesión de los usuarios que están haciendo uso de un mismo expediente.
7. El administrador del SIAF informa al usuario vía correo electrónico y con copia al jefe directo del área describiendo cual era el motivo de la incidencia.

Descripción de actividades (flujo alternativo)

A1 El administrador del SIAF informa a soporte técnico que el ordenador del área no tiene acceso a la red interna.

A2 Soporte técnico revisa incidencia y da solución a la misma

A3 Soporte técnico informa al administrador del SIAF vía correo electrónico que se solucionó la incidencia.

A4 El administrador del SIAF informa al usuario vía correo electrónico y con copia al jefe directo del área describiendo cual era el motivo de la incidencia.

B1 El administrador SIAF informa a soporte que los servicios del SIAF no están levantados.

B2 Soporte técnico revisa incidencia y da solución a la misma

B3 Soporte técnico informa al administrador del SIAF vía correo electrónico que se solucionó la incidencia.

B4 El administrador del SIAF informa al usuario vía correo electrónico y con copia al jefe directo del área describiendo cual era el motivo de la incidencia.

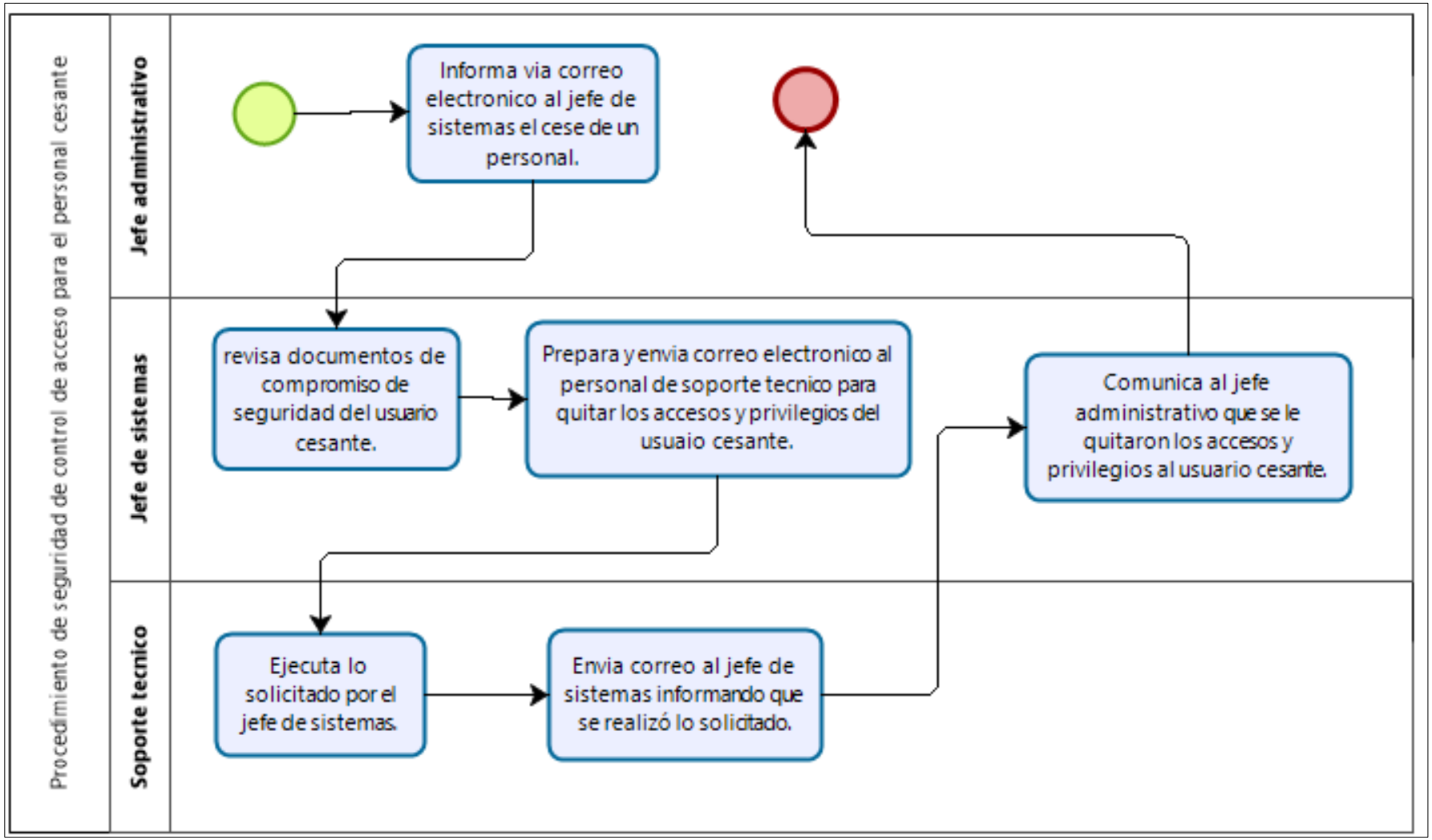


Figura 16. Proceso de seguridad de control de acceso 1/2.

Tabla 36

Procedimiento de seguridad de control de acceso para el personal cesante

Procedimiento de seguridad de control de acceso para el personal cesante			
Control de versiones del procedimiento de seguridad			
Versión	Fecha	Procedimiento	Creado
1.0	14-01-2019	Control de acceso (2/2)	Sarmiento Astudillo, Gustavo
Actores del procedimiento de seguridad			
Nº		Responsable	
1		Jefe administrativo	
2		Jefe de sistemas	
3		Soporte técnico	
Descripción de actividades			
1. El jefe administrativo informa vía correo electrónico al jefe de sistemas del cese de un personal. 2. El jefe de sistemas revisa el documento de compromiso de seguridad del usuario cesante 3. El jefe de sistemas prepara y envía correo electrónico al personal de soporte técnico para quitar los accesos y privilegios del usuario cesante. 4. Soporte técnico ejecuta lo solicitado por el jefe de sistemas. 5. Soporte técnico envía correo electrónico al jefe de sistemas informando que se realizó lo solicitado. 6. El jefe de sistemas comunica al jefe administrativo que se le quitaron los accesos y privilegios al usuario cesante.			

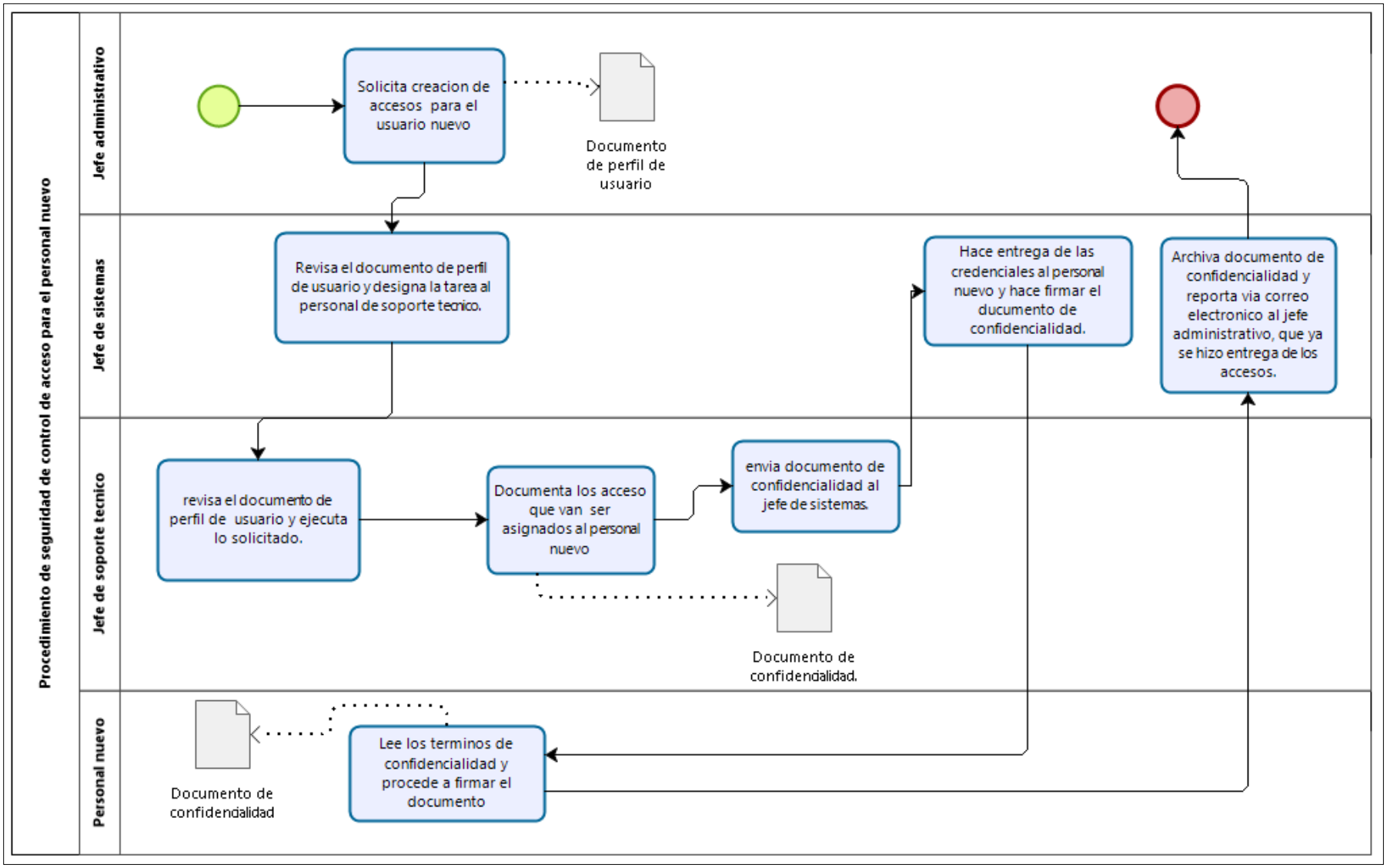


Figura 17. Proceso de seguridad de control de acceso 2/2

Tabla 37

Procedimiento de seguridad de control de acceso para el personal nuevo

Procedimiento de seguridad de control de acceso para el personal nuevo			
Control de versiones del procedimiento de seguridad			
Versión	Fecha	Procedimiento	Creado por
1.0	14-01-2019	control de acceso (1/2)	Sarmiento Astudillo, Gustavo
Actores del procedimiento de seguridad			
Nº		Responsable	
1		Jefe administrativo	
2		Jefe de sistemas	
3		Soporte técnico	
4		Personal nuevo	
Descripción de actividades			
1. El jefe administrativo solicita creación de acceso para el usuario nuevo y adjunta documento de perfil de usuarios			
2. El jefe de sistemas revisa el documento de perfil de usuario y designa la tarea al personal de soporte técnico.			
3. Soporte técnico revisa el documento de perfil de usuario y ejecuta lo solicitado.			
4. Soporte técnico documento los accesos que van a ser asignados al personal nuevo y prepara el documento de confidencialidad.			
5. Soporte técnico envía documento de confidencialidad al jefe de sistemas.			
6. El jefe de sistemas hace entrega de las credenciales al personal nuevo y hace firmar el documento de confidencialidad.			
7. El personal nuevo lee los términos de confidencialidad y procede a firmar el documento.			
8. El jefe de sistemas archiva documento de confidencialidad y reporta vía correo electrónico al jefe administrativo, que ya se hizo entrega de los accesos al personal nuevo.			

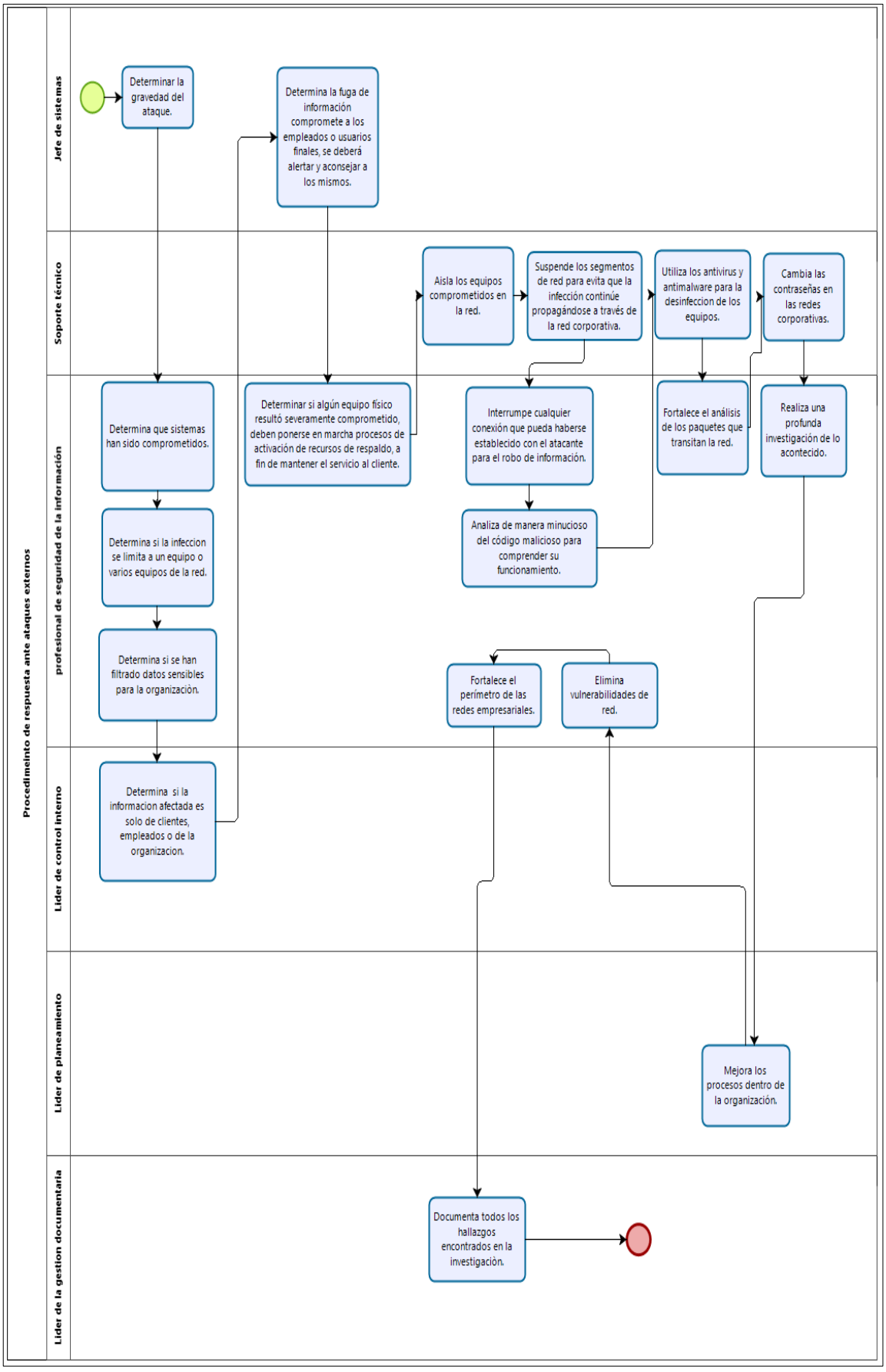


Figura 18. Proceso de seguridad de respuestas ante ataques de seguridad.

