UNIVERSIDAD PRIVADA TELESUP

FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

TESIS

IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NTP ISO/IEC 27001 PARA MEJORAR EL PROCESO DE SEGURIDAD DE INFORMACIÓN EN EL EJÉRCITO DEL PERÚ

PARA OPTAR EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS E INFORMÁTICA

AUTOR:

Bach. HUACASI HUACASI JHON RONALD

LIMA – PERÚ

2018

ASESOR DE TESIS

Mg. OVALLE PAULINO DENIS CHRISTIAN

JURADO EXAMINADOR

Mg. BARRANTES RÍOS EDMUNDO JOSÉ

PRESIDENTE

Mg. BENAVENTE ORELLANA EDWIN HUGO

SECRETARIO

Dr. MOGROVEJO COLLANTES WILLIAN MIGUEL

VOCAL

DEDICATORIA

Esta tesis la dedico a la Universidad Privada TELESUP, sus docentes y asesores que supieron transmitir su amplio conocimiento y experiencia a nosotros los estudiantes; también, dedico la presente a nuestro Dios quien nos guía por el buen camino, fortaleciéndonos en momentos más difíciles para seguir adelante y no desmayar ante los problemas.

AGRADECIMIENTOS

Gracias a Dios por permitirnos tener la oportunidad de desarrollar la presente tesis.

Gracias a la Universidad TELESUP que a través de sus docentes nos han formado profesionalmente.

Gracias siempre a la familia por apoyarnos en cada decisión y emprendimiento de nuevos proyectos.

RESUMEN

El avance científico-tecnológico que se viene generando en este último siglo, sobre todo en el campo de la informática tiene un alto impacto social en todas las instituciones tanto públicas como privadas las mismas que necesariamente deben adaptarse a los cambios implementado con equipos tecnológicos el centro de trabajo lo que genera también las inseguridades para lo cual es imprescindible la implementación de políticas de seguridad de información y sus respectivos procesos.

El objetivo del siguiente trabajo de investigación es lograr la implementación del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de seguridad de información en el Ejército del Perú.

En la investigación presente, se ha empleado el tipo de investigación aplicada, nivel de investigación explicativa y aplicando como diseño de investigación pre experimental.

Con la presente investigación se ha obtenido el resultado de implementación del sistema de gestión de seguridad de información de acuerdo a la NTP ISO/IEC 27001 que mejora el proceso de seguridad de información en el Ejército del Perú, permitiendo la identificación de activos críticos relacionados a la seguridad de la información, permitiendo también realizar la gestión de riesgos que involucra la identificación de amenazas y vulnerabilidades que presenta la dirección respecto a la seguridad de la información.

Palabras clave: Sistema de gestión de seguridad de información, gestión de riesgos, activos, vulnerabilidades y amenazas.

ABSTRACT

The scientific-technological advance that has been generated in this last century, especially in the field of information technology, has a high social impact in all public and private institutions, which must necessarily adapt to the changes implemented with technological equipment of work which also generates the insecurities for which the implementation of information security policies and their respective processes is essential.

The objective of the following research work is to achieve the implementation of the information security management system by applying NTP ISO / IEC 27001 to improve the information security process in the Peruvian Army

In the present investigation, the type of application research has been used, the level of explanatory research and applied as a pre-experimental research design.

With the present investigation the result of the implementation of the information security management system has been obtained according to the NTP ISO / IEC 27001 that improves the information security process in the Army of Peru, allowing the identification of critical assets related to the security of the information, also allowing the management of risks that involves the identification of threats and vulnerabilities that the management presents with respect to the security of the information.

Keywords: Information security management system, risk management, assets, vulnerabilities and threats.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El presente trabajo de investigación de “Implementación de un sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar los procesos de la seguridad de la información en el Ejército del Perú,”, está desarrollado en V capítulos, cada capítulo explica ampliamente el desarrollo para la implementar la NTP ISO/IEC 27001 y sus respectivos procesos, mismos que se describe a continuación.

Capítulo I. Se desarrolla “El problema de la investigación” que permite identificar el problema general y específico de la organización y posteriormente a través de un análisis, permite plantear los objetivos de la investigación y justificación de la solución adecuada, clara y concisa que requiere el problema de investigación.

Capítulo II. Se desarrolla el “Marco Teórico”, que son fundamentos teóricos que permiten el desarrollo de las bases teóricas para su comprensión adecuada del problema, para lo cual se emplea artículos científicos confiables, textos de autores reconocidos y entendidos en la materia con respecto a la seguridad de información, políticas de seguridad de información, implementación de SGSI, gestión por procesos, activos críticos y otros relacionados con el problema de investigación.

Capítulo III. En esta parte del capítulo se desarrolla “Métodos y materiales”, en donde se explica las metodologías que se emplean en el presente trabajo de investigación, especificando las técnicas, instrumentos y procesos para recolectar la información y posteriormente realizar el análisis para determinar los resultados del trabajo de investigación, dando respuesta a las hipótesis planteadas de acuerdo al problema de la investigación.

Capítulo IV. “Resultados”, de la implementación del sistema de gestión de seguridad de la información aplicando la NTP/ISO 27001 para mejorar los procesos de la seguridad de la información en el Ejército del Perú, permite

desarrollar las políticas de seguridad de la información para el control adecuado en la administración de la información clasificada.

Capítulo V y VI Se desarrolla las “Conclusiones y Recomendaciones”, donde se establece las conclusiones producto del trabajo de investigación de acuerdo a la problemática planteada y desarrollada en el trabajo, finalmente se desarrolla las recomendaciones por cada problema específico planteado en el presente trabajo de investigación con respecto a la seguridad de la información.

I. PROBLEMA DE INVESTIGACIÓN

1.1. Planteamiento del problema

En la actualidad el avance tecnológico y la globalización a través de la internet, han generado el desarrollo en diferentes sectores mejorando la calidad de vida; sin embargo, el desarrollo tecnológico también trae consigo los riesgos y amenazas en seguridad de administración de la información en las instituciones públicas y privadas que administran información clasificada y podrían poner en riesgo la Seguridad Nacional. Según manifiesta Leiva, (2015) "el uso de las Tecnologías de Información y de Comunicación se ha incorporado de forma general a la vida cotidiana de una nación. Este nuevo escenario facilita un desarrollo sin precedentes en el intercambio de información y comunicaciones, pero al mismo tiempo conlleva serios riesgos y amenazas que pueden afectar a la Seguridad Nacional. Varios son los factores que contribuyen a la proliferación de acciones delictivas en el ciberespacio, la rentabilidad que ofrece su explotación en términos económicos, políticos o de otro tipo, la facilidad y el bajo costo de las herramientas utilizadas para la consecución de ataques y la facilidad de ocultación del atacante, hacen posible que estas actividades se lleven a cabo de forma anónima, desde cualquier lugar del mundo y con impunidad. Esto tiene un impacto considerado sobre las distintas organizaciones tanto en los sectores públicos como privados, y los propios ciudadanos. Los distintos perfiles de atacantes explotan las vulnerabilidades tecnológicas con el objeto de recabar información de valor para cometer ilícitos, como así también para amenazar los servicios básicos que pueden afectar al normal funcionamiento de un país". (p. 1) También, Sánchez, (2011), indica que, "las organizaciones han de establecer estrategias y controles adecuados que garanticen una gestión segura de los procesos del negocio, primando la protección de la información. Para proteger la información de una manera coherente y eficaz es necesario implementar un Sistema de Gestión de Seguridad de la Información (SGSI). Este sistema es una parte del sistema global de gestión, basado en un análisis de los riesgos, que permite asegurar la información frente a la pérdida de: confidencialidad, integridad y disponibilidad" (p. 2).

Por otra parte, en el país el desarrollo tecnológico, se viene implementando de manera progresiva en las instituciones públicas y privadas, dichas implementaciones tecnológicas muchas veces se realizan sin aplicar políticas de gestión de seguridad de la información. En tal sentido, la Oficina Nacional del Gobierno Electrónico (ONGEI), mediante Resolución Ministerial Nº 004-2016-PCM, aprobó el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Requisitos 2ª - Edición”, en las instituciones que integran el Sistema Nacional de Informática. Asimismo, la Política Nacional de Gobierno Electrónico, aprobada mediante Decreto Supremo N° 081-2013-PCM, en su Objetivo N° 3 establece “Garantizar la integridad, confidencialidad y disponibilidad de la información en la Administración Pública mediante mecanismos de Seguridad de la Información gestionada, así como articular los mecanismos de ciber-seguridad del Estado” ONGEI, (2013).

El Ejército del Perú, tiene implementado medidas de seguridad de la información en base al Reglamento (ME 38-10 SEGURIDAD MILITAR) y otras directivas internas de seguridad de informaciones emitidas por los Jefes de las diferentes dependencias, en dicho reglamento y directivas no se aplica algún sistema de gestión de seguridad de información. En consecuencia se propone la implementación de sistema de gestión para mejora de los procesos de seguridad de informaciones en base a la Norma Técnica Peruana “NTP ISO/IEC 27001–2014 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información, con la finalidad de mejorar la administración y los procesos de seguridad de la información.

Los principales problemas que se vienen generando en la institución son la fuga de información, posibles ataques cibernéticos, falta de monitoreo de red, inadecuada administración de la información clasificada y falta capacitación y conciencia seguridad de información de los empleados. Frente al problema se propone la implementación de sistema de seguridad de la información para la mejora de los procesos de seguridad de la información, aplicando la Norma Técnica Peruana, para lo cual se desarrolla la evaluación de gestión de riesgos,

plan de seguridad de la información en donde se detalla las políticas, funciones y responsabilidades de seguridad de la información, se realiza la evaluación de aplicación de los controles y la elaboración del plan de concientización y capacitación. Los mismos que deben reducir los riesgos y amenazas que de materializarse afectarían la imagen de la institución y en casos extremos afectarían la Seguridad Nacional.

1.2. Formulación del problema

1.2.1. Problema general

¿De qué manera la implementación de un sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 mejorará el proceso de la seguridad de la información en el Ejército del Perú?

1.2.2. Problemas específicos

¿De qué manera la identificación de activos críticos aplicando la NTP ISO/IEC 27001 mejorará el proceso de la seguridad de la información en el Ejército del Perú?

¿De qué manera la gestión de riesgos aplicando la NTP ISO/IEC 27001 permitirá mejorar el proceso de seguridad de la información en el Ejército del Perú?

¿De qué manera los controles del sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001 permitirán mejorar el proceso de la seguridad de la información en el Ejército del Perú?

1.3. Justificación del estudio

El trabajo de investigación es de suma importancia por cuanto es necesario y de gran interés contar con el sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de la seguridad de la información en el Ejército del Perú. La misma que permite identificar los activos críticos y gestionar riesgos de la dirección para mitigar las amenazas y

vulnerabilidades que de materializarse generarían pérdidas de información clasificada afectando la imagen institucional e incluso puede comprometer la seguridad nacional.

1.3.1. Justificación teórica.

En nuestro país se ha creado la Ley Nº 27658, Ley de Modernización de la Gestión del Estado, que declaró al Estado Peruano en proceso de modernización de sus dependencias, entidades y organizaciones, con el fin de mejorar en los procesos de gestión pública; siendo necesario el uso de tecnologías de información y comunicación que permitan brindar mejores servicios al ciudadano, sin descuidar la seguridad de la información para lo cual las instituciones deben implementar sistemas de gestión de seguridad de información de acuerdo a Ley.

En consecuencia, la presente investigación se realiza con el fin de aportar un sistema de gestión de seguridad de la información para mejorar de los procesos de seguridad de la información, dado que la institución donde se realiza la investigación en este caso el Ejército del Perú, en su organización cuenta con diferentes Direcciones que trabajan con información CLASIFICADA por su condición misma y su misión de dar seguridad a la Nación, frente a diversas amenazas como externas e internas; las áreas de TI de la institución y en particular la Dirección de Informaciones que centraliza información delicada debe contar con normas, directivas, políticas y procedimientos en seguridad de información sustentados en la Norma Técnica Peruana (NTP) e incluso estándares internacionales.

En tal sentido, la Oficina Nacional del Gobierno Electrónico (ONGEI), mediante RESOLUCIÓN MINISTERIAL Nº 004-2016-PCM, aprobó el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001-2014, Tecnología de la información - Técnicas de seguridad - sistemas de gestión de seguridad de la información – Requisitos - 2a - Edición”, en las instituciones que integran el Sistema Nacional de Informática.

En la actualidad las áreas de TI y la Dirección de Informaciones de la institución del Estado, tiene implementado medidas de seguridad de la información a través de directivas internas (ME 38-10 SEGURIDAD MILITAR) entre otras directivas emitidas, ninguno está acorde a los procedimientos de NTP y menos de alguna norma internacional.

1.3.2. Justificación práctica.

El presente trabajo de investigación se realiza por la necesidad de implementar el sistema de gestión de seguridad de la información para mejorar los procesos de seguridad de informaciones en el área de TI de la Dirección de Informaciones de la institución, aplicando la NTP ISO/IEC 27001 de seguridad de información basada en metodología de Deming, donde los procedimientos de seguridad de información tengan soporte para la toma de decisiones y el control continuo.

El uso adecuado y oportuno de los procesos de seguridad de la información permitirá al área de TI de la institución, tomar decisiones más acertadas y oportunas, contribuyendo a la mejora continua de la organización, con información real de los incidentes de seguridad de información, respondiendo de manera oportuna previo análisis de los eventos ocurridos y realizar seguimiento a los casos y detectar puntos críticos donde esté afectando el desarrollo del trabajo.

La implementación del Sistema de Gestión aplicando la NTP para mejorar los procesos de seguridad de información en el área de TI de la institución, optimiza los procesos y la administración con respecto a la seguridad de información. Una vez implementado el sistema de gestión de seguridad de la información para mejorar los procesos de seguridad de información en el área de TI de la institución del Estado y verificado su confiabilidad podrán ser implementados en otras áreas de TI de las subdirecciones, divisiones y unidades de la institución; asimismo, se puede emplear para otros trabajos de investigación.

1.3.3. Justificación tecnológica.

La dirección cuenta con diversos recursos informáticos que hacen necesario la implementación del sistema de gestión de seguridad de la información; Existe la experiencia para el análisis, planeamiento e implementación del sistema en base a la Norma Técnica Peruana. Dando prioridad al desarrollo de los procesos críticos de identificación de activos de la organización y se ha identificado la metodología más adecuada para lograr los objetivos de la problemática en estudio; el presente proyecto responde a las necesidades inmediatas de sus procesos de implementación del SGSI, que involucra identificar los riegos, vulnerabilidades y amenazas para tomar previsiones relacionados a la seguridad de la información de la organización; por ello, seremos capaces de llevar adelante la investigación, cumpliendo con todos los objetivos planteados.

1.4. Objetivos de la investigación

1.4.1. Objetivo general

Implementar el sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de seguridad de la información en el Ejército del Perú.

1.4.2. Objetivos específicos

Identificar activos críticos aplicando la NTP ISO/IEC 27001 con la finalidad de mejorar el proceso de la seguridad de la información en el Ejército del Perú.

Identificar oportunamente riesgos aplicando la NTP ISO/IEC 27001, para mejorar el proceso de la seguridad de la información en el Ejército del Perú.

Establecer controles de acuerdo al sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de la seguridad de la información en el Ejército del Perú.

II. MARCO TEÓRICO

2.1. Antecedentes de la Investigación

En el presente capítulo realizamos y desarrollamos antecedentes de trabajos de investigación realizados con anterioridad en temas relacionados con a la seguridad de la información y procesos de mejora en las políticas de SGSI; se han encontrado trabajos similares al planteado en la presente investigación pero en ningún caso se ha encontrado el desarrollado de otro igual, a continuación se tienen los antecedente nacionales e internacionales:

2.1.1. Antecedentes nacionales

Se ha encontrado el estudio realizado por David Aurelio FERNÁNDEZ PEÑALOZA y Oscar Alexis PACHECO VARGAS (2014) trabajo de investigación denominada “MEJORA DE SEGURIDAD DE INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES DE GUARDACOSTAS BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001” UNIVERSIDAD PRIVADA SAN MARTÍN DE PORRES - LIMA.

En dicho trabajo de investigación los miembros de la Marina de Guerra del Perú se plantearon como objetivo general, diseñar un plan de sistema de gestión de seguridad de información en la comandancia de operaciones de guardacostas COMOPERGUARD basada en la norma técnica peruana NTP ISO/IEC 27001.

En dicho trabajo de tesis el método de la investigación que se aplicó fue de carácter deductivo, tipo de investigación descriptivo y diseño no experimental.

El investigador del proyecto en mención llegó a las conclusiones siguientes: (1) Se realizó al 100% el Análisis Situacional de los activos de información en las áreas COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas permitiendo conocer con que equipos de TI cuenta la comandancia. (2) Se realizó al 100% el Análisis de Riesgos de los activos de información

focalizados en el Análisis Situacional, en las áreas COSPAS-SARSAT y SIMTRAC de La Comandancia de Operaciones Guardacostas, mostrando así el impacto de los riesgos en dichas áreas. (3) En el análisis y diseño del Plan de SGSI se demostró que se minimizaron los riesgos, amenazas y vulnerabilidades en un 73% de los activos de información. (4) Se diseñó un plan de sistema de gestión de seguridad de la información para las áreas COSPAS-SARSAT y SIMTRAC de la Comandancia de Operaciones Guardacostas - COMOPERGUARD- basada en la Norma Técnica Peruana NTP-ISO/IEC 27001:2008.

Se halló el documento elaborado por Aliaga Flores Luis Carlos, (2017) en su trabajo de investigación denominada “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UN INSTITUTO EDUCATIVO”, PONTIFICIA UNIVERSIDAD CATÓLICA DE PERÚ - LIMA.

En dicho trabajo de investigación se plantea como objetivo general diseñar un sistema de gestión de seguridad de información (SGSI) basado en las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005, adoptando como framework de negocios la actual versión de COBIT.

Para éste trabajo de investigación se aplicó el método de investigación deductivo, de tipo descriptivo y diseño no experimental.

El investigador del proyecto en mención llegó a las conclusiones siguientes. (1) La información y las personas son activos más importantes que tiene cualquier organización. La falta de controles y políticas enfocadas a su seguridad puede traer consecuencias graves para el cumplimiento de los objetivos de negocio e incluso, pérdidas más graves de lo que la organización supone. (2) No hay un interés adecuado con respecto a la seguridad de información dentro de las instituciones educativas, partiendo desde la alta gerencia hasta los mismos departamentos de TI. (3) Dicha falta de interés se muestra claramente en la falta de políticas, normas y controles dentro del instituto educativo y en la falta de concientización del personal del mismo con respecto a la seguridad de la

información. (4) Un Sistema de Gestión de Seguridad de Información (SGSI) establecido en una institución educativa se muestra como la solución para que el flujo de información que se da entre los procesos críticos y los activos involucrados dentro de dichos procesos, logren el nivel de seguridad adecuado para garantizar el cumplimiento de los objetivos de TI y, en consecuencia, los objetivos organizacionales. (5) Para poder identificar adecuadamente los activos con los que cuenta cualquier organización, es importante realizar un modelado de los procesos involucrados dentro del alcance del SGSI. Para lo cual, en la presente tesis, se procedió a diagramar los procesos "core" utilizando la notación BPMN (Business Process Modeling Notation), la cual muestra de manera clara y concisa el flujo de actividades que se realizan en cada proceso.

Se revisó el trabajo realizado por Javier Alfonso Seclén Arana, (2016) su investigación denominada "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", UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS - LIMA.

En dicho trabajo el investigador se planteó como objetivo general "analizar las principales limitaciones y problemas que vienen enfrentando las entidades del sector público en la implementación del SGSI", así como también investigar las estrategias y metodologías que vienen aplicando las entidades públicas que ya han completado su ejecución, los beneficios obtenidos de haberlo realizado en sus instituciones y la importancia de fomentar la capacitación y especialización en seguridad de la información que permitan un desarrollo integral de esta implementación en las entidades del Estado.

El investigador aplicó como método de la investigación en su proyecto, siendo ésta una investigación de carácter deductivo, de tipo investigación cualitativa y diseño investigación no experimental.