Tabla 38

Procedimiento de seguridad de respuesta ante ataques externos

Procedimiento de seguridad de respuesta ante ataques externos

Control de versiones del procedimiento de seguridad

Versión	Fecha	Procedimiento	Creado
1.0	14-01-2019	Ataques externos	Sarmiento Astudillo, Gustavo

Actores del procedimiento de seguridad

Nº	Responsable
1	Jefe de sistemas
2	Profesional de seguridad
3	Líder de control interno
4	Soporte Técnico
5	Líder del área de planeación
6	Líder de gestión documental

Descripción de actividades

1. Jefe de sistemas solicita determinar la gravedad del ataque al profesional de seguridad.
2. Profesional de seguridad determina que sistemas han sido comprometidos.
3. Profesional de seguridad determina si la infección se limita a un equipo o varios equipos de la red.
4. Profesional de seguridad determina si se han filtrado datos sensibles para la organización.
5. Líder de control interno determina si la información afectada es solo de clientes, empleados o de la organización.
6. Jefe de sistemas si la fuga de información compromete a los empleados o usuarios finales, se deberá alertar y aconsejar a los mismos.
7. Profesional de seguridad Si algún equipo físico resultó severamente comprometido, deben ponerse en marcha procesos de activación de recursos de respaldo, a fin de mantener el servicio al cliente.
8. Soporte técnico aísla los equipos comprometidos en la red.
9. Soporte técnico suspende los segmentos de red para evita que la infección continúe propagándose a través de la red corporativa.
10. Profesional de seguridad interrumpe cualquier conexión que pueda haberse establecido con el atacante para el robo de información.
11. Profesional de seguridad analiza de manera minucioso del código malicioso para comprender su funcionamiento.
12. Soporte técnico utiliza los antivirus y antimalware para la desinfección de los equipos.
13. Profesional de seguridad fortalece el análisis de los paquetes que transitan la red.
14. Soporte técnico cambia las contraseñas en las redes corporativas.
15. Profesional de seguridad realiza una profunda investigación de lo acontecido.
16. Líder del área de planeación mejora los procesos dentro de la organización.
17. Profesional de seguridad elimina vulnerabilidades de red.
18. Profesional de seguridad Fortalece el perímetro de las redes empresariales.
19. Líder de gestión documental documenta todos los hallazgos encontrados en la investigación.

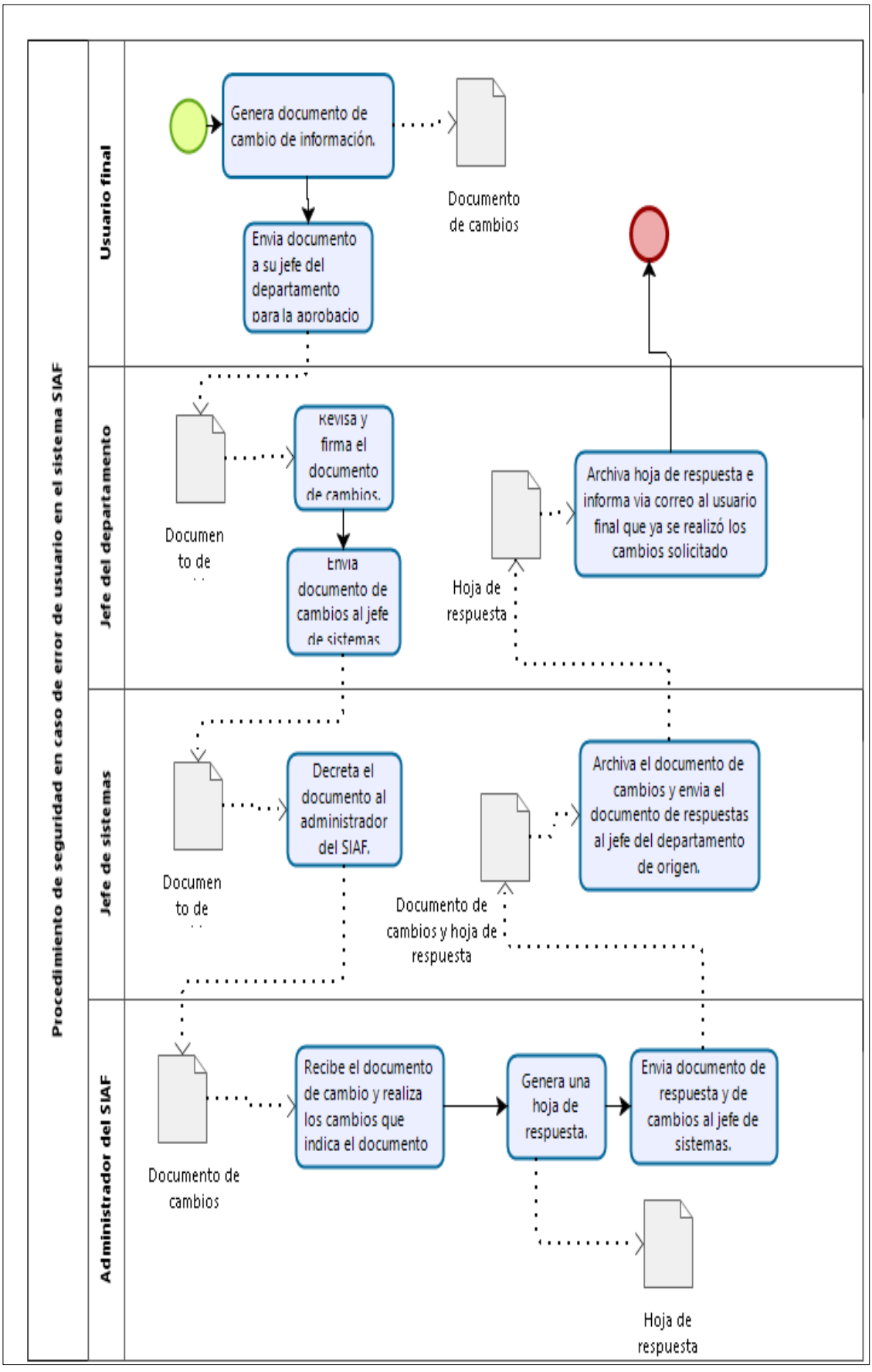


Figura 19. Procedimiento de seguridad en caso de error de usuario.

Tabla 39

Procedimiento de seguridad en caso de error de usuario en el SIAF

Procedimiento de seguridad en caso de error de usuario en el SIAF			
Control de versiones del procedimiento de seguridad			
Versión	Fecha	Procedimiento	Creado por
1.0	14-01-2019	Error de usuario	Sarmiento Astudillo, Gustavo
Actores del procedimiento de seguridad			
Nº		Responsable	
1		Usuario final	
2		Jefe del departamento	
3		Jefe de sistemas	
4		Administrador SIAF	
Descripción de actividades			
1. El usuario genera documento de cambio de información.			
2. El usuario envía documento a su jefe del departamento para la aprobación del cambio de			
3. El jefe del departamento revisa y firma el documento de cambios			
4. El jefe del departamento envía documento de cambios al jefe de sistemas.			
5. El jefe de sistemas decreta el documento al administrador del SIAF.			
6. El administrador del SIAF recibe el documento de cambio y realiza los cambios que indica el documento.			
7. El administrador del SIAF genera una hoja de respuestas.			
8. El administrador del SIAF envía documento de respuesta y de cambios al jefe de sistemas.			
9. El jefe de sistemas archiva el documento de cambios y envía el documento de respuestas al jefe del departamento de origen.			
10. El jefe del departamento informa vía correo al usuario final que ya se realizó los cambios solicitados.			

3.5. Fase iv: soporte

3.5.1. Lista de activos

Tabla 40

Lista de activos del ejército

Tabla de inventario de activos	
Ámbito	Activo
Instalaciones	Data center
Hardware	Servidores
	Firewall
	Switch
Software base	Windows server 2012
	Windows 7 y 10
	Centos Linux 6.2
	Debian
Aplicaciones	Oracle 11g
	SIAF
	SIGE
	E-pop3
	Java
	IDE Netbeans 8.1
	IDE Eclipse endigo
Datos	Datos
Red	Acceso a internet
	Red de datos
	Internet
	Intranet
Servicios	Telefonía
	Protección contra amenazas
	Energía eléctrica

Tabla de inventario de activos	
Equipos adicionales	Estabilizador
	Servidor de archivos
	Servidor de impresión
	Ups
	Router
	Switch
	Servidor de correos
Personal	Soporte técnico
	Administradores de base de datos.
	Desarrolladores
	Analista de sistemas
	Administrativos
Soporte de información	Nas
	Discos duros.
	Memorias USB y CD´s.

3.5.2. Gestión de recursos

Recursos

Presentamos los recursos determinados para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

Tabla 41

Costo capacitación anual del comité de gestión de seguridad.

Capacitación anual del comité		
Capacitación	Cant. Personas	Costo total (S/)
Capacitación 1	2	6000.00
Capacitación 2	2	6000.00
Capacitación 3	2	6000.00
Subtotal		S/.18.000

Tabla 42

Costo anual de recursos humanos

Costo anual de recursos humanos		
Integrantes	Meses trabajados	Costo Total (S/.)
Líder del área de informática y comunicaciones.	12	48,000
Líder del área de planeación.	12	36,000
Líder del área jurídica.	12	36,000
Líder del sistema de gestión.	12	36,000
El profesional de seguridad de la información.	12	36,000
Líder de control interno.	12	36,000
Líder de la gestión documental.	12	36,000
Subtotal		S/. 264.000

Tabla 43

Coste de hardware

Coste de hardware	**Monto (s/.)**
1 Computador personal	2.500
Acessórios (teclado, mouse, supresor de pico).	130
1 Impresora Epson Stylius TX125	160
Memoria USB 32 gb.	60
Subtotal	S/.2.850

Tabla 44

Coste de suministros

Suministros y otros recursos	
Gastos Varios (útiles de escritorio, viáticos y servicios etc.)	S/.900
Subtotal	S/. 900

Tabla 45

Costo total del proyecto

Coste total del proyecto	
Capacitación anual del comité	S/. 18.000
Costo anual de recursos humanos	264.000
Hardware	2.850
Suministros y otros recursos	900

3.5.3. Competencias

Historial de versiones

Tabla 46

Plantilla de historial de versiones

Versión	**Fecha**	**Motivo del cambio**	**Modificado por:**
0.1	02-01-2019	Creación del documento	Sarmiento Astudillo, Gustavo

Tabla 47

Líder del área de informática y comunicaciones

Líder	
Nombre del cargo	Líder del área de informática y comunicaciones
Perfil	
Formación	Título profesional o técnico en la especialidad Ingeniería de sistemas o computación e informática o afines.
Especialización	Capacitación acreditada en temas relacionas a la seguridad de la información (no menor a 50 horas pedagógicas presenciales).
Experiencia	**General:** Experiencia laboral general de cinco (05) años en el sector público o privado. **Específico:** Experiencia de tres (03) años en cargos y/o funciones afines en el sector público.
Conocimiento	• Ingles • NTP/ISO 27001 • Gestión de proyectos.
Competencias	• Negociación. • Proactivo, organizado y disciplinado. • Habilidad de comunicaciones oral y escrito. • Capacidad de trabajo en equipo y bajo presión. • Capacidad analítica y lógica.
Responsabilidades generales	• Elaborar periódicamente planes estratégicos y operativos. • Administrar los recursos bajo su responsabilidad.

- Comunicar los planes, objetivos, metas, políticas, normas y procedimientos al personal a su cargo.
- Dirige procesos de evaluación y cambios tecnológicos.
- Evalúa procesos y políticas de seguridad de la información.
- Define estrategias para para la gestión de seguridad informática.
- Promueve el desarrollo de proyectos tecnológicos que ayuden a mitigar los riesgos de la organización.
- Realiza estudios de factibilidad.
- Gestiona programas de capacitación en seguridad de la información.
- Evalúa y monitorea el trabajo del personal a su cargo.
- Cumple los lineamientos, normas y procedimientos administrativos y técnicos establecidos en la organización.
- Otorga responsabilidades al personal a su cargo.

Tabla 48

El líder del área de planeación

Líder	
Nombre del cargo	Líder del área de planeación
Perfil	
Formación	Título profesional o técnico en la especialidad ingeniería de sistemas o computación e informática o afines.
Especialización	Capacitación acreditada en temas relacionas a la seguridad de la información (no menor a 50 horas pedagógicas presenciales).
Experiencia	Experiencia de tres (03) años en cargos y/o funciones afines en el sector público.
Conocimiento	• Inglés. • Planificación de proyectos. • Seguridad informática.
Competencias	• Proactivo, organizado y disciplinado. • Habilidad de comunicaciones oral y escrito. • Capacidad de trabajo en equipo y bajo presión. • Capacidad analítica y lógica.
Responsabilidades generales	
• Planifica en coordinación con el líder de informática y comunicaciones para alcanzar las metas y cumplir con los objetivos de la planificación. • Impulsar planes estratégicos para aumentar la eficiencia del equipo. • Supervisa y coopera en el seguimiento de los planes de seguridad y cumplimiento de este.	

Tabla 49

El líder del área jurídica

Líder	
Nombre del cargo	Líder del área jurídica
Perfil	
Formación	Título Profesional en la facultad de derecho.
Especialización	Capacitación acreditada en temas relacionas a la seguridad de la información (no menor a 50 horas Pedagógicas presenciales).
Experiencia	Experiencia de tres (03) años en cargos y/o funciones afines en el sector público.
Conocimiento	• En creación de documentos legales. • Seguridad informática.
Competencias	• Proactivo, organizado y disciplinado. • Habilidad de comunicaciones oral y escrito. • Capacidad de trabajo en equipo y bajo presión. • Capacidad analítica y lógica.
Responsabilidades generales	• Establecer las normas del comité de gestión de seguridad de la información. • Establecer las políticas de seguridad de la información. • Aprobar políticas de seguridad de la información. • Crear nuevas políticas de seguridad que aseguren la confidencialidad, integridad y disponibilidad de la información.

Tabla 50

Líder del sistema de gestión de calidad

Líder	
Nombre del cargo	Líder del sistema de gestión de calidad
Perfil	
formación	Título profesional o técnico en la especialidad ingeniería de sistemas o computación e informática o afines.
Especialización	Capacitación acreditada en temas relacionas a la seguridad de la información (no menor a 50 horas pedagógicas presenciales).
Experiencia	Experiencia de tres (03) años en cargos y/o funciones afines en el sector público.
Conocimiento	• Inglés. • Gestión de la calidad. • Seguridad informática.
Competencias	• Proactivo, organizado y disciplinado. • Habilidad de comunicaciones oral y escrito. • Capacidad de trabajo en equipo y bajo presión. • Capacidad analítica y lógica.

Responsabilidades generales

- Supervisar que se cumplan las políticas establecidas en la organización.
- Llevar a cabo auditorías internas para la mejora constante de la seguridad de la información.
- Trabajar en conjunto con los auditores, supervisar y analizar resultados.
- Realizar reuniones de trabajo con la finalidad de revisar la calidad y eficiencia de los servicios que se ofrecen.
- Proponer cambios o ajustes en la documentación y supervisar que estos cambios se den.
- Controlar y supervisar que no esté en funcionamiento documentación obsoleta del sistema de gestión de calidad.
- Revisar y dar seguimiento al desarrollo del plan de capacitación del personal en lo relacionado con el sistema de gestión de la calidad

Tabla 51

Líder de la gestión documental

Líder	
Nombre del cargo	Líder de la gestión documental
Perfil	
Formación	Título profesional o técnico en la especialidad ingeniería de sistemas o computación e informática o afines.
Especialización	En gestión de la comunicación.
Experiencia	Experiencia de tres (03) años en cargos y/o funciones afines en el sector público.
Conocimiento	• Inglés. • Gestión de la comunicación. • Seguridad informática.
Competencias	• Proactivo, organizado y disciplinado. • Habilidad de comunicaciones oral y escrito. • Capacidad de trabajo en equipo y bajo presión. • Capacidad analítica y lógica. • Empatía.
Responsabilidades generales	
• Coordinar y supervisar las actividades técnicas y administrativas de las unidades de Archivo de la institución. • Llevar el control, con evidencias, del desempeño del personal bajo su responsabilidad.	

- Elaborar Informes de sus actividades en proceso o concluidas.
- Verificar y autorizar la digitalización de documentos.
- Verificar la aplicación de las normas y políticas en función a la documentación de la organización.
- Documentar los procesos de gestión de seguridad de la información.
- Exigir documentación de todo lo establecido y acordado por el comité de gestión de seguridad de la información.

Tabla 52

Líder de control interno

Líder	
Nombre del cargo	Líder de control interno
Perfil	
formación	Título profesional o técnico en la especialidad ingeniería de sistemas o computación e Informática o afines.
Especialización	En gestión de la comunicación.
Experiencia	Experiencia de tres (03) años en cargos y/o Funciones afines en el sector público.
Conocimiento	• Inglés. • En monitoreo y control de planes de seguridad de la información.
Competencias	• Proactivo, organizado y disciplinado. • Habilidad de comunicaciones oral y escrito. • Capacidad de trabajo en equipo y bajo presión. • Capacidad analítica y lógica.
Responsabilidades generales	• Evaluar la ejecución y desarrollo del control en la organización. • Liderar las auditorias de control interno para validar la aplicación del sistema de seguridad de la información. • Coordinar la relación con los organismos de control externo, facilitando los requerimientos de información y la coordinación en los informes de la entidad. • Liderar el fomento de la cultura del control en la institución, que contribuya al mejoramiento continuo en el cumplimiento de la misión institucional. • Velar por el cumplimiento de las leyes, normas, políticas, procedimientos, planes, programas, proyectos y metas de organización y recomendar los ajustes necesarios. • Comunicar a los directivos las conclusiones de auditoría y formular recomendaciones tendientes a corregir situaciones insatisfactorias.

3.5.4. Concientización

Acuerdo de concientización y confidencialidad de información (ANEXO 5), véase en el apartado de anexo.

Este documento contiene, de forma general, un conjunto de cláusulas que recogen la descripción de la obligación de secreto y de sus excepciones (condiciones en las que se produce la divulgación de la información y condiciones para que esta permanezca confidencial), las consecuencias de que esto se incumpla, y las obligaciones y responsabilidades que las partes suscriben en el marco de este acuerdo.

El acuerdo deberá contener (i) descripción de la información que deberá ser considerada como confidencial; (ii) razones por las cuales la información deja de ser confidencial; (iii) circunstancias en las que la información confidencial puede ser divulgada a terceros, como cuando esta se vuelve pública, o por requerimiento judicial; y (iv) cláusulas generales, como término de duración, ley aplicable, método de solución de controversias, cláusula penal, entre otros.

3.5.5. Comunicaciones

3.5.5.1. Plan de comunicaciones

Tabla 53

Control del documento

Documentos	**Información**
Documento identificación	Implementación de la NTP/ISO 27001.
Dueño del documento	Líder de área de informática comunicaciones
Fecha de la edición	02/enero/2019
Última fecha de modificación	14/enero/2019
Nombre del archivo	Implementación de la NTP/ISO 27001 para departamento de telemática de la OEE.

Tabla 54

Aprobaciones al documento

Papel	Nombre	Firma	Fecha
Patrocinador del proyecto / cliente	Telemática.		02/01/19
Comité directivo	Comité de gestión de seguridad de la información		02/01/19
Gerente del proyecto	Grl. Jefe de la OEE		02/01/19
Miembro del equipo de trabajo	Líder de área de informática y comunicaciones.		02/01/19
Representante de comunidad de usuarios	Departamento de R.R.H.H.		02/01/19
Organizaciones externas públicas y privadas	Proveedores		02/01/19

3.5.5.1.1. Requerimientos de comunicaciones

El primer paso en la elaboración de un plan de comunicaciones es identificar los receptores de información y de comunicaciones del proyecto. Luego se identifican las necesidades de comunicación del proyecto, junto con las frecuencias, los medios a emplearse y los tipos de comunicación (formales, verbales, informales) y los formatos que se usarán. De este modo, los participantes del proyecto sabrán cómo se llevarán a cabo las comunicaciones del proyecto.

Definición de comunicación

Las comunicaciones se pueden producir de diferente manera; entre otras:

- Documentos del proyecto (ej. planes, cronogramas)

- Informes de avance
- Reuniones formales de discusión de avances y problemas
- Reuniones de definición de procesos, procedimientos, estándares, criterios, etc.
- Reuniones de toma de decisiones
- Reuniones de revisiones (ej. Calidad de procesos, calidad de entregables)
- Comunicados públicos

3.5.5.1.2. Listado de receptores de comunicaciones

A continuación, se presenta una lista de ejemplo de posibles stakeholders o receptores de comunicaciones:

- Patrocinador del proyecto / cliente.
- Comité directivo.
- Gerente del proyecto.
- Miembro del equipo de trabajo.
- Comunidad de usuarios.
- Proveedores y contratistas.
- Organizaciones externas públicas y privadas.

3.5.5.1.3. Identificación de los requerimientos de comunicaciones

Identifique los requerimientos de comunicaciones probables para cada receptor completando la tabla siguiente:

Tabla 55

Requerimientos de comunicación

Receptores de la información	**Necesidad del proyecto**	**Frecuencia**	**Medios para emplear**	**Tipo de comunicación**
Patrocinador del proyecto / cliente	Implementación	2 – 4 veces cada bimestre	Documentos del proyecto	Formal escrita

Comité directivo	Informativo	2 – 4 veces cada bimestre	Documentos del proyecto e informes de avance	Formal escrita
Receptores de la información	**Necesidad del proyecto**	**Frecuencia**	**Medios para emplear**	**Tipo de comunicación**
Gerente del Proyecto	De Responsabilidad	4 – 8 veces cada bimestre	Reuniones formales de discusión de avances y problemas	Formal escrita Formal verbal
Miembro del equipo de trabajo	Distribución de actividades	Diario durante la duración del proyecto	Reuniones formales de discusión de avances y problemas, y reuniones de toma de decisiones.	Informal escrita Informal verbal
Comunidad de usuarios	Beneficios	Presentación final de aprobación del proyecto para llevarlo a la implementación.	Comunicados públicos	Informal escrita
Organizaciones externas públicas y privadas	Implementación y Apoyo	Ultimas semanas después de la aprobación.	Documentos del proyecto e informes de avance y reuniones de definición de procesos, procedimientos, estándares, criterios, etc.	Formal escrita Formal verbal

3.5.5.1.4. Plan de comunicaciones

Estas actividades son un grupo de tareas que se deben llevar a cabo para diseminar la información entre los receptores en forma “regular” o periódica.

Tabla 56

Plan de comunicaciones

Actividades de comunicaciones				
ID Actividad	Información (qué)	Receptores (quiénes)	Rangos de tiempo (cuando)	Métodos (cómo)
PT_PY	Información desde la planeación hasta el alcance del proyecto.	Patrocinador del proyecto / cliente	2 – 4 veces cada bimestre	Documentos del Proyecto
CD	La información que respecta a la culminación del proyecto, situaciones de error y solución y alcance del proyecto.	Comité directivo	2 – 4 veces cada bimestre	Documentos del Proyecto e Informes de Avance
G_PY	Problemáticas en el desarrollo del proyecto, necesidades, alcance y viabilidad.	Gerente del Proyecto	4 – 8 veces cada bimestre	Reuniones formales de discusión de avances y problemas
WK	Plan de trabajo, distribución de las actividades de desarrollo, toma de decisiones, soluciones y propuestas.	Miembro del equipo de trabajo	Diario durante la duración del proyecto	Reuniones formales de discusión de avances y problemas, y reuniones de toma de decisiones.
USR	Informar al posible beneficiario o usuario de la implementación del proyecto.	Comunidad de usuarios	Presentación final de aprobación del proyecto para llevarlo a la implementación.	Comunicados Públicos

ORG	Información desde la planeación hasta el alcance del proyecto y la viabilidad del mismo.	Organizaciones externas públicas y privadas	Ultimas semanas después de la aprobación.	Documentos del Proyecto e Informes de Avance y Reuniones de definición de procesos, procedimientos, estándares, criterios, etc.

3.5.5.1.5. Proceso de comunicaciones

3.5.5.1.5.1. Propósito

Informar a cada partícipe, responsable y persona que mantenga algún beneficio de la implementación de la NTP/ISO 27001 de la Información con la intención de recibir sea el caso las autorizaciones necesarias, e informar las responsabilidades y actividades que se llevan dentro del desarrollo del proyecto, para asegurar las relaciones mantenidas dentro de éste.

3.5.5.1.5.2. Actividades

Proporcione una representación diagramática de las actividades de comunicaciones que se llevarán a cabo para satisfacer los requerimientos de comunicaciones de los receptores dentro del proyecto.

3.5.5.1.5.3. Roles y responsabilidades

Defina los roles y las responsabilidades de todos los recursos implicados con el proceso de comunicaciones dentro del proyecto.

Tabla 57

Roles y responsabilidades

Papel	Nombre	Firma	Responsabilidades
Jefe del Depto. de sistemas	--		Entregables
Project manager del proyecto	--		Aprueba el entregable
Analista del proyecto	--		Revisa
Programadores del proyecto	--		Participa
Tester del proyecto	--		Participa
Proveedor de suministros electrónicos	--		Participa

CAPÍTULO IV
ANÁLISIS DE RESULTADOS Y CONTRASTACIÓN DE LA HIPÓTESIS

4.1. Población y muestra

4.1.1. Población

Todos los procesos de seguridad de la información de la oficina de economía del ejército del Perú.

N = indeterminado.

4.1.2. Muestra

Pande (2004), refiere que “30 es un valor indicado, estándar y que es utilizado en distintos procesos de investigación” (p.23). Para esta investigación, se tomó una muestra de 30 casos de procesos de seguridad de la oficina de economía del ejército. A comparación de distintos procedimientos estadísticos de modo aleatoria que existen para evaluar la dimensión de la muestra sabiendo o no el valor de la población.

n = 30 casos de proceso de seguridad de información.

4.2. Análisis e interpretación de resultados

4.2.1. Resultados genéricos

Tabla 58

Estructura de la NTP/ISO 27001:2014

Fases	Nombre	Actividades principales	Entregables
0	Estudio de factibilidad	Realizar los tipos de estudios existentes de factibilidad.	Factibilidad técnica Factibilidad operativa Factibilidad económica
I	Contexto de la organización	Comprender la organización y su contexto. Comprender las necesidades y expectativas de las partes interesadas.	Misión, visión de la empresa y procesos de negocio Cartera de negocio Diagrama de contexto

		Determinar el alcancé del sistema de gestión de seguridad de la información.	Gestión de alcance
			Lista de stakeholder
		Liderazgo y compromiso.	Organigrama de comité de gestión
II	Liderazgo	Roles, responsabilidades y autoridades organizacionales.	Resolución de creación del comité de gestión de seguridad y hoja de funciones
		Política.	Políticas institucionales
			Políticas seguridad de información
III	Planificación	Acciones para tratar los riesgos y las oportunidades.	Gestión de riesgos
		Objetivos de seguridad de la información y planificación para conseguirlos.	
		Recursos.	Lista de activos.
			Gestión de recursos.
IV	Soporte	Competencias.	Gestión de competencias.
		Concientización.	Acuerdo de concientización y confiabilidad.
		Comunicación.	Gestión de comunicaciones

4.2.2. Resultados específicos

Tabla 59

Resultados de pre-prueba y post-prueba para KPIs

Nº	KPI1: Tiempo para reportar incidencias(minutos)		KPI2: Porcentaje de disponibilidad de la información dentro de la institución (%)		KPI3: Porcentaje de integridad de la información dentro de la institución (%)		KPI4: Tiempo para dar respuesta a una incidencia(minutos)		KPI5: Nivel de satisfacción del Cliente	
	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba	Pre-prueba	Post-prueba
1	33	13	30	75	53	99	25	10	1	3
2	38	5	50	68	32	89	23	5	1	3
3	33	11	25	80	63	99	29	7	1	3
4	33	7	30	85	62	99	30	9	1	4
5	38	9	45	90	67	81	29	5	1	3
6	45	5	22	95	35	81	22	13	1	4
7	33	15	23	80	52	82	22	12	1	3
8	45	6	34	75	36	88	26	15	1	3
9	37	11	36	69	50	84	27	9	2	4
10	31	13	38	82	69	82	21	6	2	3
11	43	11	45	79	64	84	22	8	1	4
12	44	11	25	76	52	93	27	10	2	3
13	32	10	24	79	44	87	23	9	1	4
14	31	6	20	84	50	87	29	8	1	2
15	37	9	18	84	45	96	29	15	2	4
16	42	8	24	81	36	90	28	5	1	2
17	42	12	19	72	67	98	25	8	1	4
18	30	14	35	70	49	85	23	11	1	4
19	43	15	41	60	37	86	22	8	1	3
20	40	9	47	62	54	86	28	7	1	3
21	32	14	50	80	43	92	20	9	1	3
22	44	9	42	86	39	99	27	11	1	4
23	45	15	35	87	30	99	27	9	2	2
24	31	7	20	78	37	83	25	7	1	3
25	33	9	24	75	48	88	24	11	1	3
26	34	14	28	80	34	95	23	9	1	3
27	42	15	19	80	65	93	27	6	1	2
28	43	15	18	81	43	83	21	6	1	4
29	35	9	24	83	43	86	29	9	1	4
30	33	11	26	82	35	96	21	10	1	2

4.2.3. Análisis e interpretación de resultados

Tabla 60

Medias de los KPIs para la pre-prueba y post- prueba

Indicadores	Pre Prueba (media)	Post Prueba (media)	Comentario
KPI 1: Tiempo para reportar una incidencia de seguridad de la información (minutos).	37,4	10,6	-
KPI 2: Porcentaje de disponibilidad de la información dentro de la institución (Porcentaje).	30,6	78,6	-
KPI 3: Porcentaje de la integridad de la información dentro de la institución (Porcentaje).	47,8	89,7	-
KPI 4: Tiempo para dar respuesta a una incidencia de seguridad de la información (minutos).	25,1	8,9	-
KPI 5: Nivel de Satisfacción del Cliente.	-	-	No contrastado. Indicador cualitativo

Nota: * Fórmula para hallar el %: (procesos sin observaciones/procesos realizados) *100 = % de exactitud.

Interpretación

Según la tabla 54 se puede observar que la media del tiempo para reportar una incidencia de seguridad (KPI1) ha disminuido después de la implementación de la NTP/ISO27001, a su vez el porcentaje promedio de disponibilidad de la información dentro de la institución ha aumentado después de la implementación de la NTP/ISO27001, como también aumento el porcentaje medio de la integridad de la información dentro de la institución y el tiempo promedio para dar respuesta a una incidencia de seguridad de la información. A continuación, se realiza un análisis detallado de los indicadores presentados.

A. Indicador 1: Tiempo para reportar una incidencia de seguridad de la información: KPI_1

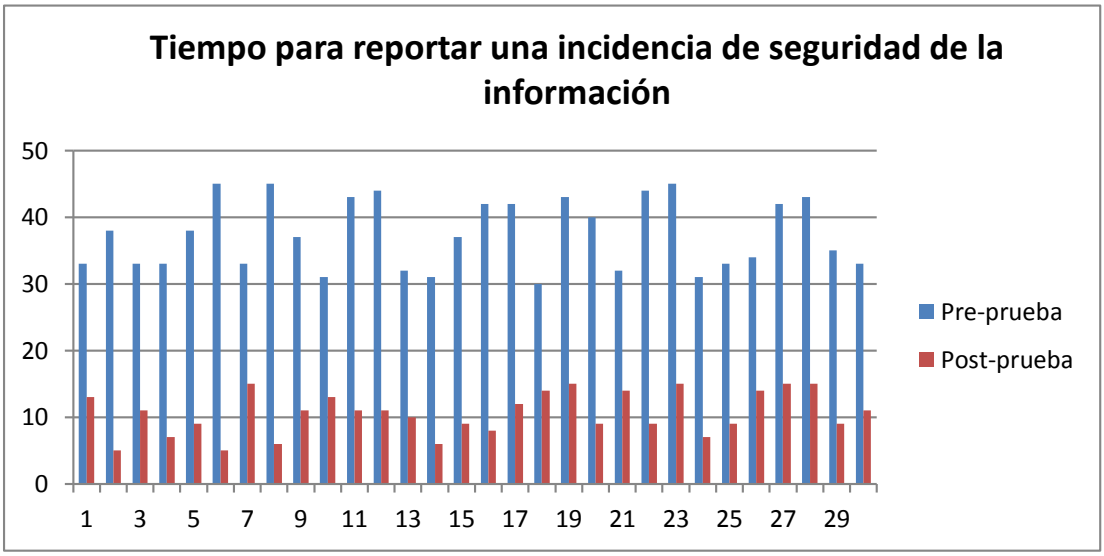


Figura 20. Resultados de Pre-Prueba y Post-Prueba para el KPI_1.