En el trabajo de investigación el investigador arribó a las siguientes conclusiones: (1) El desarrollo de la investigación nos ha permitido encontrar ocho

categorías que representan los factores que afectan la implementación del SGSI en las entidades públicas peruanas. Estos elementos han sido distribuidos en 03 niveles: I) Nivel Estratégico - Una Política Estratégica de Estado en Seguridad de la Información, II) Nivel Operativo: Una gestión eficiente de la seguridad de información, Apoyo institucional de la Alta Dirección, Una adecuada organización del SGSI, Aplicación efectiva de la normatividad en seguridad de información y III) Nivel Técnico: Desarrollo integral institucional de la NTP, Contar con un presupuesto nacional para la seguridad de la información y la especialización técnica de profesionales en SGSI como prioridad nacional. (2) impulsar desde el Gobierno Central, una Política Estratégica de Estado que conlleve a formalizar funcionalmente el cargo de Oficial de Seguridad de Información en la estructura orgánica de las entidades del sector público a través de los instrumentos de gestión institucional vigentes como son el ROF y el MOF. El diseño de esta Política es necesaria para el establecimiento operativo sobre la que se soportará la misma. (3) Establecer la creación de un Departamento de Gobierno de Seguridad de la Información -del más alto nivel- compuesto por un grupo de especialistas en seguridad de la información que opere como un solo grupo de trabajo nacional el cual tenga como principal función un monitoreo permanente de avance y ejecución del avance de la implementación del SGSI en todas las entidades públicas peruanas, lo que podría darse a través de la potenciación funcional y técnica de la ONGEI. (4) Actualmente, las entidades -tanto públicas como privadas- vienen enfrentando desafíos, en este ámbito, los cuales se han tornado más sofisticados y pueden llegar a ser potencialmente devastadores. Por ello, esta política estratégica debe incluir un acompañamiento en la gestión y la definición de sus procesos en cada una de las organizaciones involucradas. (5) Otro elemento a tener en cuenta es el presupuestal, de tal manera de contar con los recursos financieros para llevar a cabo dicha implementación que sea administrada por una entidad central como la Oficina Nacional de Gobierno Electrónico (ONGEI), que asumiría un rol más proactivo en la ejecución de la Política Estratégica de Seguridad de la Información. (6) Por último, no hay que perder de vista el factor de profesionalización de especialistas en seguridad de información en el Estado, la que actualmente es escasa y que es necesario darle un mayor recurso técnico para una eficiente ejecución operativa.

Se encontró el estudio realizado por Joel Enrique, Mercado Rojas, (2016) en su tesis llamada: “MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL E-GOBIERNO”, UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS - LIMA.

En dicho trabajo de investigación el investigador se planteó como objetivo general “elaborar un modelo de gestión de seguridad de la información para el gobierno electrónico en las entidades públicas”.

El investigador, para ésta investigación aplicó el método de la investigación de carácter deductivo, siendo el tipo de investigación descriptivo y el diseño de investigación no experimental.

En el trabajo de investigación en mención, el investigador llegó a las siguientes conclusiones: (1) Se elaboró un modelo de gestión de seguridad de la información para el gobierno electrónico resultado de la revisión y análisis de 11 modelos de seguridad de la información, en los que se identificaron los elementos más relevantes que forman parte del modelo propuesto. (2) Se ha definido una estructura organizacional con funciones definidas que contempla los procesos estratégicos, fundamentales y de soporte, la cual permite gestionar la seguridad de la información y garantizar una mejor experiencia al cliente cuando requiera interactuar con los procesos o servicios de la organización. (3) Se han identificado 05 niveles de madurez para la implementación y operación del modelo de seguridad de la información en los procesos que brindan servicio de gobierno electrónico, permitiendo la gestión de la seguridad en dichos procesos y conocer el nivel de seguridad con que se cuenta. (4) Se han establecido 114 controles de acuerdo a los niveles de madurez, iniciando con 30 en el nivel inicial (nivel 0) y finalizando con 114 en el nivel optimizado (nivel 5); asimismo se han establecido 10 documentos obligatorios para los 05 niveles. (5) Se han establecido 06 tipos de indicadores y métricas con sus respectivas características que permitan medir el desempeño de la gestión de seguridad en los servicios del gobierno electrónico. (6) Se propone una secuencia de 04 fases para la implementación del modelo en

los proceso que brindan servicio de gobierno electrónico donde se explica los pasos a seguir, desde la planeación de la seguridad hasta su revisión y mejora del sistema de seguridad de la información implementado. (7) Este modelo dispone de un alto aporte en el cumplimiento de la NTP IEC/ISO 27001:2014 y el estándar ISM3, debido a que orienta y establece elementos necesarios para la implementación del sistema de gestión de seguridad de la información, siendo útil en la gestión de los procesos que brindan servicios de gobierno electrónico. (8) El modelo establece como parte de la implantación la realización de un análisis y evaluación de riesgos; el cual es muy importante en la toma de decisiones sobre los controles a implementar y su propósito de seguridad para reducir el impacto del riesgo a un nivel aceptable. (9) El modelo permite medir la seguridad global de los procesos que brindan servicio de gobierno electrónico en relación a los controles de seguridad con los que se cuenta, lo cual genera una tendencia hacia la mejora continua.

Se encontró el estudio realizado por David Arturo, Aguirre Mollehuanca, (2014) quien elaboró un trabajo de investigación denominado “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA SERVICIOS POSTALES DEL PERÚ S.A.”, PONTIFICIA UNIVERSIDAD CATÓLICA DE PERÚ – LIMA.

Dicho trabajo de investigación lleva como objetivo general el “diseñar un sistema de gestión de seguridad de información para SERPOST según lo indicado por la NTP ISO/IEC 27001:2008 y la NTP-ISO/IEC 17999:2007 de seguridad de información”.

El investigador ha desarrollado su trabajo de investigación empleando el método de la investigación de carácter deductivo, del tipo de investigación descriptivo y diseño de investigación no experimental.

En el trabajo anteriormente mencionado el tesista arriba a las siguientes conclusiones de investigación (1) El apoyo de la alta gerencia para el diseño del sistema de gestión fue imprescindible, debido a que fue necesaria su intervención

para ayudar a concientizar a los jefes de área y dueños de los procesos a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga. (2) Es necesario difundir las normas de seguridad existentes y establecer charlas de capacitación y concientización en toda la empresa, esto debido a la poca cultura de seguridad que existe en la organización, desde las planas gerenciales hasta el personal operativo, incluyendo al personal de seguridad, debido a que se ha detectado que existen controles normados; sin embargo, estos no son conocidos por el personal y no existen métricas que permitan monitorear el cumplimiento de estas normas. (3) Existe una clara necesidad en la organización de contratar personal especializado para dar soporte a los procesos involucrados en el SGSI, debido a que los recursos actuales no se dan abasto para atender los requerimientos de los usuarios lo cual en muchos casos se ha utilizado como excusa para realizar actos que afectan la seguridad de la información como el préstamo de credenciales de usuarios, uso de un correo para varias personas o la dejadez en la generación de respaldos de información del área. (4) Es necesario mejorar la comunicación con el área de logística para acelerar los procesos de compra de aquellos activos que nos ayudaran en el tratamiento de riesgos detectados, especialmente, si estos riesgos son considerados altos o graves por la organización.

2.1.2. Antecedentes internacionales

Se encontró el estudio realizado por Lidia Constanza, Contreras Esguera, (2017) trabajo de investigación denominado “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA LA DIRECCIÓN DE SISTEMAS DE LA GOBERNACIÓN DE BOYACÁ”, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA – TUNJA - BOYACÁ.

En dicho trabajo de investigación el investigador planteó como objetivo

general el “Diseñar el Sistema de Seguridad de la Información (SGSI) basado en la norma ISO/IEC 27001 en la Dirección de Sistemas de la Gobernación de Boyacá”.

Aplicando para este trabajo de investigación el método de la investigación de carácter cualitativo, el tipo de investigación descriptivo y diseño de investigación no experimental.

El investigador en dicho trabajo de investigación arribó a las siguientes conclusiones: (1) Aplicar la Metodología Magerit para el análisis de riesgos para garantizar la seguridad de los activos de la Dirección de Sistemas de la Gobernación de Boyacá. (2) Con el Diseño de SGSI se logra una planeación anticipada de diferentes eventos, para que todo esté bajo control, lo que significa que utilizando esta estrategia la Dirección de Sistemas de la Gobernación de Boyacá minimice cualquier falla que se presente tanto es su infraestructura o de información. (3) Utilizar esta metodología SGSI permite identificar varias características como son: Conocer, gestionar y minimizar todos los posibles riesgos que puedan atentar con la seguridad de la información; Además, con el SGSI permite analizar y ordenar la estructura los sistemas de información, facilitara la definición de procedimientos de trabajo para mantener su seguridad y disponer de controles que permita medir la eficacia de las medidas tomadas con el fin de proteger a la Dirección de Sistemas de amenazas y riesgos que puedan poner en peligro la continuidad de la Entidad. (4) Con la Norma Internacional ISO 27001 estándar de calidad en los sistemas de seguridad en las Entidades, mejorará el Sistema de Gestión de Seguridad de la Información de la Dirección de Sistemas, con la finalidad de evaluar todos los requisitos para la aplicación de controles de seguridad adaptados a cada una de las necesidades que requiera la misma, todo esto con el fin de garantizar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la Gobernación de Boyacá. (5) Para la ejecución Proyecto del Diseño de un Sistema de Gestión de Seguridad de la información basado en La Norma ISO/IEC 27001 para La Dirección de Sistemas de la Gobernación de Boyacá, se tuvo en cuenta en primer lugar la observación directa, posteriormente se aplicó una encuesta a los funcionarios de la Dirección

de Sistemas y la aplicación de la prueba de análisis de red, con el fin de recolectar información, para poder identificar y definir el punto de partida del desarrollo del SGSI. (6) El conocer el inventario de activos de la Dirección de Sistemas es fundamental para saber en qué grado están expuestos ante el riesgo. Los activos tangibles e intangibles de la ya mencionada anteriormente se encuentra: Servicios, Datos de Información, Aplicaciones Software, Equipos Informáticos Hardware, Redes de Comunicación, Soportes de Información, Equipamiento Auxiliar, Instalaciones y Personal.

Se encontró el trabajo de investigación realizado por Ñauta Benavides, Rigoberto Gonzalo, (2017) quien denominó su trabajo de investigación como "PLAN DE SEGURIDAD INFORMÁTICA PARA MEJORAR LA GESTIÓN DE LA INFORMACIÓN EN LA SOCIEDAD FINANCIERA VISIONFOUND – FODEMI DE LA CIUDAD DE IBARRA", UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES – IBARRA – ECUADOR.

En dicho trabajo de investigación el investigador se planteó como objetivo general "desarrollar un plan de seguridad informática para el mejoramiento de la gestión de la información de la sociedad financiera VISIONFUND - ECUADOR – FODEMI de la ciudad de Ibarra".

El método de la investigación que aplicó el investigador para desarrollar su trabajo de investigación fue de carácter cualitativo, tipo de investigación descriptivo y diseño de investigación no experimental.

El investigador al término de su trabajo de investigación llegó a la siguientes conclusiones: (1) producto del estudio, análisis e implementación de la norma ISO 27002 para el departamento de sistemas y seguridad de la Sociedad Financiera VisionFound - FODEMI de la ciudad de Ibarra se pudo detectar muchas deficiencias en la parte de seguridad de la información. Como consecuencia, la información en todas sus formas y estados. (2) Es importante recalcar que si cumple al 100% con las políticas desarrolladas para la Sociedad Financiera VisionFound – FODEMI, no se garantiza que no tengan problemas de seguridad

ya que no existe la seguridad al 100%; con el manual de políticas de seguridad de la información y con el cumplimiento de las mismas da lugar a minimizar los riesgos asociados a los activos reduciendo impactos, fuga de información y pérdidas económicas originados por la carencia de las normas de políticas de seguridad de la información. (3) Con el manual de políticas de seguridad de la información y la implantación del presente plan para la Sociedad Financiera VisionFound - FODEMI de la ciudad de Ibarra, proporcionan una guía a seguir para trabajar en los aspectos de seguridad. (4) El departamento de sistemas de la Sociedad Financiera VisionFound - FODEMI de la ciudad de Ibarra, debe afrontar las eficiencias de la información, para lo cual debe tomar seriedad sobre lo documentado y realizar proyectos de enmendadura basados en las políticas de seguridad y por último debe realizar campañas de concientización sobre los temas abordados.

Se encontró el estudio realizado por Andrés Felipe, Doria Corcho, (2015) quien titula su trabajo de tesis como “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN MEDIANTE LA APLICACIÓN DE LA NORMA INTERNACIONAL ISO/IEC 27001:2013 EN LA OFICINA DE SISTEMAS DE INFORMACIÓN Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE CÓRDOBA”, UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA MONTERÍA – COLOMBIA.

En dicho trabajo de investigación el autor se plantea como objetivo general “diseñar un Sistema de Gestión de la Seguridad de Información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 para la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba”.

El método de la investigación que se aplicó para el trabajo en mención es de carácter cualitativo, nivel de tipo de investigación descriptivo y diseño de investigación no experimental.

El investigador, luego de realizar la investigación llegó a las conclusiones

siguientes: (1) Los sistemas de información y las TIC en general juegan un papel fundamental en la prestación de servicios de las organizaciones, satisfacción del cliente, logro de objetivos e incluso sacar ventaja competitiva. Sin embargo, el uso de la tecnología conlleva riesgos que la mayoría de las veces son desconocidos por la alta gerencia y no invierten en mecanismos de protección así como en la implementación de modelos de seguridad de la información. (2) Este proyecto permitió conocer los beneficios que genera un Sistema de Gestión de Seguridad de la Información en cualquier organización moderna y especialmente en la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba mediante la aplicación de un estándar internacional de seguridad de la información como la ISO/IEC 27001:2013, que a través de un ciclo de mejoramiento continuo, y mediante su fase de diseño permitió establecer la documentación base que requiere ésta norma. Además, se pudo conocer el estado actual de los dominios, objetivos y controles de seguridad mediante un análisis diferencial y el nivel de cumplimiento que se tiene en referencia al Anexo A del estándar. Esto a su vez, permitió elaborar las Políticas de Seguridad de la Información generales que deberían ser comunicadas a todos los funcionarios con el fin de establecer un compromiso en mantener de los niveles de riesgos aceptables. (3) Por otra parte, se pudo clasificar los activos de información y determinar el nivel de riesgo potencial de cada uno de ellos aplicando una metodología de riesgos de TI sistemática como MAGERIT, donde se pudo identificar los activos más críticos y que requieren de mayor atención y controles de seguridad dado el alto impacto que tienen en la prestación de servicios y funcionamiento óptimo de los procesos de la institución. Para ello, se propuso un documento que contiene el Plan de Continuidad del Negocio con el fin de mantener o restablecer en el menor tiempo posible el funcionamiento de los mismos. (4) Por último, se propuso el modelo COBIT como Gobierno de TI ya que presenta un enfoque integral de la institución y permite la alineación de los objetivos de TI con los objetivos y metas estratégicas de la universidad. Además, su integración con otros estándares de seguridad de la información como ISO/IEC 27001 y su ejecución en cascada o de arriba hacia abajo permite que la alta dirección tenga un mejor entendimiento de la importancia de la infraestructura de TI en el desarrollo normal de los procesos institucionales y por ende en los

objetivos misionales.

Se encontró el estudio realizado por Haineth Parra Alvernia, Javier Contreras Navarro, Diana Yisney Díaz Pacheco y Edwin Jesús López Ovalle, (2015) quienes denominaron su trabajo de investigación como “DISEÑO DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA COMUNITARIA DE ACUEDUCTO DE RIO DE ORO, CESAR “EMCAR””, UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA – OCOÑA.

En dicho trabajo de investigación los autores se plantearon como objetivo general “Diseñar las políticas de seguridad de la información de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar EMCAR”.

La metodología de investigación empleada en el presente trabajo de investigación es cualitativa, de tipo de investigación descriptivo y diseño de investigación no experimental.

En dicho trabajo de investigación se arribó a las siguientes conclusiones: (1) En el proceso de la realización de auditorías, entrevistas y encuestas en la Empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR”, permitió la identificación de amenazas y/o riesgos en cuanto a la seguridad de la información, tales como: Conexiones eléctricas no organizadas, pérdida de los datos por falta de copias de seguridad periódicas, ingreso de personal no autorizado a las instalaciones u oficinas de la empresa, plan de contingencia no elaborado, ni publicado, no hay roles y responsabilidades asignadas, no hay restricción de páginas web para los empleados, en algunos equipos de cómputo no hay asignación de usuarios, ni claves de acceso, tampoco los permisos para el ingreso al sistema, dispositivos expuestos a robos (portátiles y aparatos móviles), entre otros; por este motivo, se propuso el diseño de las políticas de seguridad de la información, buscando su confidencialidad, integridad y disponibilidad. (2) La creación de las políticas de seguridad de la información se basaron en la Norma ISO 27001:2013, tomando los dominios más aplicables a los requerimientos informáticos de la Empresa Comunitaria de Acueducto de Río de Oro, Cesar,

“EMCAR” que fueron en total 11 (once), que darán los controles para el mejoramiento de la administración de la información, cumpliendo así los objetivos propuestos del presente proyecto. (3) Siendo la información el activo más importante de la organización, los riesgos y/o amenazas se deben reducir o mitigar, por lo que la empresa Comunitaria de Acueducto de Río de Oro, Cesar, “EMCAR” no es ajena a que estos posibles ataques informáticos pongan en peligro los datos, es aquí donde las políticas de seguridad de la información deben ponerse en práctica y aplicarlas.

2.2. Bases teóricas de las variables

En esta parte de la investigación se desarrolla la definición de los temas para su mejor comprensión, teniendo como apoyo a diferentes autores e investigadores que desarrollan los conceptos de los temas resaltando la importancia de implementar el sistema de gestión de seguridad de la información en las entidades públicas y privadas de acuerdo a lo establecido por normas internacionales.

2.2.1. Sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001

El ISO/IEC27000, (2014) define “el Sistema de Gestión de Seguridad de la Información de la NTP ISO/IEC 27001 es un conjunto de políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización”.

Mientras que Salamanca, (2016) señala que “el SGSI es un conjunto de procesos para acceder a la información, asegurando la integridad, confidencialidad y disponibilidad, mitigando de esa forma los riesgos que conllevan el acceso a la información”.

El sistema de gestión de seguridad de información busca en una organización la protección de sus activos críticos, además de establecer, implementar,

monitorear, revisar y mejorar la seguridad de la información, con la finalidad de alcanzar los objetivos establecidos de la organización.

Es la Norma Técnica Peruana que establece la implementación del SGSI, **(NTP ISO/IEC 27001:2014 Tecnología de Información- Técnicas de Seguridad - Sistemas de Gestión de Seguridad de Información - Requerimientos)**, actualmente se encuentra vigente y es de cumplimiento obligatorio para las entidades del estado peruano, por resolución aprobada por la Presidencia del Consejo de Ministros (PCM).

La Oficina Nacional de Gobierno Electrónico e Informática - ONGEI - de la Presidencia del Consejo de Ministros, como ente rector de la implementación de la Política Nacional de Gobierno Electrónico, desde su creación de manera progresiva ha emitido normas, con el fin de que instituciones del estado y empresas privadas de manera voluntaria puedan implementar el SGSI para desarrollar la Seguridad de la Información de acuerdo a estándares internacionales. Sin embargo, es de obligatorio cumplimiento para las instituciones integrantes del Sistema Nacional de Informática tales como:

- El Consejo Consultivo Nacional de Informática (CCONI).
- El Comité de Coordinación Interinstitucional de Informática (CCOII).
- Las Oficinas Sectoriales de Informática y demás Oficinas de Informática de los Ministerios, de los Organismos Centrales, Instituciones Públicas Descentralizadas y Empresas del Estado.
- Los órganos de Informática de los Gobiernos Regionales.
- Los órganos de Informática de las Municipalidades.
- Los órganos de Informática de los Poderes Públicos y de los Organismos Autónomos.

Figura 01: Certificación de organizaciones
Fuente: ISO/IEC 27001

2.2.2. FASES DEL SGSI

Las fases del sistema de gestión de seguridad de información planteada por la NTP es de acuerdo al ciclo de Deming el modelo PDCA (Plan-Do-Check-Act). Para entrar a analizar el modelo PDCA hay que analizar el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo con la norma ISO/IEC 27001:2014. Se describe el proceso de especificación del SGSI y el diseño desde el inicio hasta la elaboración de planes de ejecución. En él se describe el proceso de obtener la aprobación, se define un proyecto para implementarlo y da pautas sobre cómo planificar el proyecto. Especifica el proceso de conseguir una aprobación para la implementación, define el proyecto para dicho acometido, el cual es llamado en la norma ISO 27003 proyecto de SGSI, y da instrucciones sobre cómo abordar la planificación de la gestión para implementarlo.

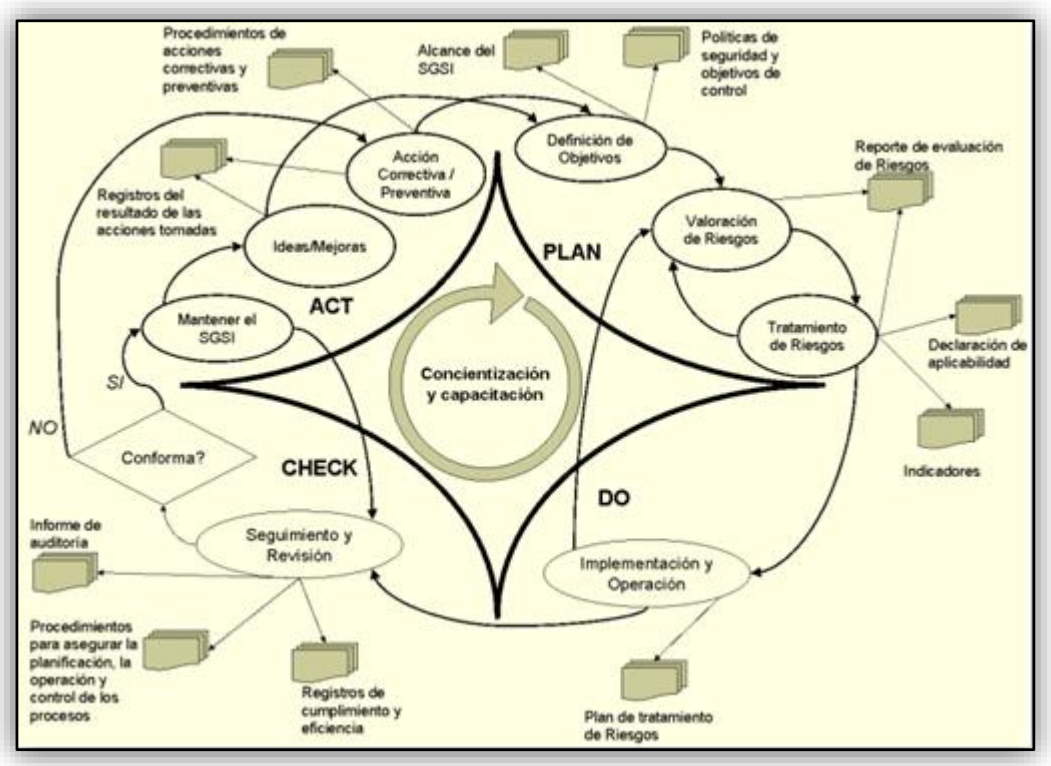


***Figura 2*: PDCA del ISO/IEC 27001**
Fuente: Criptored.

2.2.3. Planificar

El ISO/IEC 27001, (2014) establece que son “acciones para tratar los riesgos y las oportunidades; cuando se planifica para el sistema de gestión de seguridad de información, la organización debe considerar los asuntos externos e internos que son relevantes y que pueden afectar su capacidad de lograr resultados deseados”.

También Cohello, (2015) señala que “la planificación tiene que ver con las acciones para manejar los riesgos y las oportunidades. Cuando se está planificando el sistema de gestión de seguridad de la información, la organización debe considerar los problemas y lograr el mejoramiento continuo”.

Está claro que la organización debe implementar, planificar y evaluar acciones para gestionar los riesgos y oportunidades, buscando integrar los procesos del sistema de gestión de seguridad de la información. Asimismo, la organización debe establecer un criterio de valoración de riesgo aceptable que

conduzcan a resultados consistentes, válidos y comparables frente a riesgos asociados con la pérdida de confidencialidad, integridad y disponibilidad de la información.

Bojórquez Zapata & Pérez Brito, (2013) señalan que la planificación estrategia es vista como la piedra angular de todos los cursos de acción que una organización se proponga. La implementación de las estrategias permitirá el desarrollo de ventajas competitivas entre otros beneficios para las organizaciones. La formulación de estrategias tiene una orientación a largo plazo y sirve de base para todos los elementos que integran la planeación estratégica.

Se puede inferir entonces que en la actualidad, existen varios modelos de planeación estratégica diseñados para ser implementados en las empresas u organizaciones; sin embargo, de acuerdo a diferentes autores se ha mencionado que, éstos, deben ser analizados y adaptados a las condiciones y características especiales de cada empresa u organización en general.

Castellanos, (2015) “la planificación estratégica es la formulación, ejecución y evaluación de acciones para el logro de objetivos corporativos en una empresa”. La planificación estratégica optimiza los recursos, el tiempo y favorece los resultados.

Walter & Pando, (2014) el planeamiento estratégico a nivel sectorial y organizacional es un medio para fortalecer el lineamiento de la acción con los objetivos de la política. Este es un conjunto de conceptos, procedimientos y herramientas para el análisis sistemático y la revisión de la orientación de la acción, del contexto y de los modos de acción, siendo de diversos métodos y diferentes circunstancias. El planeamiento permite el alineamiento organizacional posibilitando la correspondencia de políticas a implementar y misiones a cumplir.

Proceso de planeamiento:

- Definir el alcance del sistema de gestión
- Definir la política del SGSI

- Definir la metodología para la valoración del riesgo
- Identificar los riesgos
- Elaborar un análisis y evaluación de dichos riesgos
- Identificar los diferentes tratamientos del riesgo
- Seleccionar los controles y objetivos de los mismos que posibilitarán dicho tratamiento

2.2.4. Hacer

Implantación y puesta en marcha del SGSI, definiendo 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.

Proceso hacer

- Preparar un plan de tratamiento del riesgo.
- Implantar los controles que se hayan seleccionado.
- Medir la eficacia de dichos controles.
- Crear programas de formación y concienciación.

2.2.5. Verificar

Control y evaluación del SGSI, revisando regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política, objetivos del SGSI y revisión de los controles de seguridad, los resultados de auditorías de seguridad, herramientas de vulnerabilidad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.

Proceso verificar

- Implantar una serie de procedimientos para el control y la revisión.
- Puesta en marcha de una serie de revisiones regulares sobre la eficacia del SGSI, a partir de los resultados de las auditorías de seguridad y de las mediciones.

2.2.6. Actuar

Mejora continua del SGSI, que permita emprender acciones preventivas y correctivas adecuadas en relación a la norma ISO 27001 y comunicar los hallazgos, reportes, estadísticas, así como también las acciones y mejoras a todas las entidades y partes interesadas con el nivel de detalle adecuado.

Proceso actuar

- Tomar las medidas correctivas y preventivas.

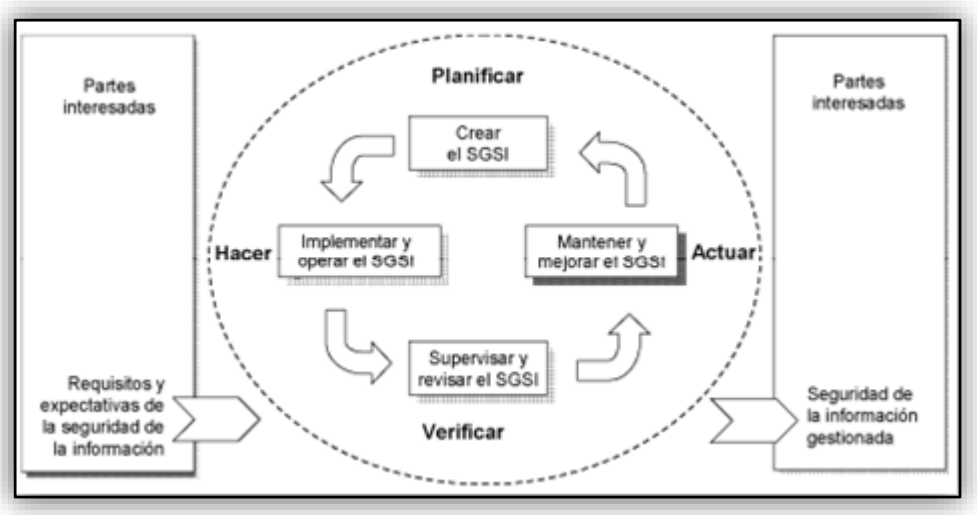


Figura 3: Modelo PDCA aplicada a los procesos del SGSI
Fuente: (Galeon, 2014)

2.2.7. Confidencialidad

El ISO/IEC 27001, (2014) señala “la confidencialidad es una característica que se aplica a la información para proteger y preservar la información; es el medio para garantizar que no esté disponible o divulgado a entidades no autorizadas”.

2.2.8. Integridad

El ISO/IEC 27001, (2014) señala “preservar la integridad de la información significa proteger la exactitud e integridad de la información y los métodos que se utilizan para procesarlo y gestionarlo.

2.2.9. Disponibilidad

El ISO/IEC 27001, (2014) señala que “la disponibilidad es una característica que se aplica a los activos, la misma que está disponible si es accesible y utilizable cuando es necesario por una entidad autorizada. En el contexto de este estándar, los activos incluyen información, sistemas, instalaciones, redes y ordenadores”.

2.2.10. Sistemas

Domínguez Coutiño, (2012) indica que “Un sistema es un conjunto de componentes que interaccionan entre sí para lograr un objetivo común, proporcionando información tanto de problemas como de oportunidades”. Partiendo de ello podemos afirmar que el sistema es una integración de partes interdependientes que pueden estar unidas o relacionadas para formar una organización compleja.

2.2.11. Información

Horacio Saroka, (2002) menciona que “la información es un conjunto de datos que permiten evaluar un problema específico, permitiendo reducir el grado de incertidumbre de quien debe tomar una decisión para alcanzar un objetivo determinado”.

El ISO/IEC 27000 (2014) considera “la información como un activo esencial para la organización y por lo tanto necesita ser protegida de forma adecuada. Dicha información puede ser transmitida por diversos medios como mensajería, comunicación electrónica o verbal; y siempre se necesita una protección

adecuada".

Por otro lado La piedra, Devece y Guiral, (2011) señalan que "toda persona, empresa y en general toda la organización, está continuamente captando una serie de datos, que le sirven para conocer mejor el entorno que le rodea. Estos datos, que constituyen la llamada información, le van a permitir tomar decisiones más acertada".

La información es fuente principal de una organización o empresa, en vista que el adecuado análisis le permite a los directivos de la organización tomar decisiones adecuadas y acertadas para el normal desarrollo de las actividades de la organización o institución permitiendo de esta forma cumplir con los objetivos de cada organización.

Según Domínguez Coutiño, (2012) "la información es un conjunto organizado de datos procesados, constituyen un mensaje que pasa al conocimiento del sujeto o de quien recibe el mensaje". Desde otro punto de vista se puede definir que la información es el resultado de la interacción de los seres vivos o sistemas expertos, la información a diferencia de datos es que se tiene una estructura teniendo diversos tipos como:

- Información pública: Es la información que pude ser conocida por cualquier persona.
- Información interna: Son informaciones propias de una empresa u organización que sirve para los equipos de trabajo.
- Información privada: Este tipo de información de carácter restringido, solo tienen acceso las personas autorizadas.

Fuentes de información

Una fuente de información es alguien que proporciona datos para desarrollar el marco teórico que explica a través de la información y los antecedentes sobre la correcta formulación de una investigación. La búsqueda de las fuentes debe hacerse de la manera más organizada posible, con el fin de

tener una máxima calidad de información que permita tomar mejores decisiones. Tenemos dos fuentes de información fundamentales:

- Fuentes primarias: Son datos obtenidos por el propio investigador o a partir de una búsqueda bibliográfica en artículos científicos, monografías o tesis.
- Fuentes secundarias: Son resúmenes o listados de referencia, basados en fuentes primarias. Es información ya procesada.

En la Dirección de Informaciones del Ejército se administra información dos fuentes de información denominadas abierta y cerrada, se considera fuente abierta toda información procedente de medios de comunicación (tv, radio, periódico, revistas, etc.), mientras que la fuente cerrada comprende información generada o procesada por instituciones legalmente constituidas.

2.2.12. Los sistemas de información

Laudon & Laudon, (2012) plantea la definición técnica de un sistema de información como “un conjunto de componentes interrelacionados que recolectan, procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización. Además, los sistemas de información pueden ayudar a los gerentes y trabajadores a analizar problemas, visualizar temas complejos y crear nuevos productos”.

Dominguez Coutiño, (2012) define que “un sistema de información está integrado de una gran variedad de elementos que se interrelacionan entre sí con el fin de apoyar las actividades de una empresa o negocio. Se considera que un sistema de información brinda información a todos los subsistemas de una organización. Es por eso que un analista se dedica a estudiar todas las partes de una organización, para entonces especificar sus sistemas de información correspondientes” (p. 34).

Se puede considerar que una organización se entiende como un sistema integrada de subsistemas que brindan información a la organización. Por lo tanto, el analista debe dedicarse al estudio de todas las partes de una organización,

para poder especificar los subsistemas de información correspondientes.

Así mismo, con frecuencia, los sistemas de información que logran la automatización de procesos operativos dentro de una organización son llamados sistemas transaccionales, ya que su función primordial consiste en procesar transacciones tales como pagos, cobros, pólizas, entradas, salidas etc. por otra parte, los sistemas de información que apoyan el proceso de toma de decisiones con los sistemas de apoyo a la toma de decisiones (DSS), sistemas para la toma de decisiones de grupo (GDSS), sistemas expertos de apoyo a la toma de decisiones (EDSS) y sistemas de información para ejecutivos (EIS).

2.2.13. Funciones de los sistemas de información

Horacio, (2002) para reducir la frecuencia de los problemas de seguridad es necesario entender sus causas y efectos de seguridad de información, para lo cual se desarrolla la recolección de datos, clasificación, comprensión, almacenamiento, recuperación, el procesamiento, la transmisión y exhibición de los sistemas de información.

a) Recolección de datos

   Horacio Saroka, (2002) la recolección de datos implica la captura y el registro de datos, es una función costosa (con frecuencia es la más cara del sistema de información) y muy expuesta a la generación de errores, aunque éste último aspecto está siendo atenuado en grado creciente por la aplicación de nuevas tecnologías de captura de datos, como la lectura de caracteres ópticos o magnéticos y la lectura de código de barras. Un criterio que disminuye tanto los costos como los errores al momento de capturar los datos, en el lugar donde se generan los datos.

b) Clasificación

   Horacio Saroka, (2002) consiste en identificar los datos, agruparlos en conjuntos homogéneos y ordenarlos tomando en cuenta la manera en que será necesario recuperarlos. Vale decir que los datos se agrupan en estructuras diseñadas conforme a las necesidades del uso que se hará de ellos.

   El diseño del sistema de clasificación debe hacerse de acuerdo con la forma

en que el usuario recuperará la información, tal diseño no puede ser adecuadamente definido si no se posee una clara comprensión de los procesos de decisión.

c) Comprensión

Horacio Saroka, (2002) la compresión nos permite reducir el volumen de los datos sin disminuir necesariamente la información; la compresión puede realizarse mediante varios métodos como la agregación, el filtrado, el uso de medidas estadísticas (tales como la media, la moda, la mediana, los cuartiles, el rango, etc.) que describen el comportamiento, real o pronosticado, de variables probabilísticas.

d) Almacenamiento

Horacio Saroka, (2002) es la conservación física de los datos y su adecuada protección. Aunque no todos los datos que procesa un sistema de información se conservan en dispositivos de computación, éstos constituyen el soporte del banco de datos de las organizaciones. Aun en la tecnología de computación permite mantener este banco de datos virtualmente en condiciones de ser consultado en forma inmediata. En materia de archivos computadorizados, la teoría y la práctica del diseño, la generación, el mantenimiento, la reorganización y la consulta de las estructuras de datos han alcanzado un alto grado de sofisticación y eficiencia.

e) Recuperación

Horacio Saroka, (2002) esta función tiene el propósito de suministrar el acceso a la base de datos, dependiendo de un apropiado sistema de clasificación. Las aplicaciones de computación en las que la recuperación y actualización de los datos, debe hacerse en tiempo real. En estos casos, la computadora interviene en alguna parte de la ejecución de la propia transacción que demanda el uso o actualización de los datos.

f) Procesamiento

Horacio Saroka, (2002) el sistema de información es un transformador de entradas en salidas a través de un proceso. Esta transformación se realiza mediante cómputos, clasificaciones, cálculos, agregaciones, relaciones, transcripciones y operaciones que emplean recursos humanos o tecnológicos

con el objetivo de convertir datos en información, la misma que toma valor y significado para un usuario. La función de procesamiento implica, principalmente, la modificación de la base de datos para mantenerla actualizada y permitir el análisis de la información para la toma de decisiones.

g) Transmisión

Horacio Saroka, (2002) Es la función de comunicación entre puntos geográficos distantes, sea por el traslado físico de los contenedores de datos (papeles, dispositivos de archivos computadorizados, cintas de audio o video, microfichas, etc.) o por la transmisión de señales (comunicación entre equipos de computación, transmisión de facsímiles, teléfono, etc.) vinculada con la tecnología de comunicaciones, y la telemática que es la combinación de las telecomunicaciones y la informática.

Las facilidades disponibles para transmitir datos entre distintos puntos físicos, permiten descentralizar los recursos de computación y las bases de datos. Esto puede hacerse con la integración de sistemas y archivos, que están interconectados, compartiendo recursos y datos y manteniendo similares grados de actualización de las bases de datos. Así, se conforman las llamadas redes de procesamiento distribuido, mediante las que se lleva la "inteligencia" de computación al mismo lugar en que se la necesita.

h) Exhibición

Horacio Saroka, (2002) esta función proporciona una salida de información legible y útil al destinatario. En un sistema de información basado en el uso de computadoras, esta función es la que implica la interfaz con el ser humano. La presentación de los resultados tiene particular importancia para inducir a los mismos a tomar la acción.

2.2.14. Proceso de seguridad de información

El ISO/27000, (2005) indica que "los procesos de seguridad de la información son el conjunto de medidas preventivas y reactivas de las organizaciones que permiten resguardar y proteger la información buscando mantener las dimensiones (confidencialidad, disponibilidad e integridad) de las mismas".

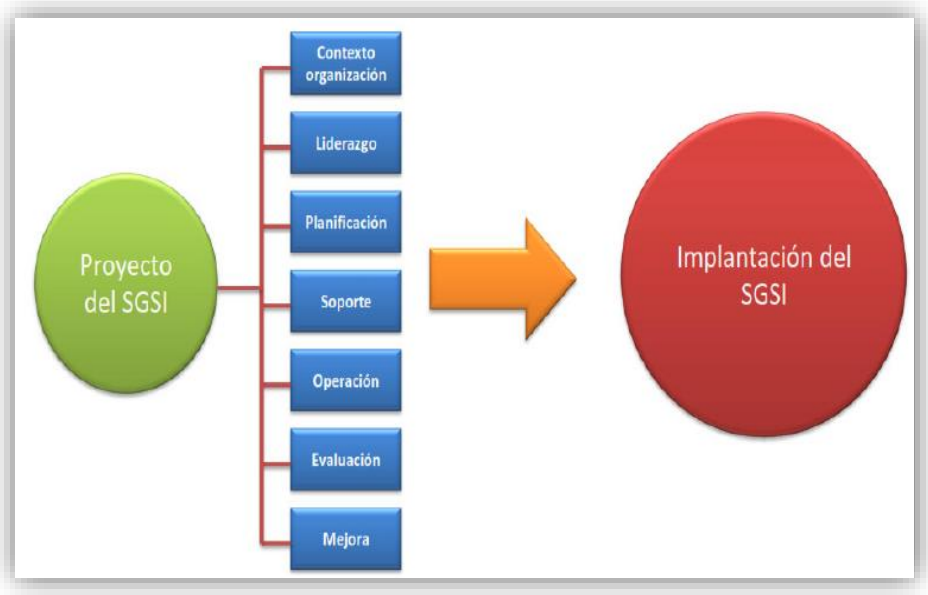


***Figura 4*: Procesos del SGSI**
Fuente: ONGEI, 2017

Por otra parte Núñez, Vélez y Bérdugo, (2004) señalan que “la metodología de mejora de procesos aplicada está basada en modelos de excelencia, el enfoque de gestión por procesos y el gestión de calidad, cuyos modelos tienen como principal objetivo a orientar a las empresas en la búsqueda constante del perfeccionamiento, por lo cual se constituyen en guías prácticas que las ayudan a mejorar y crear una cultura de calidad, midiendo en qué punto se encuentran dentro del camino de la excelencia”.