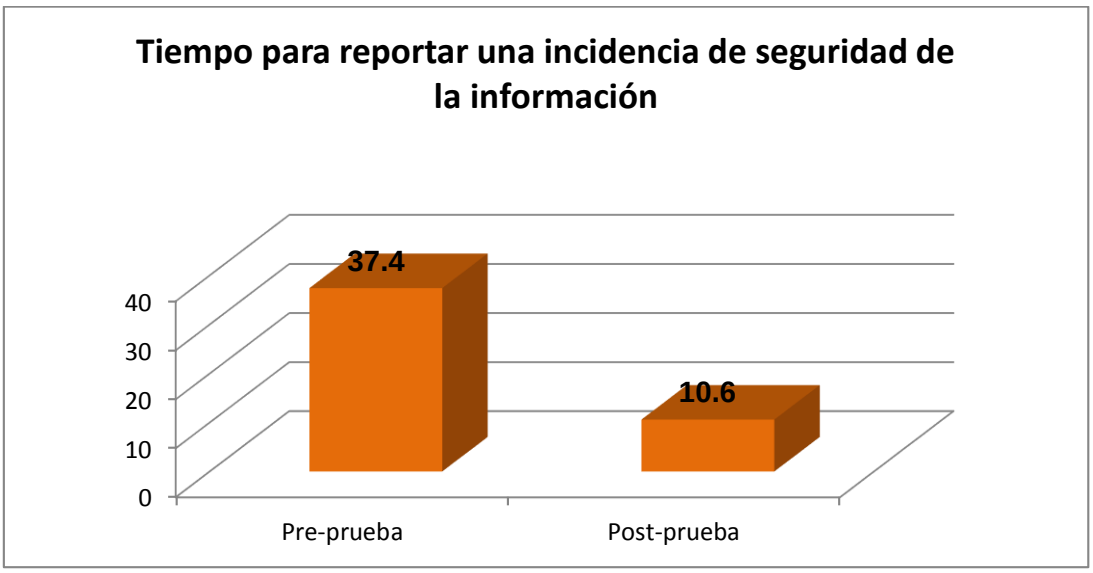


Figura 21. Promedio de resultados de Pre-Prueba y Post-Prueba para el KPI_1.

Interpretación

En la figura 21 podemos observar que la media del tiempo para reportar una incidencia de seguridad de la información es del 37.4 minutos antes de implementar la NTP/ISO 207001, luego de la implementación el tiempo promedio fue de 10.6 minutos por lo tanto podemos inferir que después de la implementación el tiempo se reduce en un 72%.

B. Indicador 2: Porcentaje de disponibilidad de la información contenida en la institución: KPI_2

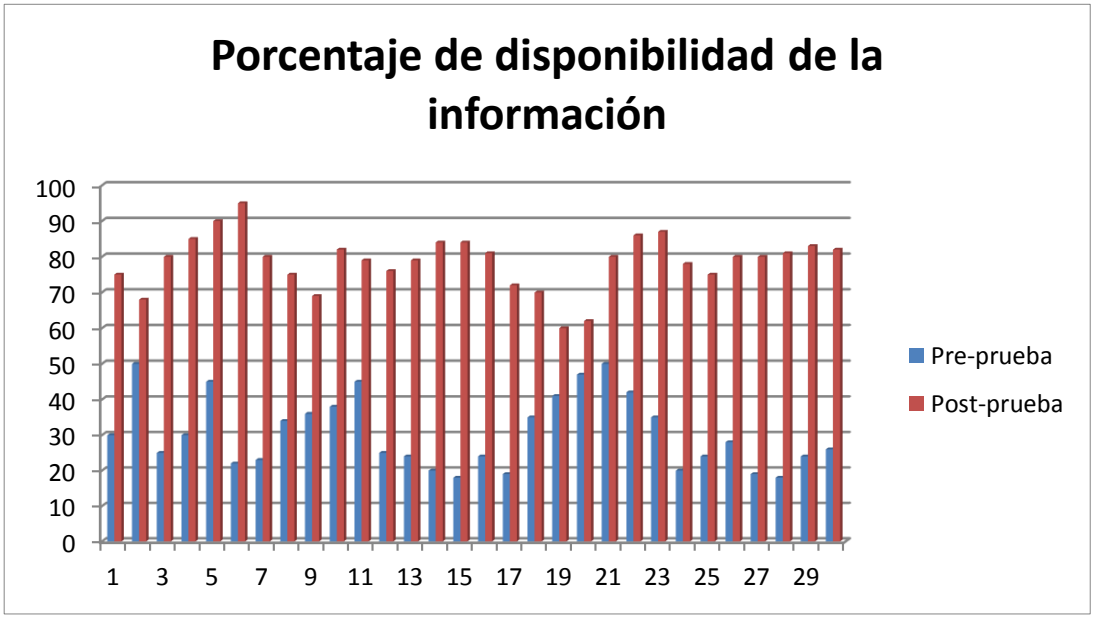


Figura 22. Resultados de Pre-Prueba y Post-Prueba para el KPI_2.

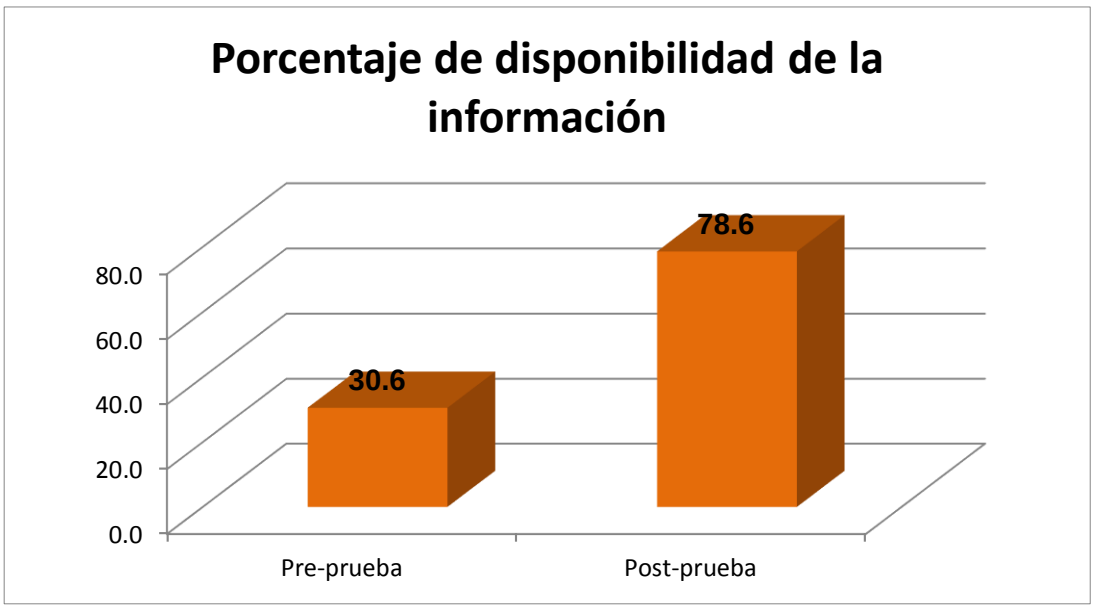


Figura 23. Promedio de resultados de Pre-Prueba y Post-Prueba para el KPI_2.

Interpretación

En la figura 23 podemos ver que el porcentaje promedio de la disponibilidad de la información antes de la implementación de la NTP/ISO27001 era de 30.6 y después de la implementación la disponibilidad de la información fue un 78.6.

C. Indicador 3: Porcentaje de confiabilidad de la información dentro de la institución: KPI_3

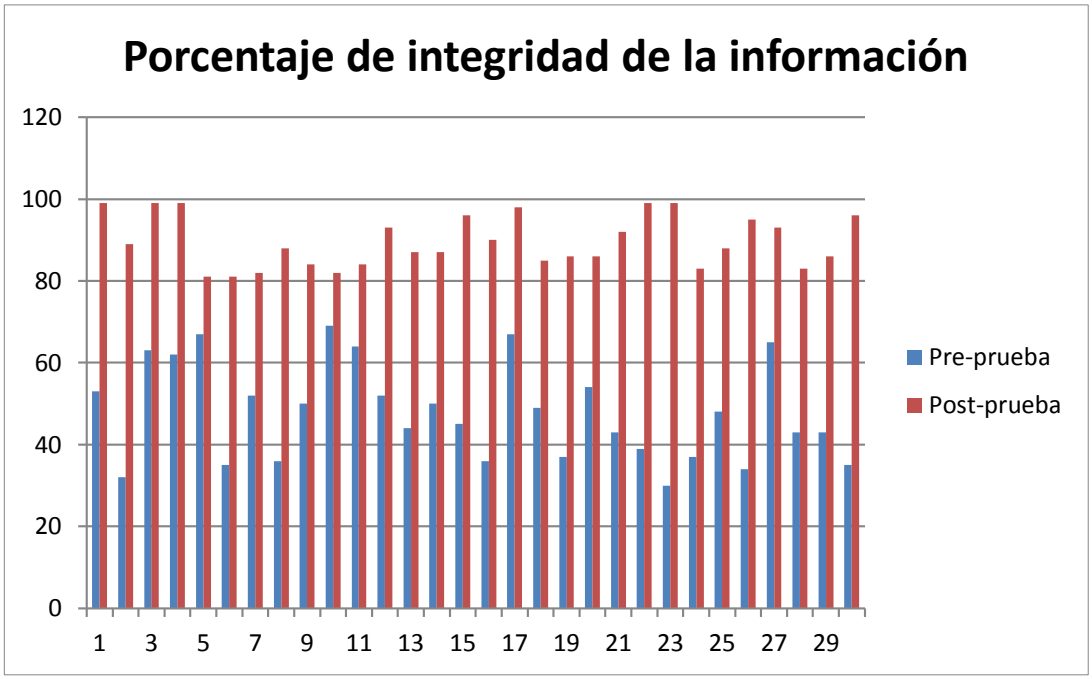


Figura 24. Resultados de Pre-Prueba y Post-Prueba para el KP_3.

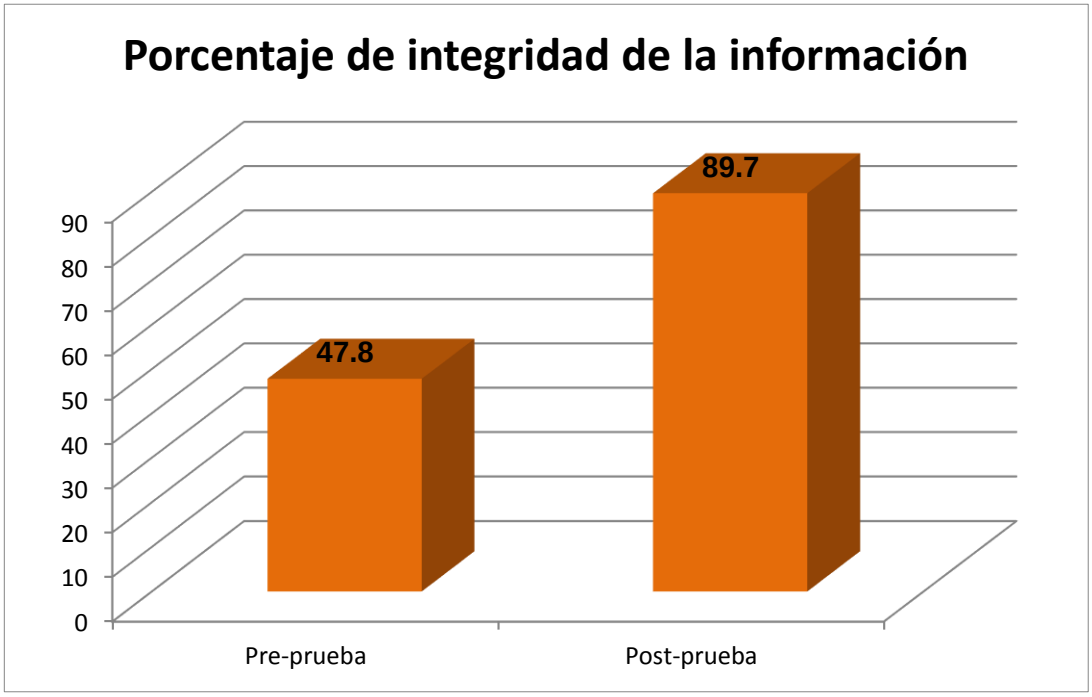


Figura 25. Promedio de resultados de Pre-Prueba y Post-Prueba para el KPI_3.

Interpretación

En la figura 24 podemos observar que después de la implementación de la NTP/ISO 27001 el porcentaje de la integridad de la información aumentó con respecto a las pruebas realizadas antes de la implementación y en la figura 25 podemos ver que el porcentaje promedio en la Pre-Prueba fue de 47.8% y en la post prueba fue de 89.7%, por lo que podemos determinar que después de la implementación, el porcentaje de integridad de la información aumentó considerablemente.

D. Indicador 4: Tiempo para dar respuesta a una incidencia de seguridad de la información: KPI_4

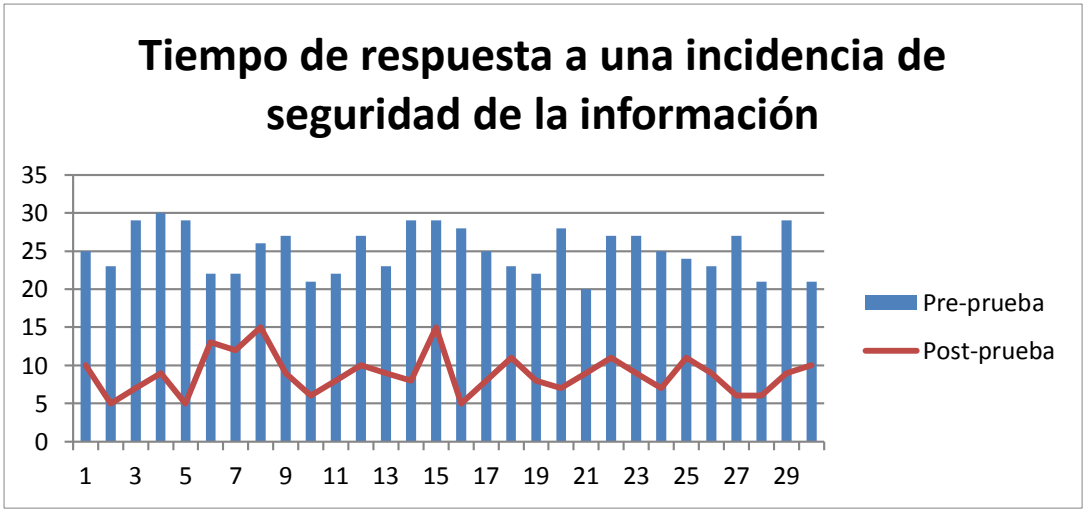


Figura 26. Resultados de Pre-Prueba y Post-Prueba para el KP_4.

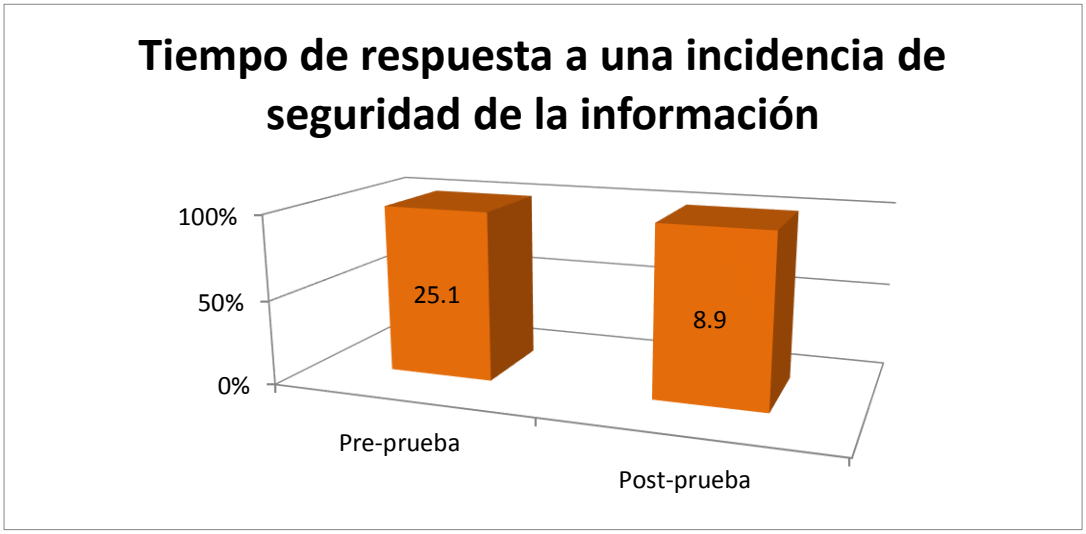


Figura 27. Promedio de resultados de Pre-Prueba y Post-Prueba para el KPI_4.

Interpretación

En la figura 26 podemos observar como el tiempo de respuesta a una incidencia de seguridad de la información se llegó a reducir en todos los casos, por lo que si observamos la figura 27 se muestra que el tiempo promedio antes de la implementación de la NTP/ISO27001 fue de 25.1 minutos y después de la implementación el tiempo fue 8.9 minutos.

E. Indicador 5: Nivel de satisfacción del usuario: KPI_4

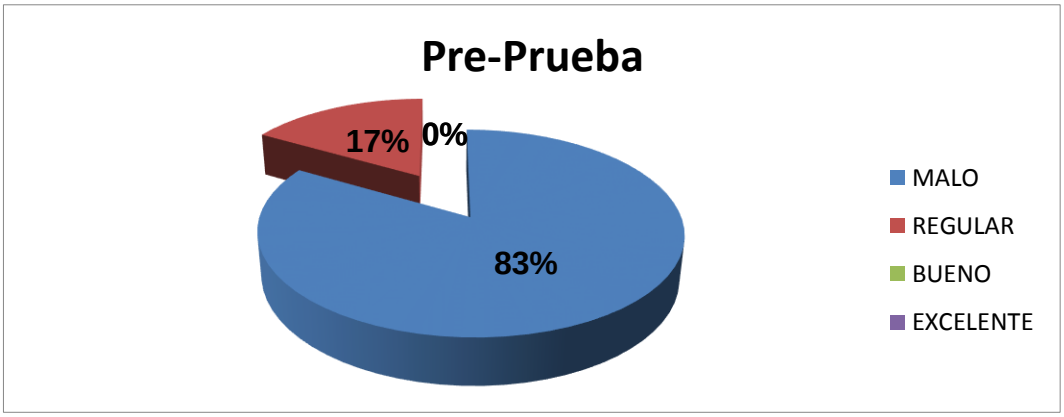


Figura 28. Gráfico de resultados de la Pre-Prueba - KPI_5

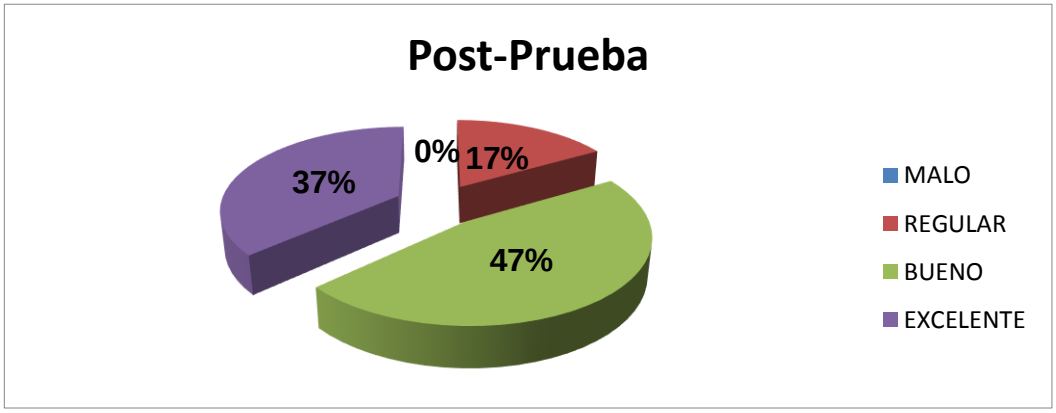


Figura 29. Gráfico de resultados de la Post-Prueba - KPI_5.

Interpretación

En la figura 28 se muestra como el nivel de satisfacción antes de la implementación de la NTP/ISO27001 no se mostraba el tipo de nivel bueno y excelente y en cambio después de la implementación el nivel de satisfacción aumento y ya se muestra el nivel bueno y excelente, reduciendo el nivel malo a un 0%. Y esto se puede aprecia en la figura 30.

4.3. Nivel de confianza y grado de significancia

Para la prueba de hipótesis para que los datos recolectados sean evaluados, se utilizó los siguientes parámetros:

El nivel de confianza será del 95%

El nivel de significancia será del 5%

4.4. Contrastación de la hipótesis

A. Contrastación para el indicador 1: Tiempo para reportar una incidencia de seguridad de la información.

a. Prueba de normalidad

Con el objetivo de seleccionar la prueba de hipótesis de investigación; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del tiempo para reportar una incidencia de seguridad de la información contaban con una distribución normal; para ello se aplicó la prueba de Shapiro-Wilk para ambos indicadores debido a que la muestra es menor a 50.

Ho= los datos tienen un comportamiento normal.

≥ P=0.05

Ha= Los datos no tienen un comportamiento normal.

< P=0.05

Tabla 61

Prueba de normalidad del indicador 1

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-prueba	Tiempo para reportar una incidencia de seguridad de la información	,881	30	,003
Post-prueba	Tiempo para reportar una incidencia de seguridad de la información	,931	30	,052

Los resultados de la prueba indican que el Sig. De la muestra del tiempo para reportar una incidencia de seguridad de la información antes fue de ,003 y de ,052 después cuyo valor es menor que 0.05 en la Pre-Prueba, pero mayor a 0.05 en la Post-Prueba entonces se rechaza la hipótesis nula, por lo que indica que el tiempo para reportar una incidencia de seguridad de la información no se distribuye normalmente en la Pre-Prueba, pero si se distribuye normalmente en la post

prueba. Lo que confirma la distribución no normal de los datos de la muestra, por lo que se usará: w – Wilcoxon.

Hipótesis alterna

La implementación de la NTP/ISO 27001 reduce el tiempo para reportar incidencias de seguridad de la información dentro de la institución.

Hipótesis nula

La implementación de la NTP/ISO 27001 aumenta el tiempo para reportar incidencias de seguridad de la información dentro de la institución.

Tabla 62

Prueba de Wilcoxon al indicador 1

	Tiempo para reportar una incidencia de seguridad de la información (Post-Prueba) - Tiempo para reportar una incidencia de seguridad de la información (Pre-Prueba)
Z	-4,785[b]
Sig. asintótica (bilateral)	,000

Los resultados de la prueba w de Wilcoxon, aplicada porque los datos no se distribuyen normalmente; demuestran que, como el resultado de la probabilidad tiende a cero en relación con la probabilidad asumida de 0.05, se rechaza la hipótesis nula, porque el tiempo para reportar una incidencia de seguridad de la información se reduce después de la implementación de la NTP/ISO 27001.

B. Contrastación para el indicador 2: Porcentaje de disponibilidad de la información dentro de la institución.

b. Prueba de normalidad

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del Porcentaje de disponibilidad de la información dentro de la institución contaban con

una distribución normal; para ello se aplicó la prueba de Shapiro-Wilk para ambos indicadores debido a que la muestra es menor a 50.

Ho= los datos tienen un comportamiento normal.

≥ P=0.05

Ha= Los datos no tienen un comportamiento normal.

< P=0.05

Tabla 63

Prueba de normalidad del indicador 2

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-Prueba	Porcentaje de disponibilidad de la información dentro de la institución	,907	30	,013
Post-Prueba	Porcentaje de disponibilidad de la información dentro de la institución	,959	30	,300

Los resultados de la prueba indican que el Sig. De la muestra del porcentaje de disponibilidad de la información dentro de la institución antes fue de ,013 y de ,300 después cuyo valor es menor que 0.05 en la Pre-Prueba, pero mayor a 0.05 en la post prueba entonces se rechaza la hipótesis nula, por lo que indica que el porcentaje de disponibilidad de la información dentro de la institución no se distribuye normalmente en la pre prueba, pero si se distribuye normalmente en la post prueba. Lo que confirma la distribución no normal de los datos de la muestra, por lo que se usará: w – Wilcoxon.

Hipótesis alterna

La implementación de la NTP/ISO 27001 incrementa el porcentaje de disponibilidad de la información dentro de la institución.

Hipótesis nula

La implementación de la NTP/ISO 27001 reduce el porcentaje de disponibilidad de la información dentro de la institución.

Tabla 64

Prueba de Wilcoxon al indicador 2

	Porcentaje de disponibilidad de la información dentro de la institución (Post-Prueba) - Porcentaje de disponibilidad de la información dentro de la institución (Pre-Prueba)
Z	-4,783[b]
Sig. asintótica (bilateral)	,000

Los resultados de la prueba w de Wilcoxon, aplicada porque los datos no se distribuyen normalmente; demuestran que, como el resultado de la probabilidad tiende a cero en relación con la probabilidad asumida de 0.05, se rechaza la hipótesis nula, porque el porcentaje de disponibilidad de la información dentro de la institución aumentó considerablemente después de la implementación de la NTP/ISO 27001.

C. Contrastación para el indicador 3: Porcentaje de integridad de la información dentro de la institución.

c. Prueba de normalidad

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del Porcentaje de integridad de la información dentro de la institución contaban con una distribución normal; para ello se aplicó la prueba de Shapiro-Wilk para ambos indicadores debido a que la muestra es menor a 50.

Ho= los datos tienen un comportamiento normal.

≥ P=0.05

Ha= Los datos no tienen un comportamiento normal.

< P=0.05

Tabla 65

Prueba de normalidad del indicador 3

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-Prueba	Porcentaje de integridad de la información dentro de la institución	,932	30	,054
Post-Prueba	Porcentaje de integridad de la información dentro de la institución	,903	30	,010

Los resultados de la prueba indican que el Sig. De la muestra del porcentaje de integridad de la información dentro de la institución antes fue de ,054 y de ,010 después; el valor es mayor que 0.05 en la Pre-Prueba, pero es menor que 0.05 en la post prueba entonces se rechaza la hipótesis nula, por lo que indica que el porcentaje de integridad de la información dentro de la institución no se distribuye normalmente en la post prueba, pero si en la Pre-Prueba. Lo que confirma la distribución no normal de los datos de la muestra, por lo que se usará: w – Wilcoxon.

Hipótesis alterna

La implementación de la NTP/ISO 27001 incrementa el porcentaje de integridad de la información dentro de la institución.

Hipótesis nula

La implementación de la NTP/ISO 27001 reduce el porcentaje de integridad de la información dentro de la institución.

Tabla 66

Prueba de Wilcoxon al indicador 3

	Porcentaje de integridad de la información dentro de la institución (Post-Prueba) - Porcentaje de integridad de la información dentro de la institución (Pre-Prueba)
Z	-4,783[b]
Sig. asintótica (bilateral)	,000

Los resultados de la prueba w de Wilcoxon, aplicada porque los datos no se distribuyen normalmente; demuestran que, como el resultado de la probabilidad tiende a cero en relación con la probabilidad asumida de 0.05, se rechaza la hipótesis nula, porque el porcentaje de integridad de la información dentro de la institución aumentó considerablemente después de la implementación de la NTP/ISO 27001.

D. Contrastación para el indicador 4: Tiempo para dar respuesta a una incidencia de seguridad de la información.

d. Prueba de normalidad

Con el objetivo de seleccionar la prueba de hipótesis; los datos fueron sometidos a la comprobación de su distribución, específicamente si los datos del tiempo para dar respuesta a una incidencia de seguridad de la información contaban con una distribución normal; para ello se aplicó la prueba de Shapiro-Wilk para ambos indicadores debido a que la muestra es menor a 50.

Ho= los datos tienen un comportamiento normal.
≥ P=0.05

Ha= Los datos no tienen un comportamiento normal.
< P=0.05

Tabla 67

Prueba de normalidad del indicador 4

	Prueba	Shapiro-Wilk		
		Estadístico	gl	Sig.
Pre-Prueba	Tiempo para dar respuesta a una incidencia	,923	30	,033
Post-Prueba	Tiempo para dar respuesta a una incidencia	,943	30	,113

Los resultados de la prueba indican que el Sig. De la muestra del tiempo para da respuesta a una incidencia de seguridad de la información antes fue de ,033 y de ,113 después; el valor es menor que 0.05 en la Pre-Prueba, pero es mayor

que 0.05 en la Post-Prueba entonces se rechaza la hipótesis nula, por lo que indica que el tiempo para dar respuesta a una incidencia de seguridad de la información no se distribuye normalmente en la pre prueba, pero si en la post prueba. Lo que confirma la distribución no normal de los datos de la muestra, por lo que se usará: w – Wilcoxon.

Hipótesis alterna

La implementación de la NTP/ISO 27001 reduce el tiempo para dar respuesta a una incidencia de seguridad de la información.

Hipótesis nula

La implementación de la NTP/ISO 27001 aumenta el tiempo para dar respuesta a una incidencia de seguridad de la información.

Tabla 68

Prueba de Wilcoxon al indicador 4

	Tiempo para dar respuesta a una incidencia (Post-Prueba) - Tiempo para dar respuesta a una incidencia (Pre-Prueba)
Z	-4,788[b]
Sig. asintótica (bilateral)	,000

Los resultados de la prueba w de Wilcoxon, aplicada porque los datos no se distribuyen normalmente; demuestran que, como el resultado de la probabilidad tiende a cero con relación a la probabilidad asumida de 0.05, se rechaza la hipótesis nula, porque el tiempo para dar respuesta a una incidencia de seguridad se redujo considerablemente después de la implementación de la NTP/ISO 27001.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

a) La primera conclusión tiene que ver con el tiempo para reportar una incidencia de seguridad de la información, el tiempo promedio antes de la implementación de la NTP/ISO 27001 era de 37.4 minutos y después de la implementación el tiempo promedio fue de 6.4 por lo cual se puede deducir que se redujo el tiempo en un 72%. (ver figura 22)

b) Se observa que el porcentaje de disponibilidad de la información dentro de la institución ha aumentado con respecto al porcentaje inicial de un 30.6 por ciento a un 78.6 por ciento, con la utilización de un procedimiento que responde al riesgo de disponibilidad de la información que gracias a la implementación de la NTP/ISO 27001.

c) Se observa que el porcentaje de confiablidad de la información dentro de la institución ha aumentado con respecto al porcentaje inicial de 47.8 por ciento a un 89.7 por ciento, con la implementación de la NTP/ISO 27001.

d) Se observa que el tiempo para dar respuesta a una incidencia de seguridad de la información se redujo de 25 minutos a 9 minutos. Logrando una efectiva atención de los usuarios de la institución y así puedan continuar con las labores diarias, esto gracias a la utilización de un procedimiento que responde al evento de un riesgo de seguridad de la información.

e) Se observa que el nivel de satisfacción del cliente aumentó considerablemente debido a que después de implementar la NTP/ISO 27001, los usuarios no presentaron un nivel de satisfacción valorada como “malo” y muy por el contrario los usuarios mostraban una satisfacción valorada como “excelente”.