La mejora continua de la seguridad de información en los procesos de la organización es primordial porque contribuyen a preservar la confidencialidad, integridad y disponibilidad de la Información, permitiendo de alguna forma elevar el nivel de conciencia y cultura de seguridad de la información en los servidores públicos de la organización.

En referencia Bravo Carrasco, (2013) proporciona valiosa información del proceso, indicando que “el flujograma de la información es un tipo de modelo que proporciona amplia información acerca de variados aspectos del proceso entre ellos flujo, información, actividades, estructura y tecnología”.

El flujo es la secuencia y temporalidad que incluye las actividades e interacciones; la información es la que transmite la línea de flujo, es el medio de comunicación el documento, comunicación electrónica u oral; las actividades son las acciones que se realizan en las organizaciones; la estructura son los roles de las personas en la organización u empresa; y en la tecnología se indica las actividades que requieren el uso del software.

De otra parte la norma ISO/IEC 27001 se enfoca en la metodología de mejora continua o conocido como ciclo de Deming. Dicho ciclo consiste en Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (en inglés Plan-Do-Check-Act) en base a la cual se puede desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar los riesgos o amenazas que puedan poner en peligro los activos de la organización entre ellos la información como activo principal de la institución.

2.2.15. Proceso.

Según MAPRO, (2016) proceso se fine como un “conjunto de actividades mutuamente interrelacionadas o que interactúan, las cuales transforman elementos de entrada en resultados. Conjunto de actividades relacionadas entre sí, que tienen el propósito de producir un resultado o producto para un destinatario de bienes y servicios (internos o externos). Generalmente los procesos involucran combinaciones de gente, máquinas, herramientas, técnicas, materiales y mejoras en una serie definida de pasos y acciones. Los procesos raramente operan en forma aislada y deben ser considerados en relación con otros procesos que pueden influir en ellos” (p. 10).

2.2.16. Identificación de activos

Se identifican los activos de la dirección que están involucrados en diferentes procesos de seguridad de información, de acuerdo al ISO 27005, se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, son los procesos e información más sensibles para la dirección. Los activos de

soporte, son los que dan el soporte adecuado a los activos primarios. Dentro de estas dos agrupaciones, se definieron los siguientes tipos específicos de activos:

- Dato: Es toda aquella información que se genera, envía, recibe y gestionan dentro de la dirección. Dentro de este tipo, podemos encontrar distintos documentos que la dirección gestiona dentro de sus procesos.
- Aplicación: Es todo aquel software que se utilice como soporte en los procesos.
- Servicio: Son los servicios que alguna área de la organización suministra a otra área o entidades externas para realizar gestión de información.
- Tecnología: Es todo el hardware donde se maneje la información y las comunicaciones.
- Instalación: Es cualquier lugar donde se alojan los activos de información. Este lugar o ambiente puede estar ubicado dentro de la organización tanto como fuera de la misma.
- Equipamiento auxiliar: Son los activos que no se hallan definidos en ninguno de los anteriores tipos.

Valoración de los Activos: Los activos que generan valor son aquellos que se necesitan proteger y cada activo tiene una importancia mayor o menor en la dirección. MAGERIT establece dos (2) tipos de valoraciones: Cualitativa que es aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización y la Cuantitativa que estima el costo del activo (incluyendo costo de compra, de reparación, configuración, mantenimiento, etc.).

Se determina la valoración de los activos de acuerdo a la dimensión de seguridad (confidencialidad, integridad y disponibilidad) de la información para ello se establece el siguiente cuadro:

Tabla 1: Dimensión de seguridad de información

Dimensión de seguridad	Nomenclatura	Definición
Disponibilidad		
Integridad		

Confidencialidad		

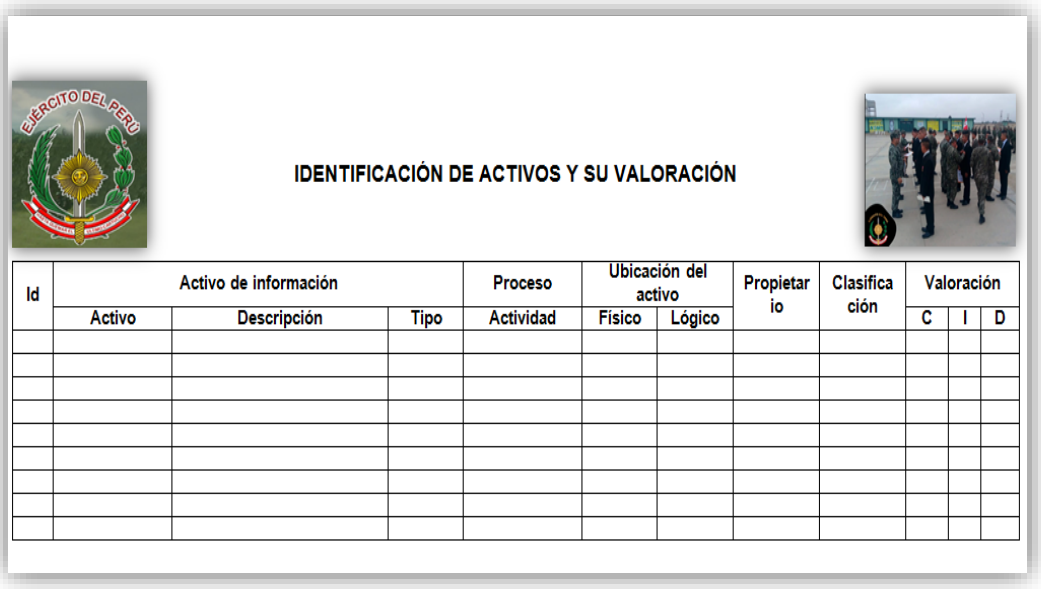
Fuente: MAGERIT

Tabla 2: Valoración de dimensiones de seguridad de información

Disponibilidad (D)		Integridad (I)		Confidencialidad (C)	
Valor	**Criterio**	**Valor**	**Criterio**	**Valor**	**Criterio**

Fuente: MAGERIT

Para determinar los activos de la dirección se establece la MATRIZ DE ACTIVOS en donde se muestra el activo, la descripción, tipo, actividad, ubicación, propietario, clasificación y la valoración (Confidencialidad, integridad y disponibilidad) como a continuación se aprecia:



Id	Activo de información			Proceso	Ubicación del activo		Propietario	Clasificación	Valoración		
	Activo	Descripción	Tipo	Actividad	Físico	Lógico			C	I	D

Figura 5: identificación de activos críticos
Fuente: Elaboración propia

2.2.17. Gestión de riesgo

El ISO/IEC 27005, (2008) define la gestión de riesgo de la información como “el potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a la organización”.

El ISO/IEC Guide 73, (2002) indica que “son actividades coordinadas para dirigir y controlar una organización con relación al riesgo. Normalmente incluye la evaluación, tratamiento, aceptación y comunicación del riesgo. Estas actividades se enfocan manejar la incertidumbre relativa de las amenazas detectadas”.

También podemos definir la gestión de riesgos como un conjunto de actividades coordinadas para dirigir y controlar una organización en lo relativo al riesgo; frente a un eventual hecho que podría afectar el desarrollo de las actividades de una determinada organización. Podemos mencionar tres actividades permanentes: identificar a priori los potenciales dificultades, determinar los riegos relevantes e implementar las estrategias para mitigar los riesgos a presentarse.

Por su parte Martínez, Espinosa, & Amador, (2014) señalan que “la gestión del riesgo en la seguridad de la información implica inversión de tiempo, esfuerzo y otros recursos con los que una pequeña organización no suele disponer, siendo esta una de las razones por las que no suelen ejecutar a gestión del riesgo como una prioridad. Las organizaciones que conocen el valor de sus activos de información y desean invertir en gestionar su riesgo, suelen acogerse a las normas de la familia ISO 27000”.

En relación a la gestión de riesgos la familia ISO/IEC 27000 no especifica la metodología a emplear lo que permite a las organizaciones implementar la gestión de riesgos con la metodología adecuada para cada organización de acuerdo a su contexto, su finalidad y sus objetivos.

Bravo Carrasco, (2013) “la gestión de procesos es una disciplina de gestión que ayuda a la dirección de la empresa a identificar, representar, diseñar,

formalizar, controlar, mejorar y hacer más productivos los procesos de la organización para lograr la confianza del cliente".

2.2.18. Proceso de evaluación del riesgo

Alexander, (2012) el proceso de evaluación del riesgo conformada por seis faces, permite a una organización estar en conformidad con los requerimientos de estándar y ayuda a cualquier organización que desee establecer un SGSI, (Ver la figura N° 6). En los siguientes párrafos una breve descripción de las fases del proceso de evaluación del riesgo será hecho para permitir a las organizaciones gestionar adecuadamente el proceso de evaluación del riesgo al implementar el estándar.

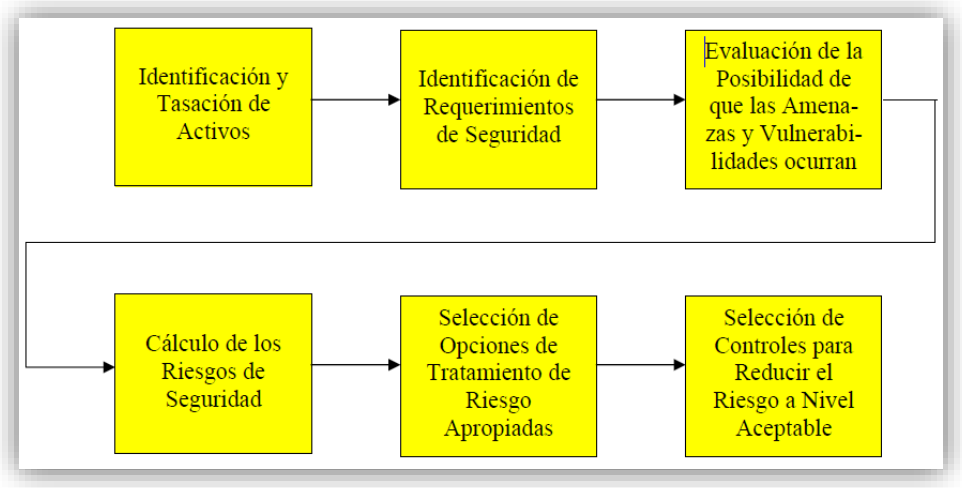


Figura 6: Procesos de evaluación de riesgo
Fuente: Alexander, (2012)

Identificación de tasación de activos: Un activo es aquel que tiene valor y utilidad para la organización, sus operaciones y su continuidad. Los activos necesitan protección para asegurar las operaciones y continuidad de la organización. Cada activo debe estar identificado y valorado apropiadamente el ISO 17799:2005 clasifica los activos de la siguiente manera:

- Activos de información: bases de datos y archivos de datos, documentación del sistema, manual del usuario, materiales de mantenimiento, procedimientos operativos de apoyo, planes de continuidad.
- Documentos impresos: contratos, lineamientos, contratos de la compañía,

documentos que contienen resultados importantes del negocio.

- Activos de software: software de aplicación, software de sistemas, herramienta de desarrollo.
- Activos físicos: equipos de comunicación y computación, medios magnéticos y otros.
- Personal: clientes, suscriptores.
- Imagen y reputación de la compañía.
- Servicios: servicios de computación y comunicación, otros servicios técnicos.

Identificación de requerimientos de seguridad: Los requerimientos de seguridad en las organizaciones derivan de tres fuentes esenciales y deben documentarse en un SGSI.:

- Reconocimiento de amenazas y vulnerabilidades que pudieran ocasionar pérdidas significativas a la organización.
- Requerimientos contractuales que deben satisfacerse por la organización.
- Principios, objetivos y requerimientos para el procesamiento de la información en apoyo a los procesos.

Identificación de amenazas y vulnerabilidades: una amenaza tiene el potencial de generar daño en la organización, el daño puede ocurrir con un ataque directo o indirecto a la información de la organización.

Las vulnerabilidades son debilidades asociadas a los activos de la organización, dicha debilidad puede ser explotada por la amenaza causando incidentes no deseados que pudieran terminar causando daño a los activos de la organización.

- Consecuencias: el daño al activo como resultado de un incumplimiento de seguridad de la información considerando los potenciales consecuencias de pérdidas o fallas de confidencialidad, integridad y disponibilidad de la información.
- Probabilidad: la real posibilidad de que tal incumplimiento ocurra frente a la

amenazas, vulnerabilidades y los controles.

Selección de opciones apropiadas de tratamiento de riesgos: de acuerdo al ISO/IEC 27001 se requiere que la organización siga cuatro posibles acciones para el tratamiento del riesgo:

- Aplicación de controles apropiados para reducir los riesgos.
- Aceptar objetivamente los riesgos y de acuerdo a los criterios.
- Evitar los riesgos.
- Transferir riesgos.

Selección de controles para reducir los riesgos a un nivel aceptable: los controles deben ser seleccionados del Anexo A del ISO/IEC 27001 la cual establece 133 controles específicos.

Riesgo: el riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Por ende, el riesgo es calculado como:

Riesgo = Probabilidad (P) x Impacto (I)

Cabe resaltar que para estimar la el riesgo se debe tener en cuenta las probabilidades de la ocurrencia de las amenazas; y el impacto que éstas podrían ocasionar, de esta forma analizar qué tan probable es que la amenaza se produzca en el futuro. Para ello se debe revisar los antecedentes de los riesgos y se debe asignar a ese riesgo un valor cualitativo (muy alta, alta, media, baja o muy baja) y cuantitativo (5, 4, 3, 2, 1) respectivamente en base a los criterios de evaluación de riesgo y determinar el nivel de riesgo que representa para la dirección.

Tabla 3: Nivel de riesgo

	Nivel de riesgo				
P / I	1	2	3	4	5
5					
4					
3					
2					

1					

Fuente: MAGERIT

Valoración del riesgo: para la organización

Tabla 4: Valoración de riesgo

Nivel de riesgo	Valor	Descripción
Muy alto		
Alto		
Medio		
Bajo		
Muy bajo		

Fuente: Elaboración propia

2.2.19. Establecimiento de Criterios de Evaluación de Impacto

Para establecer criterios de esta parte del capítulo se emplea la metodología MAGERIT, es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por el CSAE (Consejo Superior de Administración Electrónica) que supone los beneficios evidentes de emplear las tecnologías de información, pero gestionando los riesgos inherentes a ella.

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar al alcance de la misión de una organización de acuerdo a las Dimensiones de Seguridad propuesta (confidencialidad, integridad y disponibilidad).

Se define como un conjunto cualitativo y cuantitativo de medidas (criterios de evaluación de impacto) con las cuales se puede evaluar el efecto de un riesgo para los objetivos del proceso de seguridad de información en la organización. Por lo anterior se consideraron las siguientes variables de impacto a evaluar:

- Reputación / confianza.
- Seguridad de la información.
- Productividad

Los criterios de evaluación considerados son:

Tabla *5*: Criterio de evaluación de impacto

CRITERIO	VALOR DEL IMPACTO
Muy alto	5
Alto	4
Medio	3
Bajo	2
Muy bajo	1

Fuente: Elaboración propia

2.2.20. Vulnerabilidades y amenazas

Vulnerabilidad.- Vera y Albarracín, (2017) sostienen que “la vulnerabilidad es considerada como un factor interno de riesgo y alude a las características de un sistema desde el punto de vista de su exposición, capacidad para anticipar, sobrevivir, resistir y recuperarse del impacto de una amenaza natural, antrópica o socio- natural, que implica una combinación de factores que determinan el grado al que un sistema se encuentra en riesgo”.

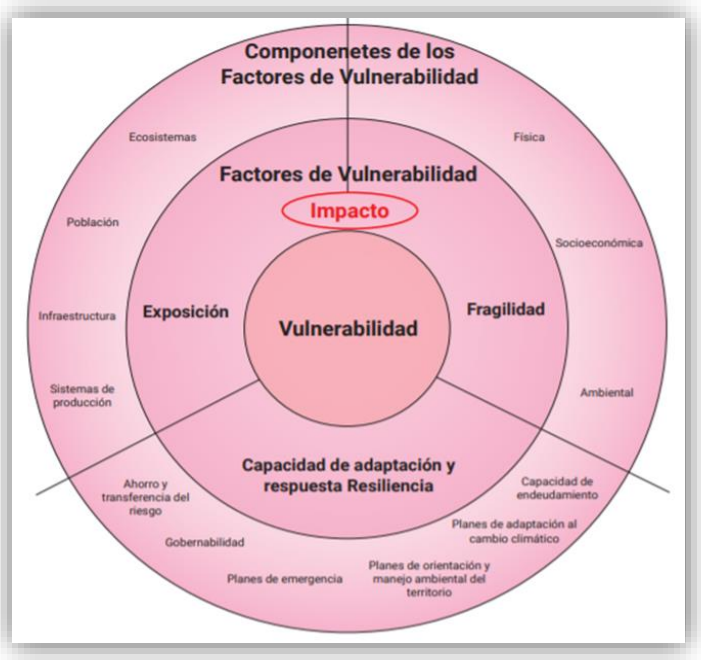


Figura 7: Componentes de factores de vulnerabilidades
Fuente: Vera y Albarracín, (2017)

Establecimiento de criterios de evaluación de probabilidad.

Se define medidas de probabilidad basados en la frecuencia de qué tan probable es que ocurran amenazas. Para ello se tiene que revisar la siguiente información:

- Las amenazas a los activos críticos
- Con qué frecuencia ha ocurrido cada amenaza en el pasado (antecedentes)

Amenaza.- Vera y Albarracín, (2017) señala que “la amenaza es la condición física con el potencial de causar consecuencias no deseables o daños sobre la población, sus medios de vida o el ambiente en general”.

De acuerdo a la metodología de MAGERIT para determinar las amenazas (ver tabla N° 6) y establecer la valoración de las mismas (ver tabla N° 7), se debe tener en cuenta los antecedentes de las amenazas y así de esa forma poder analizar la probabilidad de que la amenaza se materialice en el futuro.

Tabla 6: Tipos de amenaza

Tipo de amenaza	Definición
Ataques intencionados	Fallos deliberados causados por personas
Desastres naturales	Sucesos que pueden ocurrir sin intervención de seres humanos
De origen industrial	Sucesos que pueden ocurrir de manera accidental o deliberada
Errores y fallos no intencionados	Errores o fallos causados por personas

Fuente: MAGERIT

Valoración de Amenazas: Para establecer la valoración de las amenazas es necesario determinar la probabilidad de ocurrencia, la misma que se muestra en el siguiente cuadro:

Tabla 7: Probabilidad de ocurrencia de amenaza

Probabilidad	Valor	Rango
Muy alta		
Alta		
Media		
Baja		
Muy baja		

Fuente: Elaboración propia

Para la evaluación de la probabilidad de que suceda la amenaza se debe registrar para cada activo crítico:

- La información contextual acerca de los actores de amenaza
- El motivo de acciones deliberadas por parte de actores humanos
- La historia de cada amenaza activa
- Las áreas críticas

Cabe resaltar que para estimar la probabilidad se debe tener en cuenta los antecedentes de las amenazas; y así, de esta forma analizar qué tan

probable es que la amenaza se produzca en el futuro. Para ello se debe revisar los antecedentes de las amenazas y se debe asignar a esa amenaza un valor de probabilidad cualitativa (muy alta, alta, media, baja o muy baja) y cuantitativa (5, 4, 3, 2, 1) respectivamente en base a los criterios de evaluación de probabilidad.