5.2. Recomendaciones

a) Se recomienda que para un análisis minucioso de los riesgos se puede hacer uso de la metodología Magerit en su última versión.

b) Se aconseja que en las próximas investigaciones se debe implementar la norma ISO 27032 la cual tiene un enfoque de seguridad en los intercambios de información dentro de la red, con este estándar se busca detectar, monitorear y protegerse de los ataques de ingeniería social, hackers, spyware, malware y otros tipos de software no deseados.

c) Se aconseja que la institución direccione un presupuesto para capacitaciones o talleres de concientización sobre seguridad de la información.

d) Se aconseja que al implementar la NTP/ISO 27001 en la institución esté de la mano con las modificaciones o cambios que sufre la norma técnica peruana al transcurrir de los años.

e) Se recomienda mantener un monitoreo periódico ante posibles “nuevos” riesgos sobre el manejo de la información y “nuevas” actividades dentro del departamento telemática de la oficina de economía del ejército del Perú.

REFERENCIAS BIBLIOGRÁFICAS

Blogs

Amorín, D. (2016). *Porque la información es el activo más importante de tu empresa: backup online*. [mensaje en un blog]. David Amorín. Recuperado de https://www.linkedin.com/pulse/porque-la-informaci%C3%B3n-es-el-activo-m%C3%A1s-importante-de-tu-david-amor%C3%ADn

Firma-e. (19 de febrero de 2013). *¿Qué es SGSI?*. [mensaje en un blog]. Firma-e. Recuperado de https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

Gutzmer, I. (7 de septiembre de 2017). *Equifax anuncia incidente de ciberseguridad que involucra información del consumidor*. [mensaje en un blog]. Equifax. Recuperado de https://www.equifaxsecurity2017.com/2017/09/07/equifax-announces-cybersecurity-incident-involving-consumer-information/

ISO27000.es. (s.f.-a). *¿Qué es un SGSI?*. [mensaje en un blog]. ISO27000.es. Recuperado de http://www.iso27000.es/sgsi.html

ISO27000.es. (s.f.-b). *Sistema de gestión de la seguridad de la información*. [mensaje en un blog]. ISO27000.es. Recuperado de http://www.iso27000.es/download/doc_sgsi_all.pdf

Sitio Web

Universidad Autónoma de Tamaulipas. (s.f.). *SGSI*. Tamaulipas: UAT SGSI. Recuperado de https://sgsi.uat.edu.mx/sgsi

Universidad ESAN. (3 de mayo de 2016). *¿Qué es y para qué sirve la norma iso 27001?*. Lima: Conexión ESAN. Recuperado de https://www.esan.edu.pe/apuntes-empresariales/2016/05/que-es-y-para-que-sirve-la-norma-iso-27001/

Villegas, N. y Gaviria, S. (29 de abril de 2013). *Importancia de la implementación del sgsi 27001 en la seguridad informática de ACESCO*. Bogotá: Repositorio

Institucional UMNG. Recuperado de https://repository.unimilitar.edu.co/handle/10654/3215

Tesis

Aguirre, D. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.* (Tesis de pregrado). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5677

Aguirre, J. y Aristizábal, C. (2013). *Diseño del sistema de gestión de seguridad de la información para el grupo empresarial la ofrenda* (Tesis de pregrado). Recuperado de http://repositorio.utp.edu.co/dspace/handle/11059/4117

Alcantára, J. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la Comisaria del Norte P.N.P en la ciudad de Chiclayo* (Tesis de pregrado). Recuperado de http://tesis.usat.edu.pe/handle/20.500.12423/539

Ariasca Suma, F. (2016). *Desarrollo de una propuesta de implementación de la NTP-ISO/IEC 27001:2014, sistema de gestión de seguridad de la información, para la oficina funcional de informática del gobierno regional del Cusco* (Tesis de pregrado). Recuperado de http://repositorio.unsaac.edu.pe/handle/UNSAAC/2454?show=full

Ccesa, M. (2017). *Diseño de un sistema de gestión de seguridad de la información bajo la NTP-ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga* (Tesis de pregrado). *Recuperado d*e http://repositorio.unsch.edu.pe/handle/UNSCH/1751

Condori, H. (2012). *Un modelo de evaluación de factores críticos de éxito en la implementación de la seguridad en sistemas de información para determinar su influencia en la intención del usuario* (Tesis de maestría). Recuperado de http://repositorio.concytec.gob.pe/handle/20.500.12390/173

Cueva, P. (2017). *Gestión de la historia clínica y la seguridad de la información del hospital ii Cajamarca - Essalud bajo la NTP-ISO/IEC 27001:2014* (Tesis de maestría). Recuperado de http://repositorio.upn.edu.pe/handle/11537/13676

Espinoza, H. (2013). *Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo* (Tesis de pregrado). Recuperado de http://hdl.handle.net/20.500.12404/4957

Fernández, D. y Pacheco, O. (2014). *Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001* (Tesis de pregrado). Recuperado de http://www.repositorioacademico.usmp.edu.pe/handle/usmp/1470

Guzmán, C. (2016*). Diseño de un sistema de gestión de seguridad de la información para una entidad financiera de segundo piso* (Tesis de pregrado). Recuperado de http://alejandria.poligran.edu.co/handle/10823/654

Huamán, F. (2014). *Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano* (Tesis de pregrado). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/5582

Llanos, E. (2017). *Modelo de proceso para la implementación de la norma ISO 27001 en la concesionaria Terrapuerto Trujillo S.A.* (Tesis de pregrado). Recuperado de http://repositorio.upao.edu.pe/handle/upaorep/4421

Maldonado, E. (2016). *Norma ISO 27001 para la seguridad de información del área de registros académicos del colegio Nuestra Señora del Carmen* (Tesis de pregrado). Recuperado de http://repositorio.ucv.edu.pe/handle/UCV/18463

Maya, P. (2016). *Plan de implementación del SGSI basado en la norma ISO 27001:2013* (Tesis de maestría). Recuperado de http://hdl.handle.net/10609/53466

Olaza, H. (2017). *Implementación de la NTP ISO/IEC 27001 para la seguridad de la información de en el área de configuración y activos del Ministerio de Educación – sede Centromin* (Tesis de pregrado). Recuperado de http://repositorio.ucv.edu.pe/handle/UCV/9927

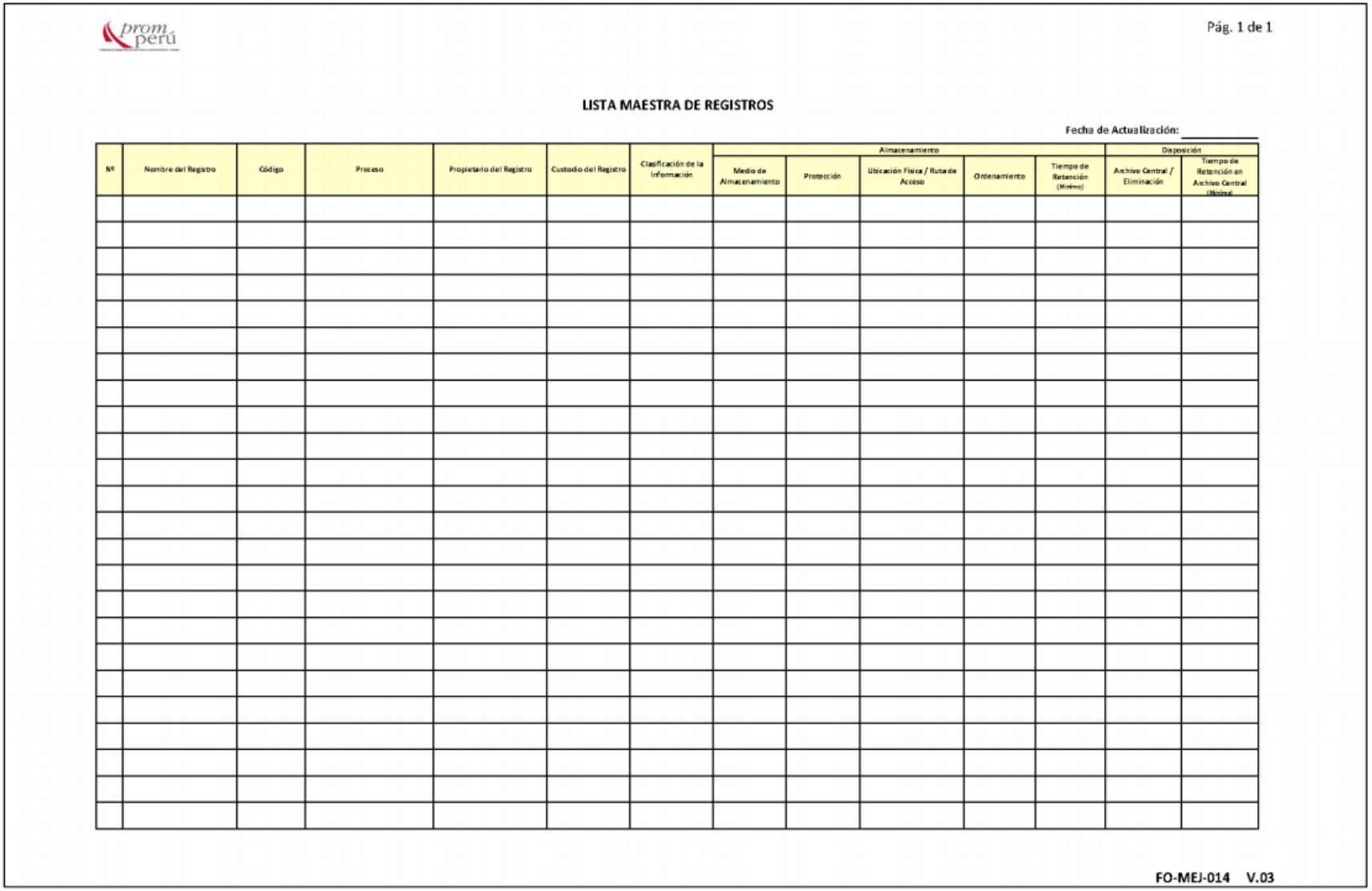
Santos, D. (2016). *Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de consultoría de software* (Tesis de pregrado). Recuperado de http://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/7616

Seclén J. (2016). *Factores que afectan la implementación del sistema de gestión de seguridad de la información en las entidades públicas peruanas de acuerdo a la NTP-ISO/IEC 27001* (Tesis de maestría). Recuperado de http://cybertesis.unmsm.edu.pe/handle/cybertesis/4884

Talavera, V. (2015). *Norma iso 27001 para la seguridad de información del área de registros académicos del colegio Nuestra Señora del Carmen* (Tesis de pregrado). Recuperado de http://repositorio.ucv.edu.pe/handle/UCV/18463?show=full

ANEXOS

ANEXO 1: Formato de lista de registros



prom perú

LISTA MAESTRA DE REGISTROS

Fecha de Actualización: _____

Nº	Nombre del Registro	Código	Proceso	Propietario del Registro	Custodio del Registro	Clasificación de la Información	Almacenamiento					Disposición	
							Medio de Almacenamiento	Protección	Ubicación Física / Ruta de Acceso	Ordenamiento	Tiempo de Retención (Mínimo)	Archivo Central / Eliminación	Tiempo de Retención en Archivo Central (Mínimo)

FO-MEJ-014 V.03

ANEXO 2: Instrucciones de llenado de formato

Instrucciones de llenado del Formato: Lista Maestra de Registros	
Campo del Formato	**Instrucción de llenado**
Nº	Colocar el número correlativo del registro.
Nombre del Registro	Colocar el nombre con el que se identifica el registro; por ejemplo "Ficha de Inscripción".
Código	Colocar el código del formato con que se identifica al registro, de acuerdo con lo señalado en "Procedimiento para el Control de Documentos"; por ejemplo "FO-DX-PRO-001". En caso el registro no provenga de un formato llenado, colocar tres guiones seguidos ("---").
Proceso	Colocar el nombre del proceso al cual pertenece el registro.
Propietario del registro	Colocar el nombre del puesto del dueño del proceso al cual pertenece el registro.
Custodio del registro	Señalar el nombre del puesto responsable de la custodia, conservación y disposición del registro.
Clasificación de la información	Señalar la categoría de información a la cual pertenece el registro, de acuerdo con la Política de Clasificación, Etiquetado y Tratamiento de la Información Administrada por PROMPERÚ. Las categorías son las siguientes: a. **Pública**: Información que puede ser conocida y utilizada sin autorización por todos los colaboradores de PROMPERÚ, o por personal externo a PROMPERÚ. b. **Uso Interno**: Información que puede ser conocida y utilizada por un grupo de colaboradores debidamente autorizados o personal externo a PROMPERÚ previo acuerdo de confidencial, para el desarrollo de sus actividades; y cuya divulgación o uso no autorizado podría ocasionar riesgos o pérdidas leves para PROMPERÚ o terceros. c. **Confidencial**: Información que puede ser conocida y utilizada por un colaborador o un grupo reducido de colaboradores, para el desarrollo de sus actividades, y cuya divulgación o uso no autorizado podría ocasionar riesgos o pérdidas significativas para PROMPERÚ o terceros.

ANEXO 3: Formato de cambios

	FORMATO PARA CONTROL A LAS SOLICITUDES DE CAMBIOS EN LAS APLICACIONES DE SOFTWARE	Código: EJEMPLO
		Versión: 01
		Fecha de Elaboración: 31/05/2016
		Vigente Desde: 24/09/2016

Dependencia:	Fecha de Aprobación:
Nombre de la aplicación:	
Descripción del desarrollo:	
Base de datos y servidor afectados:	
Tablas afectadas :	
Procedimientos o archivos afectados:	
Desarrollado por:	

Firma de aprobación del usuario que recibe: _____

ANEXO 4: Resolución de creación del comité y hoja de funciones

PERÚ	Ministerio de Defensa	Ejército del Perú	NO OFICIAL

"Año del Buen Servicio al Ciudadano"

RESOLUCIÓN PARA LA CONFORMACIÓN DEL COMITÉ DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA EL DEPARTAMENTO DE TELEMÁTICA DE LA OFICINA DE ECONOMÍA DEL EJÉRCITO.

Objetivos

Establecer, mediante una resolución, la conformación del comité de gestión de seguridad de la información para el departamento de telemática de la oficina de economía del ejército.

Introducción

La creación del comité de gestión de seguridad de la información responde a la necesidad de asegurar la información del departamento de telemática de la oficina de economía del ejército y cumpla con las premisas de confidencialidad, integridad y disponibilidad de la información, para garantizar que los colaboradores de la organización tengan acceso a la información toda vez que así lo requieran.

El comité de gestión de seguridad de la información estará integrado por personal del departamento de telemática de la oficina de economía del ejército, para garantizar el apoyo a las iniciativas de seguridad, generadas en la presente institución.

RESOLUCIÓN No 0001 del año 2018

"Por la cual se Conforma el comité de gestión de seguridad de la información para el departamento de telemática de la oficina de economía del ejército y se define las funciones."

General de brigada de la oficina de economía del ejército

Considerando:

Que el departamento de telemática de la oficina de economía del ejército, tomo la decisión de implementar un sistema de gestión de seguridad de la información, para el aseguramiento de la misma.

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 129-014/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.

RESUELVE:

***Artículo 1°** conformación de gestión de seguridad de la información, crease el comité de gestión de seguridad de la información para el departamento de telemática de la oficina de economía del ejército. El comité estará integrado así:*

1.- El líder del área de informática y comunicaciones.

2.- El líder del área de planeación.