Valoración del impacto: Se determina la valoración de los activos de la dirección de acuerdo al tipo Cualitativo que establece MAGERIT y el impacto que tiene en la institución, de acuerdo a la siguiente escala:

Tabla 8: Valoración de impacto

Impacto	**Valor**	**Descripción**
Muy alto		
Alto		
Medio		
Bajo		
Muy bajo		

Fuente: MAGERIT

Previo a la evaluación de los posibles impactos en la dirección, como resultado de las amenazas a los activos críticos, se debe revisar la información de activos críticos y amenazas. Para ello, se debe centrar en los siguientes puntos:

- Amenazas a los activos críticos
- Contexto de la amenaza (actores de amenaza, el motivo, los antecedentes)
- Contexto adicional de la amenaza

También, revisar la información registrada sobre los activos críticos; para ello, se debe centrar en los siguientes puntos:

- Justificación de la selección de activos relacionados.
- Requisitos de seguridad.
- Requisitos de seguridad más importantes.

Luego se revisa los criterios de evaluación de impacto, se debe enfocar y definir el muy alto, alto, medio, bajo y muy bajo impacto para el proceso de seguridad de información en el Ejercito del Perú. Se utiliza los criterios de

evaluación de impacto para evaluar el impacto de cada amenaza sobre los objetivos del proceso de seguridad de informaciones, donde se revisa los criterios registrados para las siguientes áreas:

- Reputación / confianza del personal.
- La vida / salud de los usuarios y funcionarios.
- Seguridad de la información.
- Productividad.

Con relación a la gestión de riesgos también se propone a la dirección la MATRIZ DE RIESGO en donde se establece la identificación del riesgo, amenaza, vulnerabilidad, riesgo, evaluación de riesgo (probabilidad, impacto y nivel de riesgo), tratamiento del riesgo con el respectivo control de la NTP ISO/IEC 27001 seguridad de la información, a continuación se muestra la ficha en mención:

FICHA DE EVALUACIÓN DE RIESGO

Id Ries go	Activo	Identificación de riesgo			Evaluación de riesgo			Tratamiento de riesgo
		Amenaza	Vulnerabilidad	Riesgo	Probab ilidad	Impact o	Nivel de riesgo	Control

Figura 8: Ficha de evaluación de riesgos
Fuente: Elaboración propia

2.2.21. Controles de SGSI

El ISO/IEC 27001, (2014) define como “una especificación para un sistema de gestión de seguridad de la información (SGSI). Un SGSI es un marco de políticas y procedimientos que incluye todos los controles legales, físicos y técnicos

involucrados en los procesos de gestión de riesgos de información de una organización.

Por su parte Tupia, (2009) afirma que “los controles son medios para manejar el riesgo, incluyendo políticas, procedimientos y lineamientos; clasificados como preventivos, detectivos, correctivos y disuasivos”.

Los controles son políticas y procedimientos que se aplican en toda la organización, los niveles y las funciones para asegurar una respuesta adecuada y oportuna frente a un riesgo o amenaza previamente establecidos. Nos permite visibilizar algunas observaciones, falta de políticas, regulación de documentos, incumplimiento de medidas de seguridad de información y otros actividades que pudieran ser irregulares y afectarían a la organización; tales actividades deben ser corregidas como corresponde.

Se ha definido un conjunto de políticas para la seguridad de la información, la misma que fue aprobado por el comando de la dirección, publicado y comunicado al personal y a las partes relevantes como la Inspectoría de la Dirección. (Ver anexo 06). A continuación se muestra campos en las que desarrolla los controles de la NTP ISO/IEC 27001:2014, norma vigente en el ámbito del territorio nacional.

- A.5. Políticas de seguridad de información.
- A.6 Organización de la seguridad de la información.
- A.7 Seguridad de los recursos humanos.
- A.8 Gestión de activos.
- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad física y ambiental.
- A.12 Seguridad de las operaciones.
- A.13 Seguridad de las comunicaciones.
- A.14 Adquisición, desarrollo y mantenimiento de sistemas.
- A.15 Relaciones con los proveedores.
- A.16 Gestión de incidentes de seguridad de la información.

- A.17 Aspectos de seguridad de la información en la gestión de continuidad del negocio.
- A.18 Cumplimiento.

Contacto con grupos especiales de interés

La dirección mantiene contactos apropiados con grupos especiales de interés u otros foros de especialistas en seguridad y asociaciones profesionales como se pudo apreciar en el V SIMPOSIO INTERNACIONAL: “CIBERDEFENSA, CIBERSEGURIDAD, CIBERINTELIGENCIA, RETOS Y AMENAZAS DEL CIBERESPACIO” desarrollado el 30 de octubre de 2018 en el auditorio del Cuartel General del Ejército – San Borja, en efecto se ha evidenciado la participación de especialistas de seguridad de información a nivel nacional e internacional.

Figura 9: V simposio internacional de ciberseguridad
Fuente: Dirección de informaciones

Los controles y sus objetivos de la NTP ISO/IEC 27001-2014, seguridad de información es evaluado por el Comité de Seguridad Información para establecer la APLICABILIDAD DE LOS CONTROLES en la Dirección. (Ver anexo 06).

Para establecer los controles específicos en la presente investigación se

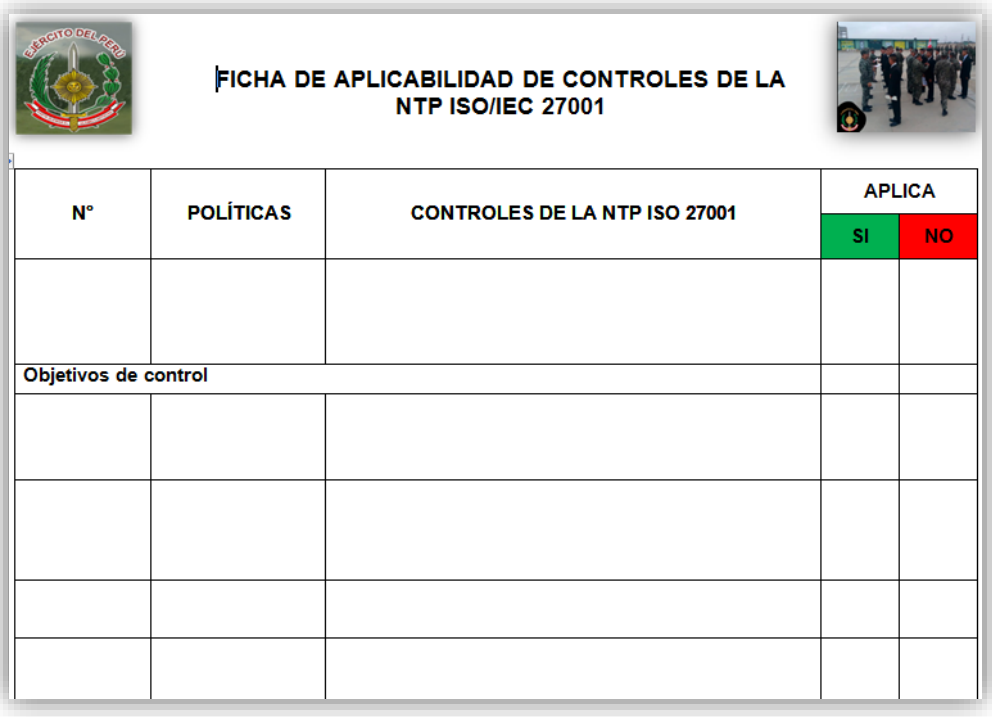
emplea la siguiente formula:

CA = TC – NA

CA = Controles aplicables de la NTP ISO/27001 en la dirección
TC = Total de controles
NA = Controles no aplicables

Figura 10: Fórmula para establecer los controles de NTP ISO/IEC 27001
Fuente: Elaboración propia

Formula que se aplica en la presente investigación para determinar la mejora de controles según la Norma Técnica Peruana NT ISO/IEC 27001 sistema de gestión de seguridad de información SGSI. (Ver anexo 06).



FICHA DE APLICABILIDAD DE CONTROLES DE LA NTP ISO/IEC 27001

N°	POLÍTICAS	CONTROLES DE LA NTP ISO 27001	APLICA	
			SI	NO
Objetivos de control				

Figura 11: Ficha de aplicabilidad de controles de la NTP ISO/IEC 27001
Fuente: Elaboración propia

2.2.22. Bizagi Process Modeler

Bizagi, (2013), define como “una solución informática de distribución libre desarrollada por la empresa Bizagi que permite diagramar y documentar los procesos de una organización de forma gratuita utilizando la notación Business

Process Management BPM”.

Bizagi process modeler, también permite exportar el trabajo a un archivo imagen PNG, JPG y BMP o a archivos Word o PDF; siendo su mayor ventaja el de ser de distribución libre, en efecto se puede orientar a las necesidades de las entidades públicas, de esa forma evitar el uso de herramientas que necesiten el pago de licencias para no afectar el presupuesto designado, es por ello que, en la presente investigación se utilizará esta herramienta tecnológica.

2.2.23. WAMPSERVER

WampServer es un entorno de desarrollo gratuito, su nombre corresponde al acrónimo de:

- Windows : Sistema operativo.
- Apache : Servidor web.
- MySQL : Gestor de base de datos.
- PHP : Como lenguaje de programación.

Wampserver nos permite crear aplicaciones web, con Apache, PHP y gestión de base de datos MySQL. También viene con PHPMyAdmin para facilitar la administración de sus bases de datos; siendo una solución empaquetada que permite reproducir el servidor de producción. A continuación podemos mostrar algunas de las funcionalidades más importantes que trae wampserver:

- Permite administrar la configuración del servidor.
- Se puede acceder a los registros establecidos.
- Se tiene el acceso a los archivos de configuración.
- Permite cambiar el idioma en el menú.
- Acceso a la configuración de Apache.
- Acceso a la configuración de PHP.
- Acceso a la configuración de MySQL.
- Instalación de varias versiones de Apache, PHP, MyQSL.
- Permite editar los archivos de configuración cuando se

realizan cambios.

- Permite instalación de gestión libre de parque informático (GLPI).
- Entre otras funciones de Apache, PHP Y MyQSL.

2.2.24. Gestión Libre de Parque Informático (GLPI)

La mencionada herramienta es una distribución basada en el Proyecto de gestión libre del parque informático (GLPI) y otras tecnologías de código abierto, tales como: Fusion Inventory, MariaDB o Linux. Es un sistema de gestión de servicios de TI, las funciones con que cuenta GLPI facilita el trabajo de los administradores de TI, permitiendo a los profesionales crear su propia base de datos incluyendo el soporte para múltiples usuarios, múltiples ubicaciones, gestión multilingüe, notificaciones mediante emails y petición de ayuda directa para usuarios.

También GLPI, permite crear, mantener, administrar y realizar el inventario de los datos de activos de la dirección como son: ordenadores, software, smartphones, tablets, impresoras, consumibles, entre otros activos integrados por GLPI, ayudando a la estandarización de los procesos, reducir los costos, optimizar la productividad del personal y en caso particular de la investigación permite realizar el seguimiento correspondiente de las incidencias para el respectivo análisis y posterior toma de decisiones por el comando de la dirección respecto a la seguridad de las informaciones.

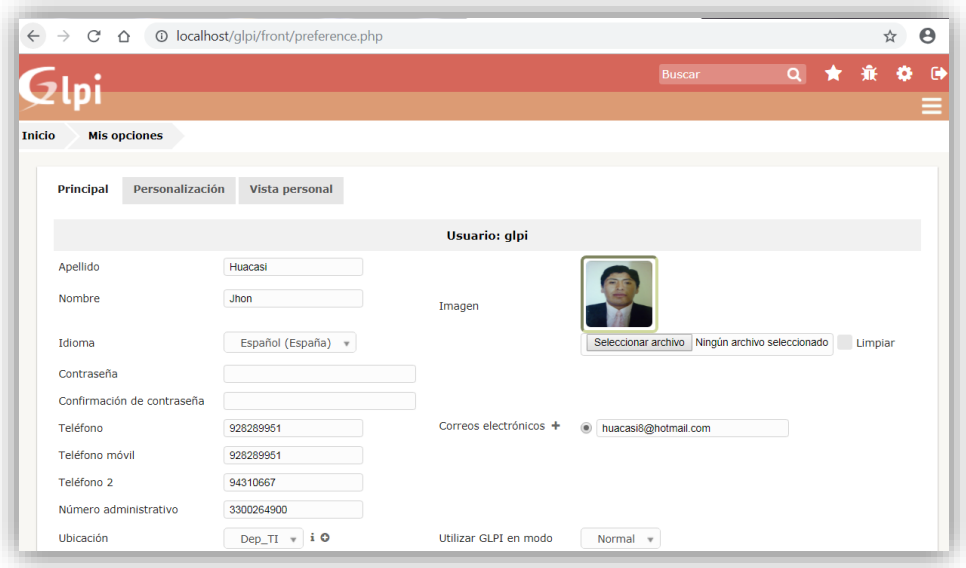


Figura 12: Usuario principal de GLP
Fuente: Elaboración propia

Principales funcionalidades de GLPI

- Gestión multi-entidad, multi-parques y multi-estructuras.
- Gestión multilingüe de 45 idiomas disponibles aproximadamente.
- Soporte multi-usuarios.
- Inventario de activos como ordenadores, periféricos, programas y componentes asociados.
- Gestión administrativa y financiera.
- Gestión de licencias de acuerdo a ITIL (Information Technology Infrastructure Library).
- Informes estadísticos en PNG, SVG o CSV.
- Gestión de empresas y de contactos asociados.
- Gestión de contratos y documentos.
- Base de datos de conocimientos integrada.
- Gestión de expedición de tickets y solicitudes.
- Funcionalidades de monitoreo.
- Generador de reportes de hardware, red o intervenciones.

2.3. Definición de términos básicos

a) Información: “La información como un activo esencial para la organización y por lo tanto necesita ser protegida de forma adecuada” ISO/IEC 27000, (2014).

b) Activo: “Cualquier elemento o información, tenga o no valor contable para la organización” ISO/IEC 27000, (2014).

c) Riesgo: “Efecto de la incertidumbre en los objetivos” ISO/IEC 27000, (2014).

d) Confidencialidad: “La confidencialidad es una característica que se aplica a la información para proteger y preservar la información; es el medio para garantizar que no esté disponible o divulgado a entidades no autorizadas”. ISO/IEC 27001, (2014).

e) Integridad: “Preservar la integridad de la información significa proteger la exactitud e integridad de la información y los métodos que se utilizan para procesarlo y gestionarlo”. ISO/IEC 27001, (2014).

f) Disponibilidad: “La disponibilidad es una característica que se aplica a los activos, la misma que está disponible si es accesible y utilizable cuando es necesario por una entidad autorizada. En el contexto de este estándar, los activos incluyen información, sistemas, instalaciones, redes y ordenadores”. ISO/IEC 27001, (2014).

g) Amenaza: “Causa potencial de un incidente inesperado, que podría resultar e daño a un sistema o a la organización”. ISO/IEC 27000, (2014).

h) Tecnología: “La tecnología es la actividad que utiliza los conocimientos generados por la ciencia aplicada para satisfacer necesidades mediante la producción de bienes y servicios” Arias, (2012).

i) Informática: El término informática proviene del francés informatique, acuñado por el ingeniero Philippe Dreyfus en 1962 (Romero, Saldivar, Delgado y Sanchez, (2012).

j) Archivo: “Toda la información que se transmite a la computadora se guarda en lo que se denominan archivos, los cuales se forman con base en un conjunto de información binaria” Romero, Saldivar, Delgado y Sánchez, (2012).

k) Sistema operativo: “El sistema operativo es el encargado del funcionamiento de las computadoras; en él se encuentran los programas que nos permiten

realizar diversas actividades” Romero, Saldivar, Delgado y Sanchez, (2012).

l) Sistema: “Un sistema es un conjunto de elementos interrelacionados de modo tal que producen como resultado algo superior y distinto a la simple agregación de los elementos” Saroka, (2002).

m) Proceso: “Conjunto de actividades interrelacionadas o interactivas que transforma las entradas en salidas” ISO/IEC 27000, (2014).

n) Almacenamiento: “Esta función se vincula con la conservación física de los datos y con su adecuada protección” Saroka, (2002).

o) Auditoria: “es el proceso independiente y documentado que permite obtener evidencia y determinar objetivamente el grado en que se las normas y procedimientos” ISO/IEC 27000, (2014).

p) Ataque: “Intentar destruir, exponer, alterar, deshabilitar, robar u obtener acceso no autorizado o hacer un uso no autorizado de un activo” ISO/IEC 27000, (2014).

q) Hardware: “Es el conjunto de elementos duros que conforman un equipo de cómputo” Romero Mora, Saldivar Vaquera, Delgado Ibarra, & Sanchez Montufar, (2012).

r) Archivo: “Toda la información que se transmite a la computadora se guarda en lo que se denominan archivos, los cuales se forman con base en un conjunto de información binaria” Romero Mora, Saldivar Vaquera, Delgado Ibarra, & Sanchez Montufar, (2012).

s) Ejército del Perú: “Es una institución de la Fuerzas Armadas, dependiente del Ministerio de Defensa, responsable de organizar y preparar la fuerza para disuadir amenazas y proteger al Perú de agresiones, con el fin de contribuir y garantizar la independencia, soberanía e integridad territorial de la República” D. S. 006-2016 ROF del MINDEF, (2016).

t) Vulnerabilidad: “Es considerada como un factor interno de riesgo y alude a las características de un sistema de estar expuesta una amenaza natural, antrópica o socio-natural, que implica una combinación de factores que determinan el grado al que un sistema se encuentra en riesgo” Vera y Albarracín, (2017).

2.4. Contexto de la organización

2.4.1. Visión

Ejército disuasivo, reconocido, respetado e integrado a la sociedad.

2.4.2. Misión

Controlar, vigilar y defender el territorio nacional y participar en el desarrollo económico y social, control del orden interno y acciones de defensa civil, de acuerdo a ley, en beneficio de los intereses del Estado, de manera permanente y eficaz.

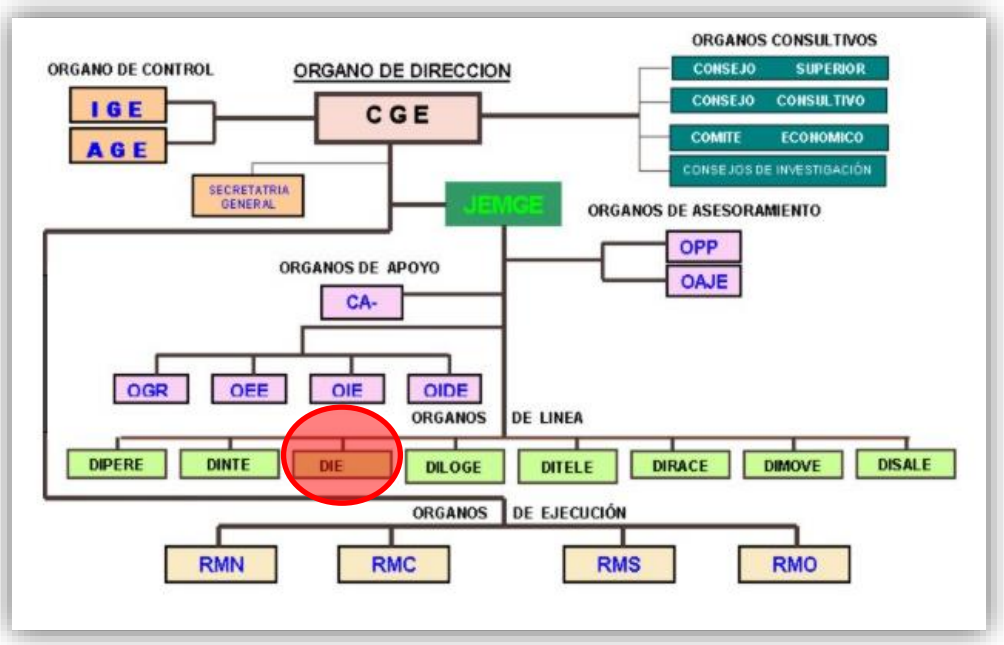


Figura 13: Organigrama del Ejercito del Perú
Fuente: Dirección de informaciones

2.4.3. Objetivos

- Preparar a las Fuerzas Armadas para enfrentar con éxito las amenazas y riesgos a la seguridad nacional.
- Fortalecer la gestión estratégica institucional asegurando la modernización del Ejército.
- Incrementar la preparación de la fuerza operativa del Ejército asegurando el cumplimiento de sus roles constitucionales.

- Mejorar la administración de los recursos humanos, logísticos y financieros del Ejército, asegurando su gestión eficiente y transparente.
- Fortalecer la educación integral del personal del Ejército, asegurando la disponibilidad de personal altamente capacitado.

2.4.4. Implementación de Procesos en el Ejército

Enfoque metodológico que sistematiza actividades y procedimientos, tareas y formas de trabajo con la finalidad de convertirlas en una secuencia garantizando que los bienes y servicios generen impactos positivos para el personal, en función de los recursos disponibles. La implementación de los procesos implica la identificación, el análisis, la mejora y cambio en la organización; además, incluye el uso de herramientas, metodologías y controles que permiten y facilitan el desarrollo de los procesos.

La gestión por procesos implica el desarrollo de las siguientes actividades:

- La identificación de los requerimientos, necesidades y expectativas de los diferentes destinatarios de las prestaciones y servicios públicos, así como de otros posibles grupos de interés.
- La identificación de todos los procesos necesarios para la prestación del servicio público y la adecuada gestión de la entidad: procesos misionales, de soporte a la gestión y estratégicos; lo que se denomina mapa de procesos.
- La definición del objetivo de cada uno de los procesos, así como de los beneficios que aporta a los grupos de interés a los que va dirigido.
- La definición secuencial detallada y precisa, de las diferentes actividades que componen el proceso o procedimiento concreto, para el cumplimiento de los diferentes requerimientos, y en su caso su diagrama.
- La definición de las obligaciones, así como de las autoridades y directivos encargados la definición de indicadores, que permitan

la medición y control del desarrollo de la marcha adecuada del proceso.

- La definición y desarrollo de un sistema de gestión que permita el seguimiento, evaluación y mejora continua, de la calidad de los procesos, y la prestación del servicio.
- La implementación de sistemas de gestión normalizados o estandarizados.

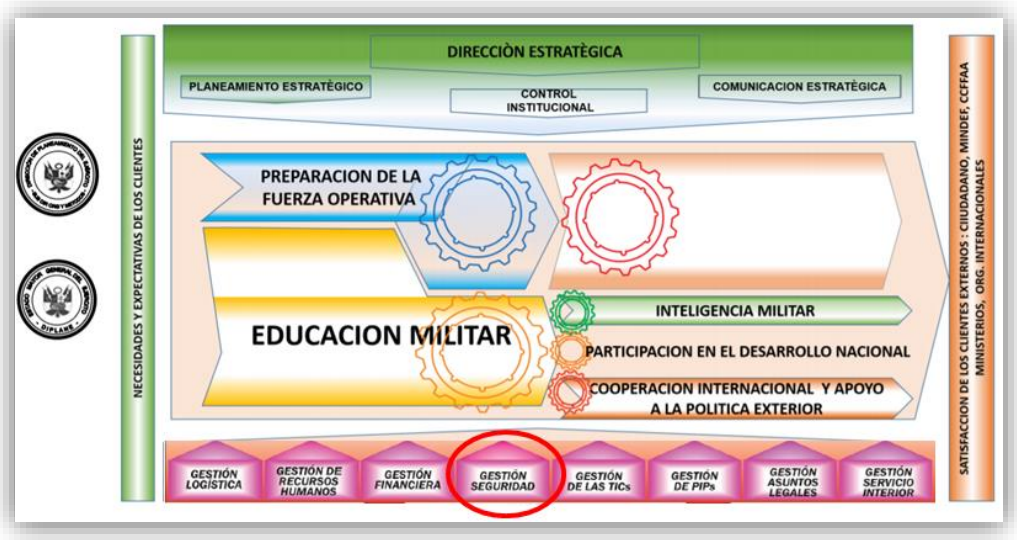


Figura 14: Mapa de procesos de la dirección
Fuente: Dirección de informaciones

2.4.5. Proceso de seguridad de información en la dirección

Para tener el mejor panorama y comprensión de los servicios que brinda la Dirección como una institución del estado, y de acuerdo al análisis previo se considera necesario realizar la identificación de los procesos de la información en diferentes áreas y niveles. Dichos procesos se describen en las tabla 9.

Considerando que los procesos son un conjunto de actividades mutuamente interrelacionadas, los cuales transforman elementos de entrada en resultados con valor agregado, y que los procesos de diferentes niveles o macro procesos son el nivel de mayor agregación, se ha visto por conveniente considerar los siguientes procesos como se detalla en la tabla 9.

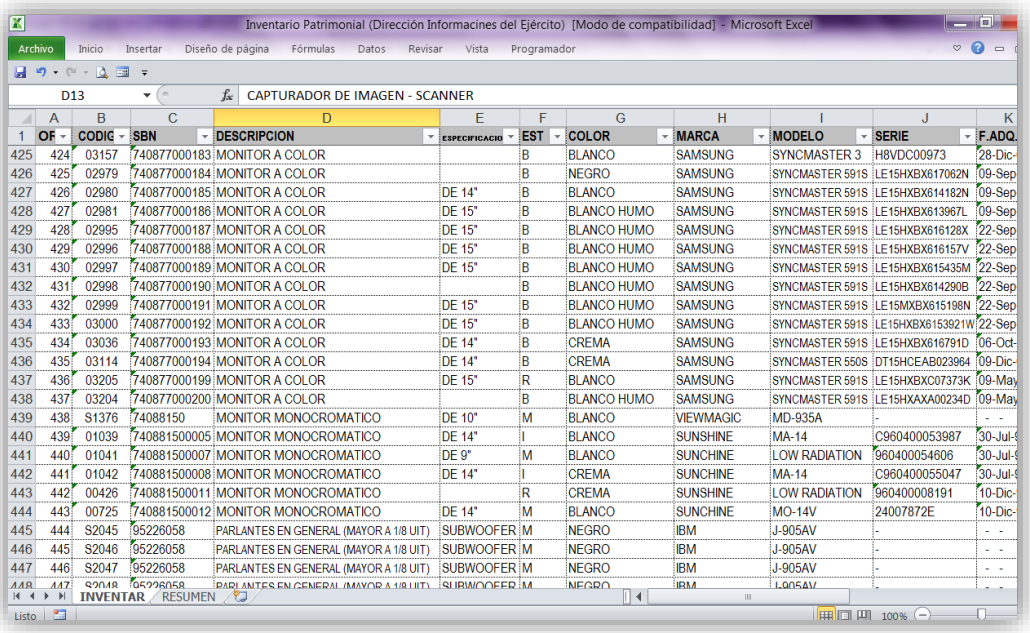
Tabla 9: Procesos estratégicos, operativos y de apoyo

Procesos estratégicos	Procesos operativos	Procesos de apoyo o soporte
• Gestión de políticas de dirección • Gestión de planes y presupuesto • Gestión de imagen institucional.	• Gestión de búsqueda de información • Gestión de análisis de información • Gestión de producción de información	• Gestión logística • Gestión de recursos humanos • Gestión financiera • **Gestión de la seguridad** • **Gestión de las tecnologías de la información y las comunicaciones (TIC)** • Gestión de proyectos de inversión • Gestión de asuntos legales • Gestión del servicio interior

Fuente: Dirección de informaciones

2.4.6. Identificación de activos

En este proceso la dirección tiene considerado el inventario general de la dirección como activos críticos de manera que dificulta la administración exclusiva de activos de información que permitan realizan un análisis integral de la seguridad de información.



	A	B	C	D	E	F	G	H	I	J	K
1	OF	CODIG	SBN	DESCRIPCION	ESPECIFICACIO	EST	COLOR	MARCA	MODELO	SERIE	F.ADQ.
425	424	03157	740877000183	MONITOR A COLOR		B	BLANCO	SAMSUNG	SYNCMASTER 3	H8VDC00973	28-Dic-
426	425	02979	740877000184	MONITOR A COLOR		B	NEGRO	SAMSUNG	SYNCMASTER 591S	LE15HXBX617062N	09-Sep
427	426	02980	740877000185	MONITOR A COLOR	DE 14"	B	BLANCO	SAMSUNG	SYNCMASTER 591S	LE15HXBX614182N	09-Sep
428	427	02981	740877000186	MONITOR A COLOR	DE 15"	B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXBX613967L	09-Sep
429	428	02995	740877000187	MONITOR A COLOR	DE 15"	B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXBX616128X	22-Sep
430	429	02996	740877000188	MONITOR A COLOR	DE 15"	B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXBX616157V	22-Sep
431	430	02997	740877000189	MONITOR A COLOR	DE 15"	B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXBX615435M	22-Sep
432	431	02998	740877000190	MONITOR A COLOR		B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXBX614290B	22-Sep
433	432	02999	740877000191	MONITOR A COLOR	DE 15"	B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15MXBX615198N	22-Sep
434	433	03000	740877000192	MONITOR A COLOR	DE 15"	B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXBX6153921W	22-Sep
435	434	03036	740877000193	MONITOR A COLOR	DE 14"	B	CREMA	SAMSUNG	SYNCMASTER 591S	LE15HXBX616791D	06-Oct-
436	435	03114	740877000194	MONITOR A COLOR	DE 14"	B	CREMA	SAMSUNG	SYNCMASTER 550S	DT15HCEAB023964	09-Dic-
437	436	03205	740877000199	MONITOR A COLOR	DE 15"	R	BLANCO	SAMSUNG	SYNCMASTER 591S	LE15HXBXC07373K	09-May
438	437	03204	740877000200	MONITOR A COLOR		B	BLANCO HUMO	SAMSUNG	SYNCMASTER 591S	LE15HXAXA00234D	09-May
439	438	S1376	74088150	MONITOR MONOCROMATICO	DE 10"	M	BLANCO	VIEWMAGIC	MD-935A	-	- -
440	439	01039	740881500005	MONITOR MONOCROMATICO	DE 14"	I	BLANCO	SUNSHINE	MA-14	C960400053987	30-Jul-9
441	440	01041	740881500007	MONITOR MONOCROMATICO	DE 9"	M	BLANCO	SUNCHINE	LOW RADIATION	960400054606	30-Jul-9
442	441	01042	740881500008	MONITOR MONOCROMATICO	DE 14"	I	CREMA	SUNCHINE	MA-14	C960400055047	30-Jul-9
443	442	00426	740881500011	MONITOR MONOCROMATICO		R	CREMA	SUNSHINE	LOW RADIATION	960400008191	10-Dic-
444	443	00725	740881500012	MONITOR MONOCROMATICO	DE 14"	M	BLANCO	SUNCHINE	MO-14V	24007872E	10-Dic-
445	444	S2045	95226058	PARLANTES EN GENERAL (MAYOR A 1/8 UIT)	SUBWOOFER	M	NEGRO	IBM	J-905AV	-	- -
446	445	S2046	95226058	PARLANTES EN GENERAL (MAYOR A 1/8 UIT)	SUBWOOFER	M	NEGRO	IBM	J-905AV	-	- -
447	446	S2047	95226058	PARLANTES EN GENERAL (MAYOR A 1/8 UIT)	SUBWOOFER	M	NEGRO	IBM	J-905AV	-	- -
448	447	S2048	95226058	PARLANTES EN GENERAL (MAYOR A 1/8 UIT)	SUBWOOFER	M	NEGRO	IBM	J-905AV	-	- -

Figura 15: Inventario de activos críticos de la dirección
Fuente: Dirección de informaciones

Para determinar el tiempo total del proceso de identificación de activos críticos de la dirección se emplea ficha de observación posteriormente se establecen valores con la siguiente formula:

TIA= DRt + PTt + APt + ETt + EAt + RVt

TIA= tiempo total del proceso de identificación de activos
DRt= designación de los responsables
PTt= elaboración del plan de trabajo
APt= aprobación del plan de trabajo
ETt= ejecución del trabajo
EAt= elaboración de acta de activos
RVt= revisión y visto bueno por el director
t = tiempo

$$\sum_{n=t}^{6} TIA_t$$

Figura 16: Fórmula para hallar tiempo de proceso de identificación de activos
Fuente: Elaboración propia

Tabla 10: Ficha de observación de tiempo en proceso de identificación de activos

FICHA DE OBSERVACIÓN

DIMENSIÓN: IDENTIFICACIÓN DE ACTIVOS
INDICADOR: TIEMPO TOTAL PARA IDENTIFICAR ACTIVOS

ENTIDAD:	DIRECCIÓN DE INFORMACIONES DEL EJÉRCITO	FORMULA	TIA= DRt + PTt + APt + ETt + EAt + RVt
DISTRITO:	SAN BORJA		
INSTRUMENTO:	FICHA DE OBSERVACIÓN		
OBJETIVO:	MEDIR EL TIEMPO DEL PROCESO DE IDENTIFICACIÓN DE ACTIVOS		

N°	ÁREA	FECHA DE REGISTRO	DRt	PTt	APt	ETt	EAt	RVt	TIA

Fuente: Elaboración propia

2.4.7. Gestión de riesgos

En gestión de riesgos se ha determinado que la dirección cuenta con “PLAN DE SEGURIDAD” en donde se establece los procesos de seguridad de manera integral involucrando diferentes campos (seguridad de instalación, seguridad de comunicaciones, seguridad armamento, seguridad contra incendios, seguridad contra ataque externo, seguridad personal y seguridad de información).

En dicho plan de seguridad se identifican diferentes amenazas como: crimen organizado, corrupción, minería ilegal, conflictos sociales, trata de personas, delincuencia común, narcotráfico, terrorismo y afectación a la seguridad digital.

Amenaza: afectación a la seguridad digital.

Nº	Conceptos Estratégicos	Temas específicos
1	Vulneración de los sistemas de informáticos de organismos públicos y privados.	✓ Organizaciones que buscan ejercer control y presión mediante el uso del ciberespacio. ✓ Grupos de poder adversarios al Estado y las FFO que ejercen presión para obtener información de carácter sensible o generar efectos disruptivos premeditados. ✓ Entidades de Inteligencia que buscan y explotan información a través de ciberoperaciones.
2	Vulneración de los sistemas informáticos que soportan las capacidades nacionales, la soberanía y la seguridad nacional	✓ Cibercriminalidad. ✓ Ciberactivismo. ✓ Hacktivismo. ✓ Ciberespionaje. ✓ Cibersabotaje. ✓ Ciberterrorismo.
3	Vulneración de los derechos digitales de los ciudadanos.	✓ Manipulación de información. ✓ Fraude digital. ✓ Robo de información e identidad. ✓ Interrupción de servicios básicos. ✓ Intervención de comunicaciones digitales

Figura 17: Amenazas identificadas por la dirección
Fuente: Dirección de informaciones

2.4.8. Controles de seguridad de información

Los controles de seguridad de información identificados en la dirección son mínimas que no aplican ninguna metodología de análisis para la identificación de amenazas, vulnerabilidades y el riesgo, éste último involucra también la identificación de activos críticos para la evaluación correspondiente.

- Directiva N° 058-16- EP– Medidas de Seguridad.
- Directiva N° 27658/b-5 Nov 2017 Seguridad Militar.
- Directiva N° 32142/b-3 Mar 2018 Adopción de Medidas de Seguridad.
- Manual de seguridad 38-10 EP.
- Orden interna N° 1429/DIE/03.03 Sobre ataques informáticos.
- Orden interna N° 25357/DIE/a.03 de Abr 18 cumplir con disposiciones del CCFFAA en seguridad militar.
- Orden interna N° 25356/DIE/a.03 de 25 Feb 18 disposiciones de seguridad de información del CCFFAA.
- Orden interna N° 322255/b-3 del 03 Abr 18 Adopción de medidas de seguridad para regular la publicación de información sensible de documentos, videos, fotos y otros en las redes sociales.
- FAX N° 14473/B-7/03 del 12 Ene 18 Adopción de medidas de seguridad con los equipos informáticos.
- Orden interna N° 31771/a.5 del 15Mar 18 Adopción de medidas de seguridad con los equipos informáticos.
- FAX N° 14475/B-7/03 del 15 Ene18 medidas de seguridad de información sensibles.
- Orden interna N° 31836/b.03 del 30 Feb 18 publicación sensible de información.
- Orden interna N° 31902/b.03 del 07Mar 18 medidas de seguridad para evitar producción de documentación clasificada.
- Directiva N° 001/CGE/03 del 11Ene 18 medidas de seguridad de información sensible.

Por consiguiente, podemos afirmar que se han identificado en total catorce (14) controles relacionados a la seguridad de información de la dirección; además, se pude indicar que las directivas, orden interna, FAX y manuales tienen sus propios procesos de elaboración sin contar con una metodología o bases internacionales respecto a SEGURIDAD DE INFORMACIÓN.

Para establecer y determinar los controles específicos de la dirección, en la

presente investigación se emplea la siguiente formula:

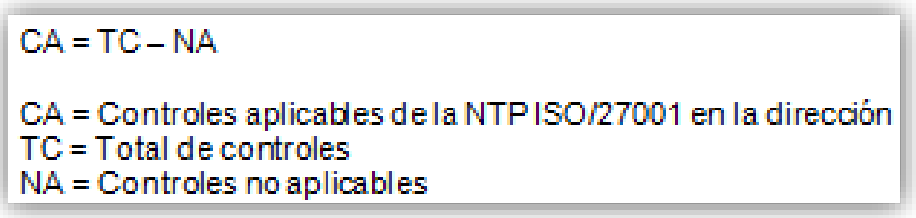


Figura 18: Fórmula para determinar controles de la NTP ISO/IEC 27001
Fuente: Elaboración propia

Fórmula que se aplica en la presente investigación para determinar los controles implementados por la dirección, las mismas que establecen los parámetros de seguridad de la información.

III. MÉTODOS Y MATERIALES

3.1. Hipótesis de la investigación

3.1.1. Hipótesis general

La implementación de un sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 permite mejorar el proceso de seguridad de la información en el Ejército del Perú.

3.1.2. Hipótesis específicas

H_1. La identificación de activos críticos aplicando la NTP ISO/IEC 27001, mejora el proceso de seguridad de la información en el Ejército del Perú.

H_2. La identificación oportuna de riesgos aplicando la NTP ISO/IEC 27001 permite mejorar el proceso de la seguridad de la información en el Ejército del Perú.

H_3. Los controles del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 permiten mejorar el proceso de la seguridad de la información en el Ejército del Perú.

3.2. Variables de estudio

3.2.1. Variable independiente

Sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001.

El Sistema de Gestión de Seguridad de la Información (SGSI) aplicando la NTP ISO/IEC 27001, se define como “un conjunto de políticas, procedimientos, directrices, recursos asociados y actividades, gestionadas colectivamente por una organización, en la búsqueda de la protección de activos críticos de una organización como es la información. El SGSI permite establecer, implementar,

operar, monitorear, revisar, mantener y mejorar la seguridad de información de una determinada organización para alcanzar los objetivos establecidos". (ISO/IEC27000: 2014).

3.2.2. Variable dependiente:

Procesos de seguridad de información.

Sobre el particular Núñez, Vélez y Bérdugo, (2004) señalan que "la metodología de mejora de procesos aplicada está basada en modelos de excelencia, el enfoque de gestión por procesos y el gestión de calidad, cuyos modelos tienen como principal objetivo orientar a las empresas en la búsqueda constante del perfeccionamiento, por lo cual se constituyen en guías prácticas que las ayudan a mejorar y crear una cultura de calidad, midiendo en qué punto se encuentran dentro del camino de la excelencia".

Para el trabajo de investigación se optó por la IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NTP/ISO 27001 PARA MEJORAR EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO DEL PERÚ, considerando la vigencia de la Norma Técnica Peruana sobre seguridad de la información en las instituciones del estado y con mayor razón en una institución que se encarga de administrar información clasificada y relacionada a la Seguridad Nacional respecto de actores internos y externos como el terrorismo nacional e internacional respectivamente.