3.- El líder del área jurídica.

4.- El líder del sistema de gestión de calidad.

5.- El líder de la gestión documental

6.- El líder de control interno.

7.- El profesional de seguridad de la información.

***Párrafo 1°** El comité podrá evitar cada sesión, si voz y sin voto a aquellas personas que consideren necesarias para la naturaleza de los temas a tratar.*

***Artículo 2°** Objetivo del comité de seguridad de la información. EL comité deberá asegurar que exista una dirección de apoyo gerencial para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos adecuados en el organismo.*

***Artículo 3°** Funciones del comité. El comité de seguridad de la información del departamento de telemática de la oficina de economía del ejército. Tendrá dentro de sus funciones las siguientes.*

1. *Coordinar la implementación del modelo de seguridad y privacidad de la información y el sistema de seguridad y privacidad de la información al interior del departamento de telemática de la oficina de economía del ejército.*
2. *Revisar los diagnósticos del estado de la seguridad de la información en el departamento de telemática de la oficina de economía del ejército.*
3. *Acompañar e impulsar el desarrollo de proyectos de seguridad el departamento de telemática de la oficina de economía del ejército.*
4. *Coordinar y dirigir acciones específicas que ayuden a tener un ambiente seguro y establecer los recursos necesarios para alcanzar las metas y objetivos del departamento de telemática de la oficina de economía del ejército.*
5. *Recomendar roles y funciones específicas que se relacionen con la gestión de seguridad de la información del departamento de telemática de la oficina de economía del ejército.*
6. *Aprobar el uso de metodologías, estándares y procesos específicos para la seguridad de la información del departamento de telemática de la oficina de economía del ejército.*
7. *Participar en la participación y evaluación de los planes de acción para mitigar los riesgos del departamento de telemática de la oficina de economía del ejército.*
8. *Realizar revisiones periódicas del sistema de gestión de seguridad de la información (como mínimo una vez al año) y según los resultados de la revisión definir las acciones a tomar para mejorar el SGSI para el departamento de telemática de la oficina de economía del ejército.*
9. *Promover la difusión y sensibilización de la gestión de seguridad de la información para el departamento de telemática de la oficina de economía del ejército.*
10. *Poner en conocimiento al departamento de telemática de la oficina de economía del ejército, los documentos generados al interior del comité de seguridad de la oficina de la información que impacten de manera transversal a la misma.*
11. *Revisar periódicamente el manual de políticas de seguridad del departamento de telemática de la oficina de economía del ejército*

Párrafo. Una vez establecido el comité de gestión de seguridad de la información, este podrá proponer por escrito el reglamento, en el cual fijará el alcance de cada una de las funciones operativas señaladas en el presente artículo.

***Artículo 4°** secretaria técnica: La secretaria técnica del comité definirá al interior del comité y el secretario(a) elegido(a) y será reemplazado cada 12 meses.*

Artículo 5 *Funciones de la secretaría técnica. Las funciones de la secretaria serán las siguientes:*

1. *Elaborar las actas de las reuniones del comité y verifica su formalización por partes de sus miembros.*
2. *Citar a los integrantes del comité a las sesiones ordinarias o extraordinarias.*
3. *Remitir oportunamente a los miembros la agenda de cada reunión.*
4. *Llevar la custodia y archivos de las actas y demás documentos.*
5. *Servir de interlocutor entre terceros y el comité.*
6. *Realizar seguimiento a los compromisos y tareas pendientes del comité.*
7. *Presentar los informes que requiera el comité.*

Artículo 6° *Reuniones del comité de seguridad de la información. El comité de gestión de seguridad de la información deberá reunirse, como mínimo cada dos meses, previa convocatoria del secretario técnico del comité.*

Artículo 7° *sesiones extraordinarias. Los miembros que conforman el comité de gestión de seguridad del departamento de telemática de la oficina de economía del ejército podrán ser citados a participar de las sesiones extraordinarias de trabajo cuando sea necesario, de acuerdo a temas de riesgos, incidencias o afectaciones de continuidad dentro del sistema de gestión de seguridad informática.*

Artículo 8° *Vigencia y derogatoria: La presente Resolución rige a partir de la fecha de su expedición.*

PUBLIQUESE Y CÚMPLASE

Dado en Lima el 11 de mayo del 2017

GENERAL DE BRIGADA,

Luis Enrique Bedoya Perales

Elaborado	*Revisado*	*Aprobado*
Sarmiento Astudillo, Gustavo	*Gonzales Aybar, Geampierre*	*Luis Enrique Bedoya Perales*

ANEXO 5: Acuerdo de concientización y confidencialidad de información

ACUERDO DE CONCIENTIZACIÓN Y CONFIDENCIALIDAD DE INFORMACIÓN

De una parte, la Oficina de Economía del Ejército, constituido y regido bajo el Decreto Legislativo N° 1137, Ley del Ejército del Perú, con domicilio en la Av. Boulevard S/N, distrito de San Borja, Lima, debidamente representado por el Jefe de la Oficina de Economía del Ejército, suscribe el presente acuerdo de confidencialidad, a quien en adelante se le denominará "**La OEE"**; y, de otra parte, el Sr _____,

(Cargo)_____iden tificado con DNI **N°**_____ y CIP N° _____con dirección domiciliaria en _____ _____, y quien en lo sucesivo se le denominará "**USUARIO"**, se ha acordado celebrar el presente documento que se regirá por las siguientes cláusulas:

CLAUSULA PRIMERA. - ANTECEDENTES:

Las partes declaran que, como parte de su relación laboral es necesario que se provean de ciertos datos con relación a sus funciones, información y documentación que están obligados a guardar confidencialidad respecto de los mismos y sus antecedentes.

Debido a la naturaleza del trabajo, el **USUARIO** y sus funciones la persona que tiene acceso y/o maneja información clasificada del La OEE, independientemente del soporte, sea físico o magnético, digital, óptico u otros que se creen; así mismo, es quien realiza cualquier operación o procedimiento técnico, ya sea automatizado o no, tales como: recopilar, almacenar, conservar, elaborar, modificar, extraer, consultar y utilizar datos.

CLAUSULA SEGUNDA. - OBJETO:

El presente acuerdo tiene el objeto de garantizar la confidencialidad de los datos e intercambio de información entre ambas partes, cualquiera fuera la forma o modalidad de creación, almacenamiento, organización y acceso a través de su adecuado tratamiento, en un marco de respeto a los derechos fundamentales que en ella se reconocen.

CLAUSULA TERCERA. - OBLIGACIONES DE LA OEE:

Adoptar las medidas técnicas, organizativas y legales necesarias que garanticen la confidencialidad de la información y evitar su alteración, pérdida, tratamiento o acceso no autorizado, estas medidas deben ser apropiadas y acordes con el tratamiento que se vaya a efectuar.

No recopilar datos por medios fraudulentos, desleales o ilícitos, los mismos que deben ser actualizados, necesarios y oportunos, con relación a la finalidad que haya sido obtenida.

CLAUSULA CUARTA. - OBLIGACIONES DEL USUARIO:

EL USUARIO es consciente de la importancia de su responsabilidad en cuanto a guardar confidencialidad de la información, ya sea dentro o fuera de las instalaciones de La OEE. Por lo tanto, el usuario manifiesta haber leído, entendido y se compromete a cumplir con todas las disposiciones que normen la confidencialidad, cualquiera sea su fuente o registro: oral, escrito impreso, magnético, electrónico, fax, fotografía, video o cualquier otro medio de conservación. Del mismo modo, declara que, durante su vinculación laboral con la OEE, no intentará tener acceso, copiar, compartir o hacer conocer a terceros ninguna información a través de cualquier medio de comunicación y/o redes sociales.

El USUARIO se compromete a utilizar todos los medios razonables para proteger la información confiada a su persona y a no hacer uso de sus privilegios de acceso a la información más allá de lo estrictamente necesario para el cumplimiento de sus funciones, del mismo modo, no compartirá su contraseña de acceso, ni comprometerá la confidencialidad de la información contenida en ella.

El USUARIO no transportará información clasificada fuera de las instalaciones de La OEE; cuando por razones de servicio se requiera trasladar la misma, lo hará sólo con autorización del Oficial de Seguridad, adoptándolos medios necesarios para garantizar la confidencialidad.

El USUARIO acepta que la terminación de su vinculación con La OEE, cualquiera que sea la causa, no determinará la terminación de los compromisos que asume mediante el presente documento. Al término de su vinculación laboral devolverá toda la información que se le haya sido concedido, cualquiera sea su fuente: escrito impreso, magnético y/o cualquier medio de soporte de información.

CLAUSULA QUINTA. -INCUMPLIMIENTO: Ambas partes reconocen que los compromisos asumidos en el presente documento constituyen obligación esencial al cargo y relación del USUARIO con la OEE, y que su incumplimiento ocasionará una sanción disciplinaria de acuerdo con la Ley N° 29131, Ley del Régimen Disciplinario de las Fuerzas Armadas, independientemente de la responsabilidad civil y/o penal en que pudiera incurrir.

CLAUSULA SEXTA. -VIGENCIA: El presente acuerdo surtirá efectos a partir de la fecha de la firma del presente documento y tendrá vigencia aun después de concluido el vínculo entre las partes. Esta obligación subsiste aun después de finalizada la relación laboral con la OEE.

El obligado puede ser relevado de la obligación de confidencialidad cuando medie consentimiento previo, informado inequívoco del titular de los datos personales, resolución judicial consentida o ejecutoriada, o cuando medien razones fundadas relativas a la Defensa Nacional, seguridad pública, sin perjuicio del derecho a guardar secreto profesional.

CLAUSULA SEPTIMA. -DERECHO DE AUDITAR Y MONITOREAR: En las actividades que impliquen información clasificada, la OEE con el Oficial de Seguridad de la información y el encargado de la administración de la seguridad del DETELE-OEE, podrán monitorear a los usuarios y detectar las actividades de procesamiento de información no autorizadas, independientemente de las auditorías programadas por la Inspectoría de la OEE, IGE, OCI y otras determinadas por el Comando.

CLAUSULA OCTAVA. -LEGISLACIÓN APLICABLE: El presente acuerdo de confidencialidad se regirá por las siguientes normas:

1. Ley N° 29733, Ley de Protección de Datos Personales y su reglamento aprobada con el Decreto Supremo N°003-2013PCM del 21 Mar 13.

2. Ley N° 30096, Ley de Delitos Informáticos, modificada por la ley N° 30171.

3. Norma técnica peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información aprobada con RM-0042016-PCM del 08 Ene 16.

4. Decreto legislativo Nº 1094, Código Penal Militar Policial.

5. Ley de Régimen Disciplinario de las Fuerzas Armadas aprobada con DS-008-2013-DE del 02 Oct 13.

6. Reglamento de seguridad militar del ejército RE 34-10.

7. Directiva única para el funcionamiento del sistema de telemática del ejército (Dufsitele). 8. Otras normas y/o disposiciones que se dicten para garantizar la seguridad de la información.

Y en prueba o señal de conformidad, las partes firman por duplicado el presente documento, en San Borja a los a los ____ días del mes de_____ del 20____.

USUARIO:

_____

Firma

_____

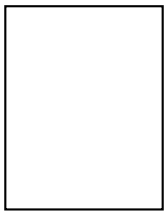
Nombres y Apellidos

_____

Grado

_____

Cargo



ANEXO 6: Gestión informática de remuneraciones

16.11.1.6 FICHA DE PROCEDIMIENTO					
1) Nombre	**Gestión Informática de remuneraciones**				
2) Objetivo	• Procesamiento de información del personal del ejército para el pago de remuneraciones en la fecha establecida por el estado				
3) Alcance	• Detele de la OEE • Copere.				
4) Proveedor	5) Entrada	6) Descripción de las actividades		7) Salidas	8) Destinatario de los bienes y servicios
		Actividades	Ejecutar		
• Dpto de Ejecución Financiera • Secc Devengados • Dpto Tesorería • Planillas y presupuesto del Copere.	• Necesidad de informatizar los datos de remuneraciones.	• Descargar a la BD-OEE la información del personal en actividad remitido por PLANILLAS-COPERE. • Descargar del SIAF a la BD-OEE la información del personal validado por el AIRHSP-MEF remitido por P-COPERE. • Cruzar la información y actualizar las cuentas validadas en el AIRHSP-MEF. • Comunicar al Dpto de Tesorería para su verificación, control y girado.	Analista, programador y el administrador de la BD de la OEE.	Información Actualizada y validad para el girado.	• Detele de la OEE. • Dpto. de Tesorería.
9) indicadores	• Indicador de eficacia. • Indicador de eficiencia. • Indicador de calidad.				
10) Registros	• Formato TXT en CD, Reporte en el SAAF.				

ANEXO 7: Aprobación de las fases de gasto

16.11.1.7 FICHA DE PROCEDIMIENTO					
1) Nombre	**APROBACION DE LAS FASES DE GASTO**				
2) Objetivo	• Obtener la aprobación del MEF de las fases de gastos, registrados por los departamentos y unidades.				
3) Alcance	• Departamento involucrado en la fase del gasto de la OEE. • Unidades Operativa encargado de ejecutar su presupuesto				
4) Proveedor	*5) Entrada*	*6) Descripción de las actividades*		*7) Salidas*	*8) Destinatario de los bienes y servicios*
		Actividades	*Ejecutar*		
Sectoristas encargados del compromiso, devengado y girado de la OEE.	*Información ingresada de las fases de gasto (compromiso, devengado y girado) en el SAFE-SIGE.*	• *Registrar los documentos de las fases de gasto en el SAFE-SIGE.* • *Interfaz de envío (SIGE al SIAF).* • *Si hay datos mal ingresados, se verifica para su posterior corrección.* • *Transmitir al MEF la información cargada al SIAF.* • *Recepción del MEF la información enviada.* • *Interfaz de recepción (SIAF al SIGE).* • *Si hay rechazo, se verifica el motivo para su posterior corrección por el sectorista.*	• *Analista del SIAF-OEE.* • *Analista de la interfaz del DETELE.* • *Analista del SIAF del MEF.*	*Información validada por el MEF en las diferentes Fases de gastos, para lograr el girado.*	• *DETELE de la OEE.* • *Dpto. de Ejecución Financiera* • *Secc. de Devengamos* • *Dpto. de Tesorería.*
9) indicadores	• *Indicador de Eficacia.* • *Indicador de Eficiencia.* • *Indicador de calidad.*				
10) Registros	• *Aprobación de la fase del gasto.*				

ANEXO 8: Formato de planeamiento de seguridad

Hoja de trabajo para desarrollar un planteamiento de seguridad

Recursos de la fuente			Tipo de usuario del que hay que proteger al recurso	Posibilidad de amenaza	Medidas que se implementarán para proteger al recurso de la red
Número	Nombre	Importancia del recurso			

ANEXO 9: Formato de plan de Auditoria Interna

PLAN DE AUDITORIA INTERNA

PROCESO O AREA A AUDITAR:

OBJETIVO DE LA AUDITORIA:

ALCANCE DE LA AUDITORIA:

CRITERIOS DE AUDITORIA:

AUDITORES

NOMBRE AUDITOR

AUDITADO		INICIO DE LA ACTIVIDAD DE AUDITORIA		CIERRE DE LA ACTIVIDAD DE AUDITORIA		AUDITOR
ACTIVIDAD O CRITERIO	CARGO DEL RESPONSABLE DEL PROCESO	FECHA	HORA	FECHA	HORA	