3.2.3. Operacionalización de la variable

VARIABLES	DIMENSIONES	INDICADORES	ITEMS/ FORMULA	ESCALA DE MEDICION	INSTRUMENTO
I: SISTEMA DE GESTION DE SEGURIDAD DE INFORMACION APLICANDO LA NTP ISO/IEC 27001	SGSI	Activos	¿La organización cuenta con información de activos críticos? ¿La organización cuenta con información de análisis de riesgo de los activos críticos? ¿La entidad cuenta con personal capacitado para realizar análisis de riesgos? ¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo? ¿Se han definido acciones para establecer niveles de riesgo? ¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos? ¿Existe algún software para la gestión de incidentes? ¿Se cuenta con personal capacitado para la gestión de incidentes? ¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto? ¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red? ¿Los encargados de Auditoría llevaron a cabo revisiones de seguridad en el pasado? ¿Los encargados de Auditoría participan en la elaboración de los planes de mejora? ¿Area de Auditoría tiene personal capacitado para llevar adelante las auditorías técnicas? ¿Existe planificación para realizar auditorías con el fin de controlar el SGSI? ¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control? ¿Se han documentado las mejoras en la organización? ¿Existe una planificación para establecer políticas de seguridad de la información en la organización? ¿Las políticas y procedimientos están documentados? ¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)? ¿Los encargados de TI participan en la elaboración de los planes de mejora?	Si/No	ENCUESTA
		Riesgos			
		Controles			
D: PROCESOS DE SEGURIDAD DE LA INFORMACIÓN	Identificación de activos	Tiempo de identificación de activos	$TIA = DR_t + PT_t + AP_t + ET_t + EA_t + RV_t$ TIA= tiempo total del proceso de identificación de activos DR_t= designación de los responsables PT_t= elaboración del plan de trabajo AP_t= aprobación del plan de trabajo ET_t= ejecución del trabajo EA_t= elaboración de acta de activos RV_t= revisión y visto bueno por el director t = tiempo	$\sum_{n=t}^{6} TIA_t$	FICHA DE OBSERVACION
	Gestión de riesgos	Nivel de riesgo	Ri = Pr x Im Ri = Riesgo Pr = Probabilidad Im = Impacto	Ri=Pr x Im	
	Aplicabilidad de controles	Controles de la NTP	CA = TC – NA CA = Controles aplicables de la NTP ISO/27001 en la dirección TC = Total de controles NA = Controles no aplicables	CA =TC -NA	

Figura 19: Cuadro de operacionalización de las variables
Fuente: Elaboración propia

3.3. Diseño de la investigación

3.3.1. Tipo de investigación

La presente investigación tiene por objetivo implementar el sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de seguridad de la información en el Ejército del Perú, en cuyo trabajo de investigación se emplea el tipo de investigación aplicativa y de nivel de investigación explicativa, como señala Hernandez Sampieri, Fernandez Collado y Baptista Lucio (2010) “los estudios explicativos van más allá de la descripción de conceptos o fenómenos; están dirigidos a responder a las causas de los eventos físicos o sociales. Su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se da éste, o por qué dos o más variables están relacionadas”. Las investigaciones explicativas son más estructuradas e implican los propósitos de (exploración, descripción y correlación), además de que proporcionan un sentido de entendimiento del fenómeno a que hacen referencia. Una explicación completa requeriría de otras proposiciones que informaran por qué y cómo están relacionadas esas variables.

3.3.2. Diseño de investigación

Como afirma Espinoza, (2010) “el diseño de investigación es una organización esquematizada para relacionar y controlar las variables de investigación, tiene como objetivo asignar restricciones controladas a las observaciones de los fenómenos”. De lo cual podemos deducir que el diseño de investigación sirve como un instrumento de dirección en apoyo al investigador, estableciendo las acciones a seguir para encontrar posibles soluciones a los problemas.

También señala Espinoza, (2010) cuando en una investigación se necesita manipular variables, es necesario realizar un diseño experimental, que sirve para organizar la obtención de datos a partir de la reproducción de las propiedades del objeto de investigación en un modelo o en un prototipo. Según el grado de control

que se tenga de las variables se puede dividir en investigación:

- Pre-experimental,
- Cuasi-experimental y
- Experimental.

En este tipo de diseños se utilizan signos y símbolos que hacen más simple y comprensible el diseño:

X: Tratamiento experimental, para varios experimentos X1, X2.

O: Observación o medición, para varias observaciones O1, O2.

En la presente investigación se aplica el diseño pre-experimental, que son diseños que no pueden controlar los factores que influyen contra la validez interna y externa, pero ilustran la forma en que las variables extrañas pueden influir en la validez interna. Este tipo de diseño se desarrolla la pre y post prueba:

Diseño de un grupo con pre prueba y post prueba

Se evalúa los efectos del tratamiento comparándolo con una medición previa, su diseño es:

O1 → X → O2

X: Tratamiento aplicado al grupo experimental (VI).

O1: Observación de la variable dependiente antes de tratamiento.

O2: Observación de la variable dependiente después de tratamiento.

Diseño de un grupo con post prueba

Se evalúa los efectos del tratamiento, su diseño es:

X → O

X: Tratamiento aplicado al grupo experimental.

O: Observación de los efectos mediante una post prueba.

3.4. Población y muestra de estudio

3.4.1. Población

Según Arias, (2012) señala que “en términos más precisos es la población objetivo, es un conjunto finito de elementos con características comunes para los

cuales serán extensivas las conclusiones del trabajo de la investigación. Ésta queda delimitada por el problema y por los objetivos del estudio". En el caso particular de la presente investigación se cuenta con población finita y accesible en donde realmente se tiene acceso y de la cual se extrae la muestra. La población objetivo queda delimitada con claridad y precisión en el problema de investigación en este caso la interrogante formulada y en el objetivo general del estudio. Es decir, se especifican los sujetos o elementos que serán analizados en la investigación y a los que se pretende hacer inferencias a partir de la muestra.

Es por ello que esta investigación se desarrolla con la población del Ejército del Perú, con sede administrativa ubicada en el Jirón Boulevard S/N – San Borja - Lima, con 350 empleados de la dirección.

3.4.2. Muestra

Siendo la muestra un subgrupo de la población de interés de donde se recolectan datos, para tener mayor accesibilidad para recabar la información, se estima realizar la investigación en un área específica de la Dirección de Informaciones del Ejército del Perú, vale decir 38 empleados del área TI de la dirección en mención.

3.5. Técnicas e instrumentos de recolección de datos

3.5.1. Técnicas de recolección de datos

Según Arias, (2012) "existen diferentes técnicas de recolección de datos, distintas formas, procedimientos formas particulares de obtener datos o información. Entre ellos tenemos la observación directa, la encuesta en sus dos modalidades (oral o escrita), la entrevista, el análisis documental, análisis de contenido, etc.".

En la presente investigación se utilizará la técnica de la encuesta y fichas observación, métodos de investigación que nos permitirán requerir datos a un grupo de personas que están involucradas con el tema de estudio y que nos

permitirán acceder a la información de manera directa y de fuente primaria. En este sentido, se aplicó la técnica de encuesta con un cuestionario compuesto por 20 preguntas cerradas, por otra parte se emplea la ficha de observación para obtener datos e información de la Dirección de Informaciones del Ejército del Perú – San Borja – Lima.

3.5.2. Instrumentos de recolección de datos

Observación

Es un método para reunir datos sobre el objeto de investigación, con el fin de elaborar información sobre su funcionamiento. La observación se realiza utilizando nuestros sentidos y utilizando instrumentos que amplían nuestros sentidos. Según Heinemann (2003) “La observación científica es la captación previamente planeada y el registro controlado de datos con una determinada finalidad para la investigación, mediante la percepción visual o acústica de un acontecimiento”.

Proceso de observación

El proceso de observación se realiza sobre el objeto, materia de investigación para lo cual se parte de un marco conceptual que contiene la información conocida sobre el objeto, capacitación del observador para lograr una mejor comprensión del objeto, permite construir o seleccionar los instrumentos y tecnologías que ayudarán a medir las propiedades del objeto a investigar. El producto de la observación son los datos.

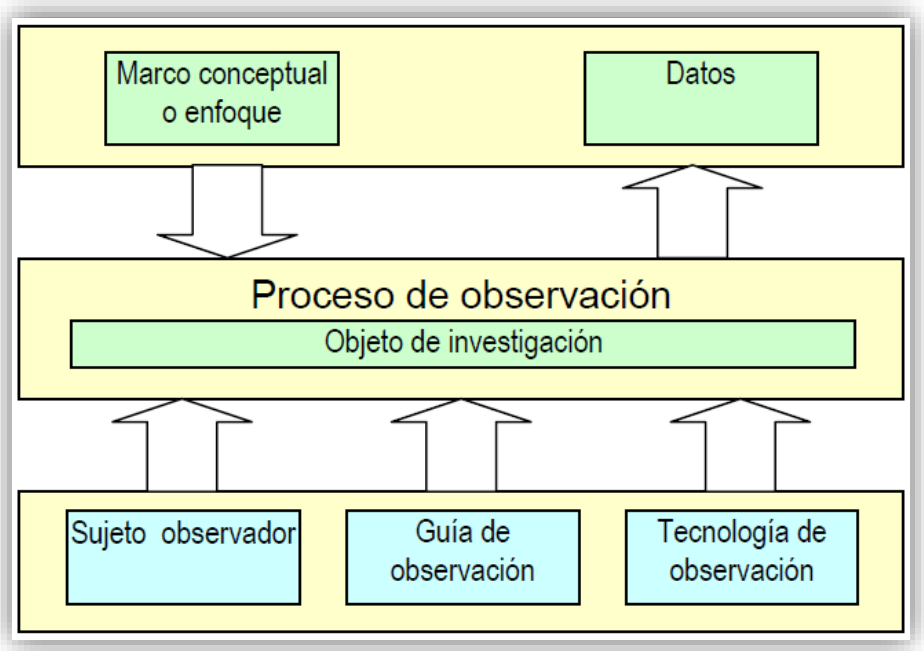


Figura 20:Proceso de observación
Fuente: Espinoza (2010)

También en la presente investigación se utiliza el instrumento de encuesta que según Espinoza, (2010) “es aquella técnica que permite obtener información de primera mano para describir o explicar un problema, aplicándose a una muestra representativa de una determinada población”. Para esta investigación se aplica pre-encuesta y post encuesta es decir antes y después de la implementación del sistema de gestión de seguridad de la información aplicando al NTP ISO/IEC 27001 para mejorar procesos de seguridad de la información en el Ejército del Perú, con el fin de minimizar riesgos de fuga de información.

3.5.3. Validación y confiabilidad del instrumento

Tabla 11

Validación de expertos

Tabla 11: Validación de expertos

Mgtr. Ing. Edmundo Barrantes Ríos	Experto Temático
Mgtr. Ing. Christian Ovalle Paulino	Experto Metodólogo

Fuente: Elaboración propia

3.5.4. Confiabilidad del instrumento por Alfa de Cron Bach

Tabla 12: Fiabilidad de instrumento por Alfa Cron Bach

Alfa de Cronbach	Alfa de Cronbach basada en los elementos tipificados	N° de elementos
96.86%	97.10%	20 preguntas

Fuente: Elaboración propia del autor

3.5.5. Métodos de análisis de datos

Para la presente investigación los datos recolectados fueron ingresados en una matriz de hoja de cálculo del programa de SPSS v22.0.0.0 (ver tabla 21, 22, 23, 24, 25 y 26) donde ha sido procesado la información; posteriormente, fueron tabulados en el programa de Microsoft Office Excel 2010 (ver tabla 20, 21,22 y 23) para su mejor análisis y comprensión del problema de investigación. Se ha realizado el proceso de análisis de los factores que intervienen en la fuga de información de la Dirección de Informaciones del Ejército del Perú. Para el proceso de análisis de identificación de activos críticos de la dirección se ha empleado la ficha de observación pre y post implementación del sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001.

También se ha aplicado la matriz de riesgos para la evaluación de amenazas y vulnerabilidades que intervienen la gestión del riesgo, para lo cual se ha establecido valores cualitativos y cuantitativos respecto al impacto y probabilidad de materialización de las amenazas que podrían poner en riesgo la seguridad de la información de la dirección.

3.5.6. Aspectos deontológicos

Según Jeremy Bentham, la deontología se puede considerar como una teoría ética que se ocupa de regular los deberes, traduciéndolos en preceptos, normas morales y reglas de conducta que consisten en hacer en cada ocasión lo que es recto y apropiado. Cuando esta teoría se aplica al estricto campo profesional hablamos de deontología profesional; en consecuencia, la que determina los deberes que son mínimamente exigibles a los profesionales en el desempeño de

su actividad, siendo plasmados códigos de ética que rigen la actuación de los colegiados con el fin de los profesionales obtengan resultados deseables.

En tal sentido, considero que como profesional en servicio a la sociedad y a la patria, prima en mí la honestidad y la sinceridad para considerar los derechos de autor en el presente trabajo de investigación.

También, el presente trabajo de investigación se desarrolla en el marco normativo se siguen lineamientos emitidos por el MINDEF (Ministerio de Defensa), EP (Ejército del Perú) y otros del ámbito de la dirección.

Razón por la cual se siguieron las normas éticas al realizar el presente trabajo de investigación pre experimental bajo las directrices en cuanto a normas para la elaboración de esta investigación y respetando los derechos de autor en cuanto a investigaciones referenciadas.

IV. RESULTADOS

4.1. Resultados de encuesta de la implementación del sistema de gestión de seguridad de la información.

En la encuesta realizada al personal de la dirección se ha obtenido los siguientes resultados:

Tabla 13: Encuesta de SGSI - Pre implementación

Sistema de Gestión seguridad de la Información – Pre	Frecuencia	Porcentaje
Si	12	31.6
No	26	68.4
Total	38	100.0

Fuente: Elaboración propia

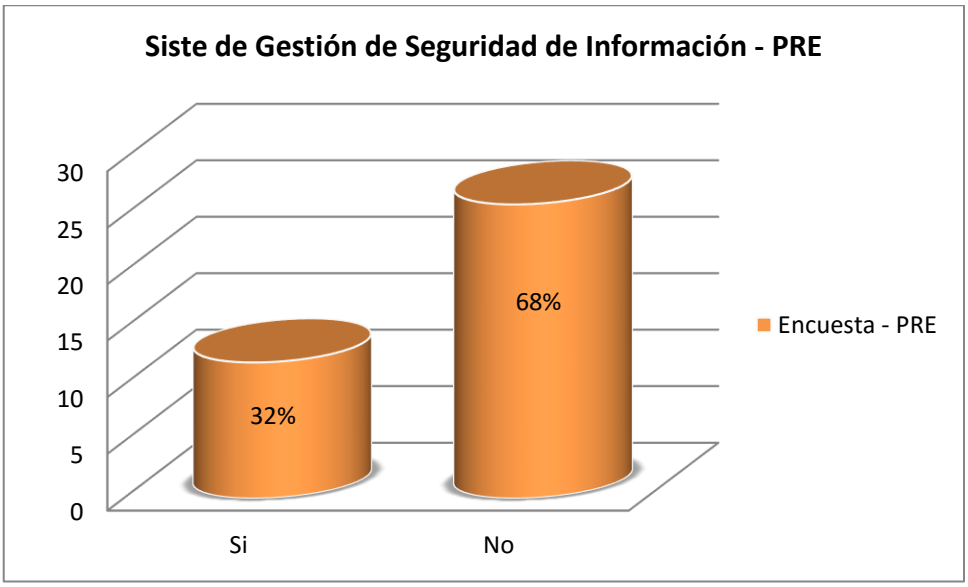


Figura 21: Cuadro estadístico antes de implementación del SGSI
Fuente: Elaboración propia

De los resultados obtenidos, se observa que de los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, 12 opinan que cuentan con información del Sistema de Gestión de seguridad de Información que representa el 32%, mientras que 26 afirman que no cuentan con SGSI que representa el 68% de los encuestados de la dirección.

Tabla 14: Encuesta de SGSI - Post implementación

Sistema de Gestión seguridad de la Información - Post	Frecuencia	Porcentaje
Si	38	100.0
No	0	0
Total	38	100.0

Fuente: Elaboración propia

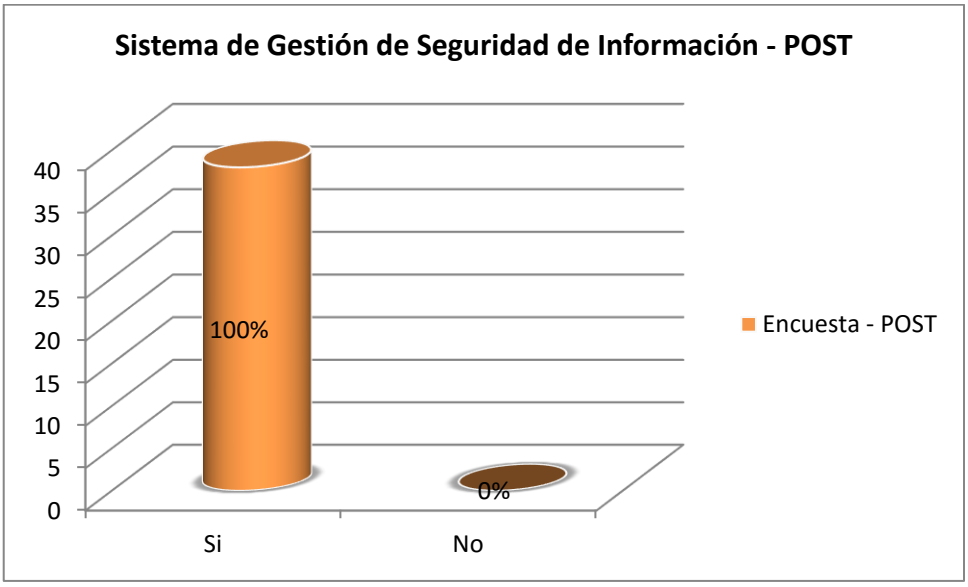


Figura 22: Cuadro estadístico después de la implementación del SGSI
Fuente: Elaboración propia

De los resultados obtenidos, se observa que los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, es decir el 100% opinan que el sistema de gestión de seguridad de la información mejora aplicando la NTP ISO/IEC 27001, la misma que en porcentaje.

Tabla 15: Identificación de activos-Pre implementación

Identificación de activos - Pre	Frecuencia	Porcentaje
Si	12	31.6
No	26	68.4
Total	38	100.0

Fuente: Elaboración propia

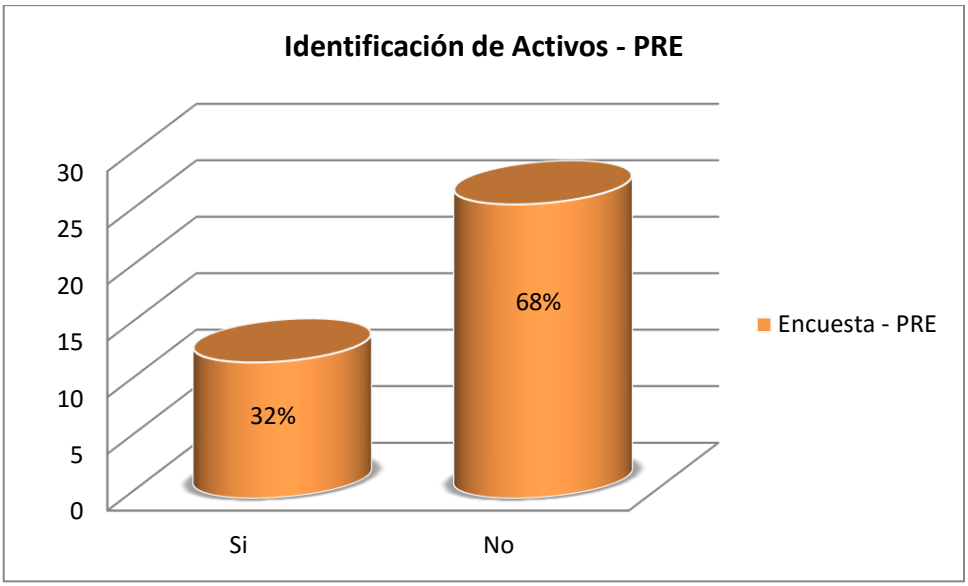


Figura 23: Identificación de activos de información
Fuente: Elaboración propia

De los resultados obtenidos, se observa que de los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, 12 opinan que cuentan con información de identificación de activos, que representa el 32% de los encuestados, de otro parte 26 afirman que no cuentan con información de identificación de activos críticos, lo que representa el 68%.