NOMBRE Y FIRMA
AUDITOR JEFE

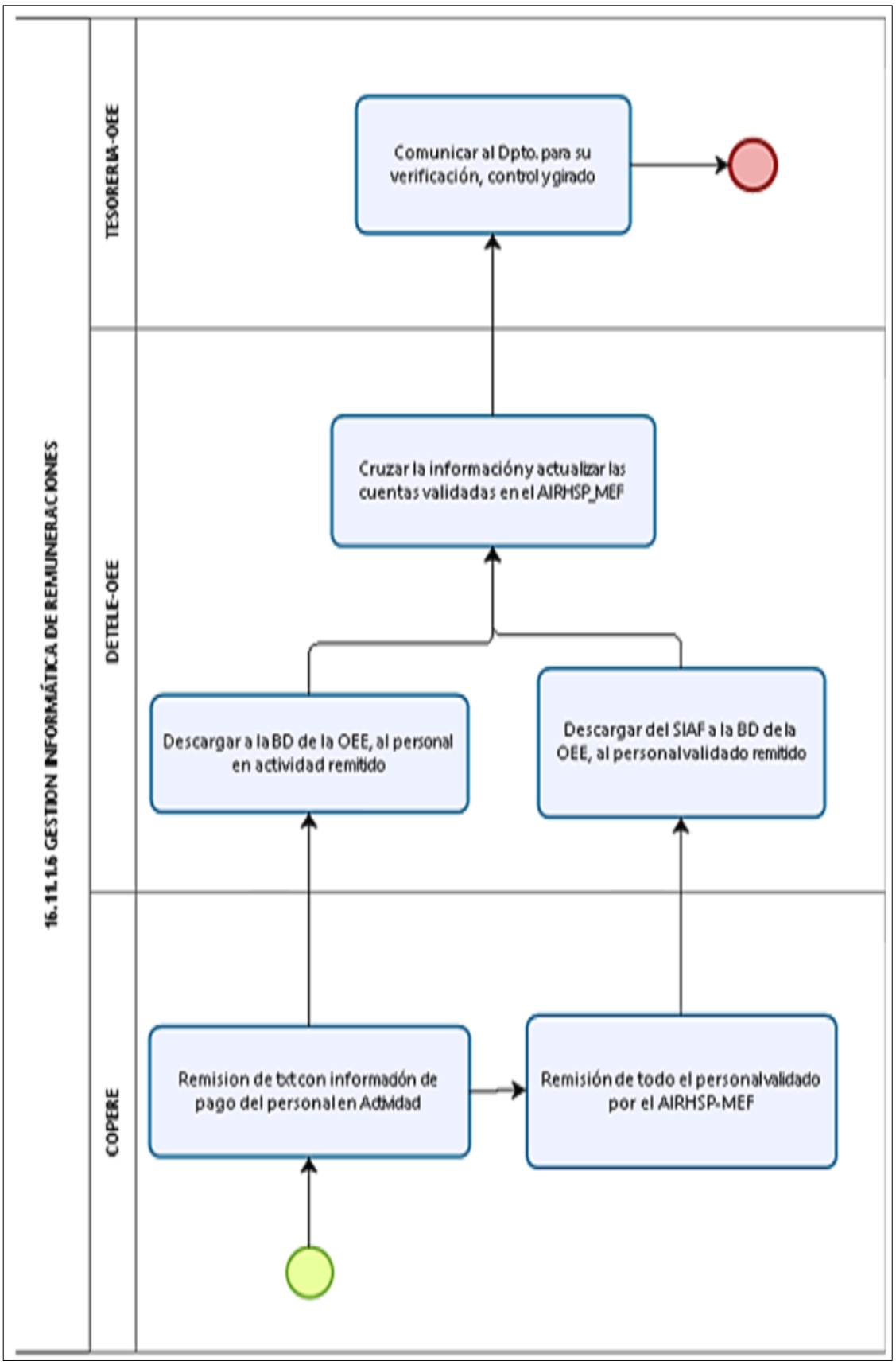
NOMBRE Y FIRMA
FIRMA DEL AUDITOR(ES)

NOMBRE Y FIRMA
FIRMA DEL AUDITADO

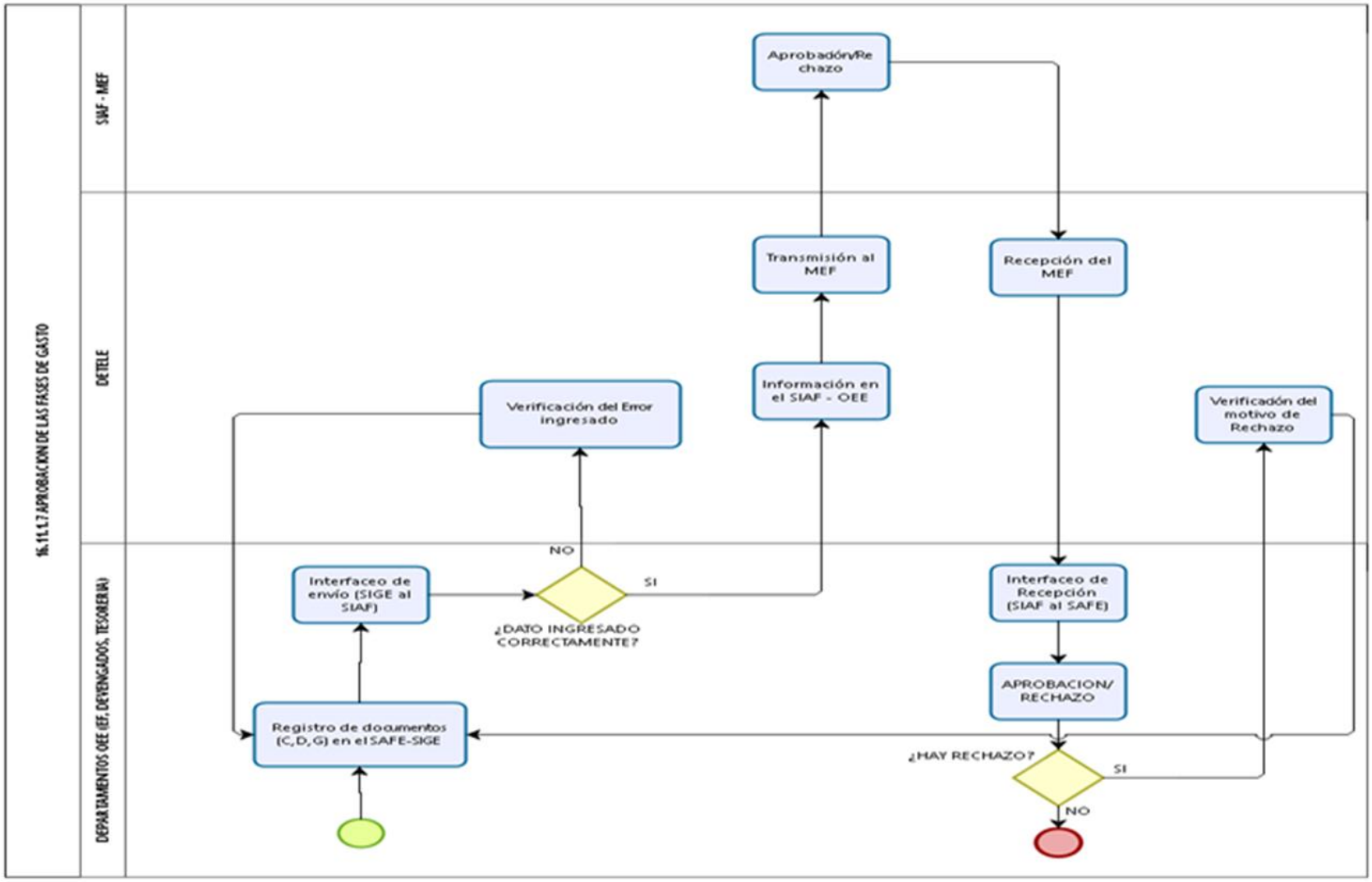
ANEXO 10: Matriz de consistencia

IMPLEMENTACIÓN DE LA NTP/ISO 27001 PARA MEJORAR EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL DEPARTAMENTO TELEMÁTICA DE LA OFICINA DE ECONOMÍA DEL EJÉRCITO DEL PERÚ.									
Preguntas de investigación	**Objetivos**	**Hipótesis**	**Variables**	**Definición conceptual**	**Definición operacional**	**Dimensiones**	**Indicadores**	**Escala de los indicadores**	**Metodología**
General	**General**	**Principal**	**VI: NORMA TÉCNICA PERUANA / ISO 27001**	Es una norma internacional de buenas prácticas, que se emplea para la certificación de los sistemas de gestión de seguridad de la información en las organizaciones empresariales. (Conexión ESAN, 2016)	La implementación de la NTP/ISO 27001 se efectuará mediante el diagnóstico y evaluación del proceso de seguridad de la información, se planificará las actividades a realizar mediante el flujo de trabajos concurrentes basándose en actividades específicas reduciendo los riesgos sobre la información.	PRESENCIA - AUSENCIA			**Tipo de Estudio:** Estudio Aplicado. **Diseño metodológico:** Experimental. **Nivel:** Pre-experimental
¿EN QUÉ MEDIDA LA IMPLEMENTACIÓN DE LA NTP/ISO 27001 MEJORARÁ EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL DEPARTAMENTO DE TELEMÁTICA DE LA OFICINA DE ECONOMÍA DEL EJÉRCITO DEL PERÚ?	DETERMINAR EN QUÉ MEDIDA LA IMPLEMENTACIÓN DE LA NTP/ISO 27001, MEJORA EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL DEPARTAMENTO DE TELEMÁTICA DE LA OFICINA DE ECONOMÍA DEL EJÉRCITO DEL PERÚ	SI SE IMPLEMENTA LA NTP/ISO 27001, ENTONCES MEJORARÁ EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL DEPARTAMENTO DE TELEMÁTICA DE LA OFICINA DE ECONOMÍA DEL EJÉRCITO DEL PERÚ							
Específicas	**Específico**	**Secundarias**	**VD: PROCESO DE SEGURIDAD DE LA INFORMACIÓN**	El Sistema de Gestión de la Seguridad de la Información, es el principal concepto de lo que está conformada la ISO 27001, esta se debe realizar mediante un proceso sistémico, documentado y conocido por toda la empresa. Según ISO 27001, el SGSI, consiste en preservar la confidencialidad, integridad y disponibilidad, además de todos los sistemas implicados en el tratamiento dentro de la Organización. (ISO 27000.es, s.f.-a)	La mejora del proceso de seguridad de información será evaluada mediante un cuestionario de realización de tareas, así mismo se ejecutarán entrevistas.	Rendimiento de la implementación de la NTP/ISO 27001	Tiempo para reportar una incidencia de seguridad de la información	Razón	**Población:** Se identifica como los procesos de seguridad de la información en el departamento de telemática de la Oficina de Economía del Ejército del Perú desde su fundación hasta la actualidad, en el cual existen una cantidad indeterminada de elementos por analizar. **Técnica de muestreo:** Probabilística: Aleatoria simple. **Muestra:** Para esta investigación se tomó una muestra de 30 procesos de seguridad de la información en el departamento de telemática de la Oficina de Economía del Ejército del Perú, ya que se trata de un valor adecuado, estándar y se utiliza en varios procesos de investigación. (Pande, 2004)
	Disminuir el tiempo para reportar incidencias de seguridad de la información en el departamento de telemática de la oficina de economía del ejército del Perú.								
	Aumentar la disponibilidad de información en el departamento de telemática de la oficina de economía del ejército del Perú.						Porcentaje de disponibilidad de la información dentro de la institución	Razón	
	Aumentar el porcentaje de confidencialidad de la información en el departamento de telemática de la oficina de economía del ejército del Perú.						Porcentaje de confidencialidad de la información dentro de la institución	Razón	**Técnica:** Observación, Encuestas y Análisis documental. **Instrumento:** Cuestionario, ficha de observación y ficha de análisis documental. **Análisis:** Estadística descriptiva - inferencial.
	Disminuir el tiempo para para dar respuesta a una incidencia de seguridad de la información en el departamento de telemática de la oficina de economía del ejército del Perú..					Satisfacción de la implementación de la NTP/ISO 27001	Tiempo para dar respuesta a una incidencia de seguridad de la información	Razón	

ANEXO 11: Gestión informática de remuneraciones



ANEXO 12: Aprobación de las fases de gasto



ANEXO 13: Formato de cuestionario

ENCUESTA AL USUARIO

Objetivo de la encuesta: La presente encuesta tiene como objetivo identificar el desempeño del sistema desde el punto de vista del usuario en el Proceso de Seguridad, para tener claridad sobre la situación actual.

Esta encuesta consta de 5 Preguntas.

Lea atentamente cada una de ellas y responda

Género: _____ Edad_____

¿Logramos cumplir sus expectativas durante el proceso de Seguridad?

SI ☐ *NO* ☐

¿Cómo evalúa el tiempo de atención frente al proceso de seguridad?

Excelente ☐ *Bueno* ☐ *Regular* ☐ *Malo* ☐

¿Cómo evalúa el nivel de seguridad brindada a su información?

Excelente ☐ *Bueno* ☐ *Regular* ☐ *Malo* ☐

¿En general cómo califica el servicio recibido?

(Amabilidad, calidad y oportunidad basada en los acuerdos de niveles de servicios)

Excelente ☐ *Bueno* ☐ *Regular* ☐ *Malo* ☐

GLOSARIO DE TÉRMINOS

A

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

Acción preventiva: (Inglés: Preventive action). 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.

Accreditation body: Véase: Entidad de acreditación.

Aceptación del riesgo: (Inglés: Risk acceptance). Decisión informada de asumir un riesgo concreto.

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

Alcance: (Inglés: Scope). Ámbito de la organización que queda sometido al SGSI.

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

Análisis de riesgos: (Inglés: Risk analysis). Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Análisis de riesgos cualitativa: (Inglés: Qualitative risk analysis). 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: (Inglés: Quantitative risk analysis). Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.

Auditor: (Inglés: Auditor). Persona encargada de verificar, de manera independiente, el cumplimiento de unos determinados requisitos.

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

Autenticación: (Inglés: Authentication). Provisión de una garantía de que una característica afirmada por una entidad es correcta.

C

Compromiso de la Dirección: (Inglés: Management commitment). 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: (Inglés: Confidentiality). 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: (Inglés: Corrective control). 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: (Inglés: Detective control). 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 disuasorio: (Inglés: Deterrent control). Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.

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

Corrección: (Inglés: Correction). 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: (Inglés: Statement of Applicability; SOA). 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: (Inglés: Disaster). 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: (Inglés: Guideline). Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

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

E

Estimación de riesgos: (Inglés: Risk evaluation). 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: (Inglés: Risk assessment). Proceso global de identificación, análisis y estimación de riesgos.

Evidencia objetiva: (Inglés: Objective evidence). 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.

G

Gestión de claves: (Inglés: Key management). Controles referidos a la gestión de claves criptográficas.

Gestión de incidentes de seguridad de la información: (Inglés: Information security incident management). Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

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

I

Identificación de riesgos: (Inglés: Risk identification). Proceso de encontrar, reconocer y describir riesgos.

Impacto: (Inglés: Impact). 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: (Inglés: Information security incident). 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: (Inglés: Integrity). Propiedad de la información relativa a su exactitud y completitud.

Inventario de activos: (Inglés: Assets inventory). 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/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.

O

Objetivo: (Inglés: Objetive). Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

P

Parte interesada: (Inglés: Interested party / Stakeholder). 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 tratamiento de riesgos: (Inglés: Risk treatment plan). Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Proceso: (Inglés: Process). Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del riesgo: (Inglés: Risk owner). Persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

R

Recursos de tratamiento de información: (Inglés: Information processing facilities). Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

Riesgo: (Inglés: Risk). 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.

S

Seguridad de la información: (Inglés: Information security). Preservación de la confidencialidad, integridad y disponibilidad de la información.

Selección de controles: (Inglés: Control selection). Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: (Inglés: ISMS). Véase: Sistema de Gestión de la Seguridad de la Información.

Sistema de Gestión de la Seguridad de la Información: (Inglés: Information Security Management System). 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.

T

Tratamiento de riesgos: (Inglés: Risk treatment). Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad: (Inglés: Accountability). 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: (Inglés: Vulnerability). Debilidad de un activo o control que puede ser explotada por una o más amenazas.