Tabla 16: Identificación de activos - Post implementación

Identificación de activos – Post	Frecuencia	Porcentaje
Si	38	100.0
No	0	00.0
Total	38	100.0

Fuente: Elaboración propia

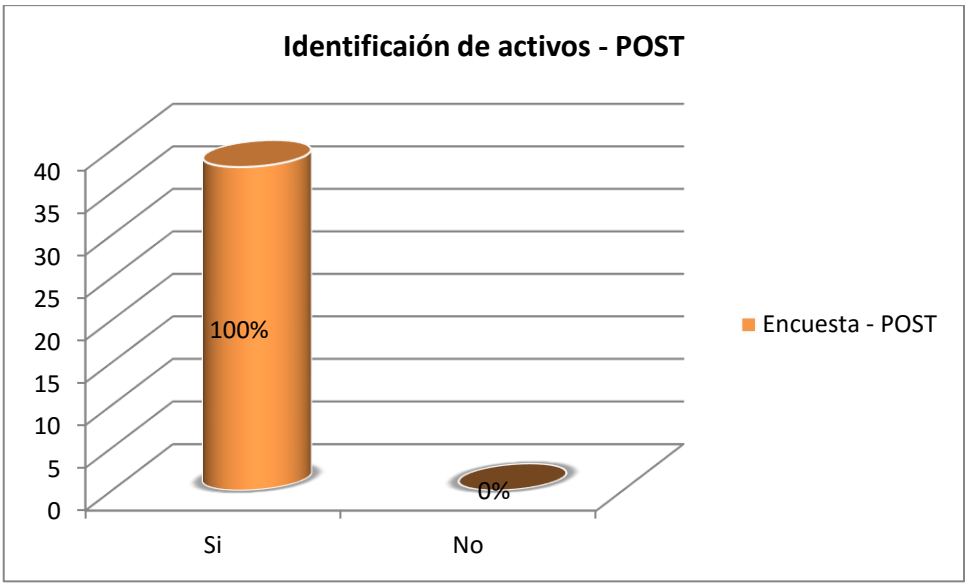


Figura 24: Identificación de activos críticos
Fuente: Elaboración propia

De los resultados obtenidos, se observa que los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, opinan que la identificación de activos mejora aplicando la NTP ISO/IEC 27001, representando el 100% de opinión favorable.

Tabla 17: Gestión de riesgo-Pre implementación

Gestión de Riesgos - Pre	Frecuencia	Porcentaje
Si	14	36.8
No	24	63.2
Total	38	100.0

Fuente: Elaboración propia

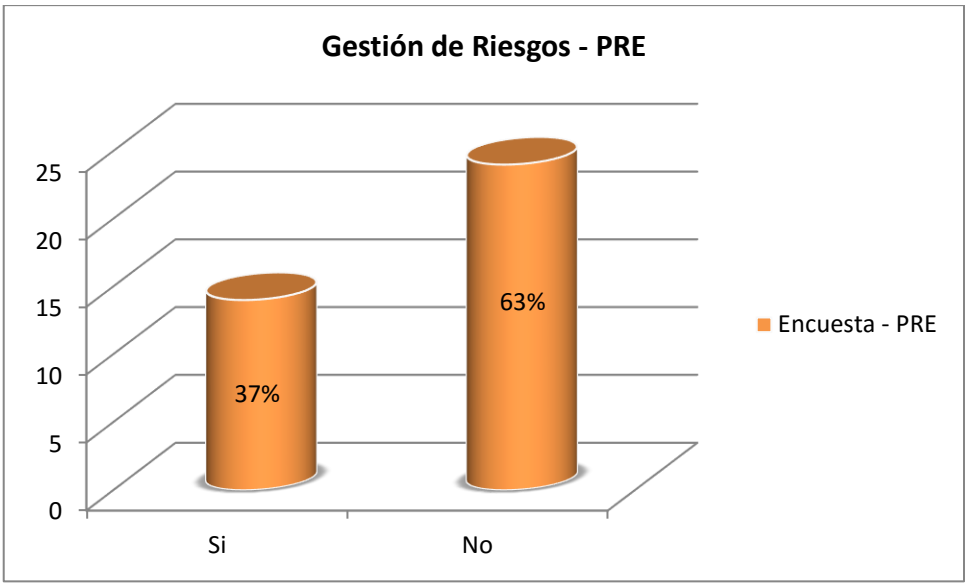


Figura 25: Gestión de riesgos antes de la implementación del SGSI
Fuente: Elaboración propia

De los resultados obtenidos, se observa que de los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, 14 opinan que cuentan con información de gestión de riesgos, representado en 37% que opina sobre gestión de riesgos en la dirección; mientras que 24 opinan que no cuentan con información de gestión riesgos en la dirección lo que representa el 63%.

Tabla 18: Gestión de riesgo-Post implementación

Gestión de Riesgos - Post	Frecuencia	Porcentaje
Si	38	100.0
No	0	00.0
Total	38	100.0

Fuente: Elaboración propia

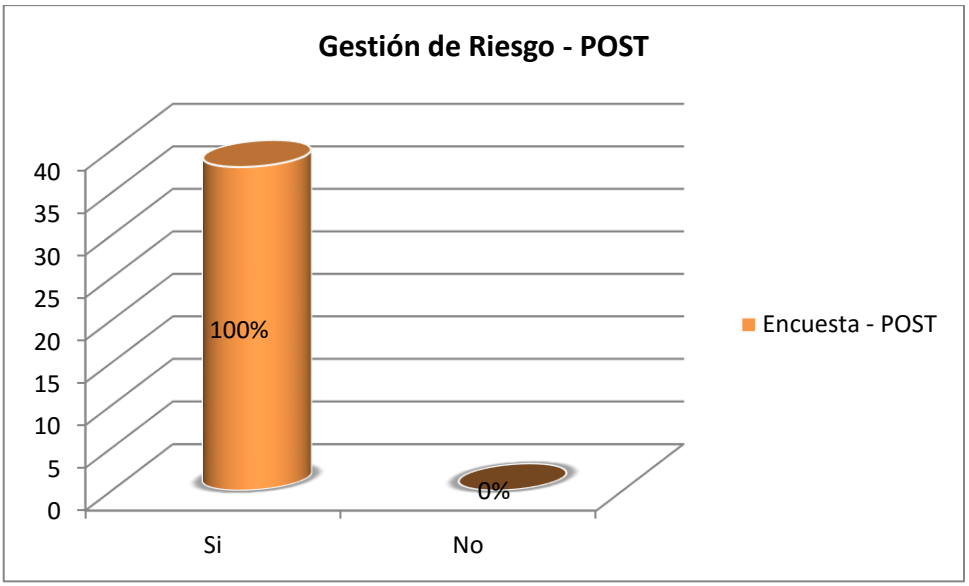


Figura 26: Cuadro estadístico después de la implementación del SGSI
Fuente: Elaboración propia

De los resultados obtenidos, se observa que los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, opinan que la gestión de riesgos mejora aplicando la NTP ISO/IEC 27001, es decir el 100% tiene opinión favorable sobre la gestión de riesgos implementado para mejorar el proceso de seguridad de información en la dirección.

Tabla 19: Controles de la NTP ISO/IEC 27001 - Pre implementación

Controles NTP ISO/IEC 27001– Pre	Frecuencia	Porcentaje
Si	0	0
No	38	100.0
Total	38	100.0

Fuente: Elaboración propia

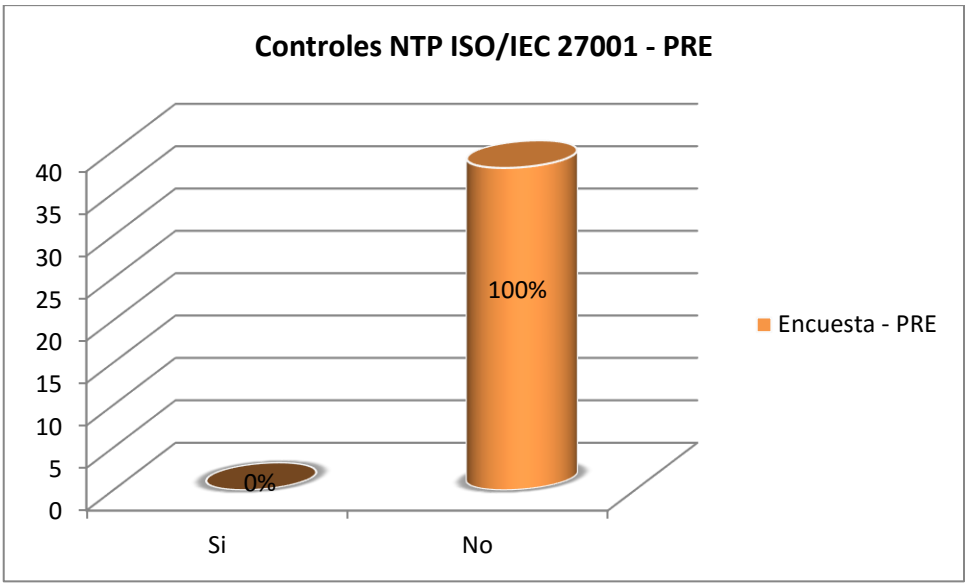


Figura 27: Controles de la NTP ISO/IEC 27001
Fuente: Elaboración propia

De los resultados obtenidos, se observa que los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, opinan que NO cuentan con información de controles del SGSI, es decir que el 100% de los encuestados afirman que no tienen implementado los controles de la Norma Técnica Peruana ISO/IEC 27001.

Tabla 20: Controles de la NTP ISO/IEC 27001

Controles NTP ISO/IEC 27001 – Post	Frecuencia	Porcentaje
Si	31	81.6
No	7	18.4
Total	38	100.0

Fuente: Elaboración propia

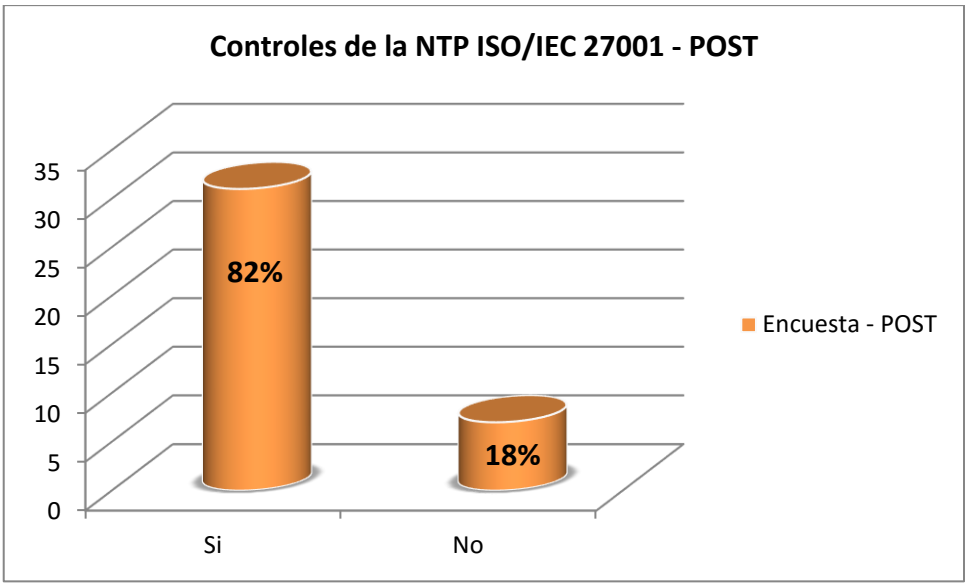


Figura 28: Controles de la NTP ISO/IEC 27001
Fuente: Elaboración propia

De los resultados obtenidos, se observa que de los 38 encuestados de la Dirección de Informaciones del Ejército del Perú, 31 opinan que la implementación de los controles aplicando la NTP ISO/IEC 27001, mejora el proceso de control de seguridad de información en la dirección lo que representa el 82% que opinan que la implementación de los controles de acuerdo a la norma técnica peruana de ISO/IEC 27001 mejora los controles relacionados con la seguridad de información en la dirección y el 18% opina que lo contrario, ello por falta de capacitación por lo que se sugiere a la dirección realizar la capacitación debida.

4.2. CONTRASTACIÓN DE HIPÓTESIS

4.2.1. HIPÓTESIS GENERAL

La implementación del sistema de gestión de seguridad de la información aplicando la NTP/ISO 27001 mejora el proceso de seguridad de la información en el Ejército del Perú.

Prueba de Hipótesis:

Ho: la proporción de la implementación del sistema de gestión de seguridad de la información es igual a la proporción de la implementación del sistema de gestión de seguridad de la información aplicando la NTP/ISO 27001, (Post.).

Ha: la proporción de la implementación del sistema de gestión de seguridad de la información es diferente a la proporción de la implementación del sistema de gestión de seguridad de la información aplicando la NTP/ISO 27001, (Post.).

Nivel de significancia: α = 0.05

Prueba estadística:

Tabla 21: Estadística de grupo de factor de sistema de seguridad

	Factor Sistema de Seguridad	N	proporción	Desviación estándar	Media de error estándar
Sistema de Seguridad	Sistema de Seguridad Post	38	1,00	,000	,000
	Sistema de Seguridad Pre	38	,32	,471	,076

Fuente: Elaboración propia

Tabla 22: Prueba de muestra independiente de varianzas

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	Gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Sistema de Seguridad	Se asumen varianzas iguales	235,592	,000	8,954	74	,000	,684	,076	,532	,836
	No se asumen varianzas iguales			8,954	37,000	,000	,684	,076	,529	,839

Fuente: Elaboración propia

Criterio de decisión:

Como Sig. es igual a 0.000, en la prueba de Levene, se concluye que las varianzas no son iguales. Por lo tanto en la prueba t, como sig. (bilateral) es 0.000, se rechaza la hipótesis nula.

A un nivel de significación del 5% existe evidencia estadística para concluir que la proporción de la implementación del sistema de gestión de seguridad de la información es diferente a la proporción de la implementación del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001.

Por lo tanto se concluye que la implementación del sistema de gestión de seguridad de la información **sí mejora** el proceso de seguridad de la información en el Ejército del Perú, aplicando la NTP ISO/IEC 27001.

4.3. HIPÓTESIS ESPECÍFICAS

Hipótesis Especifica 1: La identificación de activos críticos aplicando la NTP ISO/IEC 27001 mejora el proceso de la seguridad de la información en el Ejército del Perú.

Prueba de Hipótesis:

Ho: La proporción de la identificación de activos críticos es igual a la proporción de la identificación de activos críticos aplicando la NTP ISO/IEC 27001.

Ha: La proporción de la identificación de activos críticos es diferente a la proporción de la identificación de activos críticos aplicando la NTP ISO/IEC 27001.

Nivel de significancia: α = 0.05

Prueba estadística:

Tabla 23: Estadística de grupo de activos críticos

	Factor Activos críticos	N	Porporcion	Desviación estándar	Media de error estándar
Activos críticos	Activos críticos Post	38	1,00	,000	,000
	Activos críticos - Pre	38	,32	,471	,076

Fuente: Elaboración propia

Tabla 24: Prueba de muestras independientes varianzas de activos críticos

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	T	Gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Activos críticos	Se asumen varianzas iguales	235,592	,000	8,954	74	,000	,684	,076	,532	,836
	No se asumen varianzas iguales			8,954	37,000	,000	,684	,076	,529	,839

Fuente: Elaboración propia

Criterio de decisión:

Como Sig. es igual a 0.000, en la prueba de Levene, se concluye que las varianzas no son iguales. Por lo tanto en la prueba t, como sig. (bilateral) es 0.000, se rechaza la hipótesis nula.

A un nivel de significación del 5% existe evidencia estadística para concluir que La proporción de la identificación de activos críticos es diferente a la proporción de la identificación de activos críticos aplicando la NTP ISO/IEC 27001.

Por lo tanto se concluye que la identificación de activos críticos mejora el proceso de seguridad de la información en el Ejército del Perú, aplicando la NTP ISO/IEC 27001.

Hipótesis especifica 2: La identificación oportuna de riesgos aplicando la NTP ISO/IEC 27001 mejora el proceso de seguridad de la información en el Ejército del Perú,

Prueba de Hipótesis:

Ho: La proporción de la identificación de riesgos es igual a la proporción de la identificación de riesgos aplicando la NTP ISO/IEC 27001.

Ha: La proporción de la identificación de riesgos es diferente a la proporción de la identificación de riesgos aplicando la NTP ISO/IEC 27001.

Nivel de significancia: α = 0.05

Prueba estadística:

Tabla 25: Estadística de grupo de gestión de riesgo

	Factor_Gestion_Riesgo	N	Proporción	Desviación estándar	Media de error estándar
Gestión_Riesgo	Gestión de riesgos Post	38	1,00	,000	,000
	Gestion de riesgos – Pre	38	,37	,489	,079

Prueba de muestras independientes

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	T	Gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Gestión_Riesgo	Se asumen varianzas iguales	497,280	,000	7,964	74	,000	,632	,079	,474	,790
	No se asumen varianzas iguales			7,964	37,000	,000	,632	,079	,471	,792

Fuente: Elaboración propia

Criterio de decisión:

Como Sig. es igual a 0.000, en la prueba de Levene, se concluye que las varianzas no son iguales. Por lo tanto en la prueba t, como sig. (bilateral) es 0.000, se rechaza la hipótesis nula.

A un nivel de significación del 5% existe evidencia estadística para concluir que La proporción de la identificación de riesgos es diferente a la proporción de la identificación de riesgos aplicando la NTP ISO/IEC 27001, (Post.).

Por lo tanto se concluye que la identificación oportuna de riesgos mejora los procesos de seguridad de la información en el Ejército del Perú, aplicando la NTP ISO/IEC 27001.

Hipótesis especifico 3: Los controles del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 mejoran el proceso de la seguridad de la información en el Ejército del Perú.

Prueba de Hipótesis:

Ho: La proporción de Los controles del sistema de gestión de seguridad de la información es igual a la proporción de Los controles del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001, (Post.).

Ha: La proporción de Los controles del sistema de gestión de seguridad de la información es diferente a la proporción de Los controles del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001, (Post.).

Nivel de significancia: α = 0.05

Prueba estadística:

Tabla 26: Estadística de grupo de factor controles

	Factor Control	N	Media	Desviación estándar	Media de error estándar
Controles	Controles Post	38	,82	,393	,064
	Controles Pre	38	,00	,000	,000

Fuente: Elaboración propia

Tabla 27: Prueba de muestras independientes de factor controles

		Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias						
									95% de intervalo de confianza de la diferencia	
		F	Sig.	t	Gl	Sig. (bilateral)	Diferencia de medias	Diferencia de error estándar	Inferior	Superior
Controles	Se asumen varianzas iguales	55,757	,000	12,801	74	,000	,816	,064	,689	,943
	No se asumen varianzas iguales			12,801	37,000	,000	,816	,064	,687	,945

Fuente: Elaboración propia

Criterio de decisión:

Como Sig. es igual a 0.000, en la prueba de Levene, se concluye que las varianzas no son iguales. Por lo tanto en la prueba t, como sig. (bilateral) es 0.000, se rechaza la hipótesis nula.

A un nivel de significación del 5% existe evidencia estadística para concluir que La proporción de Los controles del sistema de gestión de seguridad de la información es diferente a la proporción de Los controles del sistema de gestión de seguridad de la información aplicando la NTP ISO7IEC 27001.

Por lo tanto se concluye que Los controles del sistema de gestión de seguridad de la información mejoran el proceso de la seguridad de la información en el Ejército del Perú, aplicando la NTP ISO/IEC 27001.

V. DISCUSIÓN

5.1. Análisis de discusión de resultados

La investigación realizada tiene como objetivo principal establecer la Implementación del Sistema Gestión de Seguridad de Información aplicando la NTP ISO/IEC 27001 para mejorar los procesos de seguridad de información en el Ejército del Perú, en cumplimiento de la Resolución Ministerial Nº 004-2016-PCM, que fue aprobada y es de aplicación obligatoria por entidades del estado. En efecto el investigador Javier Alfonso Seclén Arana de la UNMSM, al concluir su trabajo de investigación sobre 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 concluye que ha encontrado ocho categorías que afectan la implementación del SGSI distribuidos en tres niveles (Estratégico, Operativo y Técnico) en el nivel técnico identificó “contar con un presupuesto nacional para la seguridad de la información”, de acuerdo a la presente investigación y análisis, un presupuesto nacional correspondería a un nivel estratégico, pero eso sí, dicho presupuesto debe estar orientado a la capacitación en temas de identificación de activos, gestión de riesgos, implementación de controles, todo ello en base a la NTP-ISO/IEC 27001 que promueve y regula a través de la ONGEI la implementación del sistema de gestión de seguridad de la información (SGSI) en las entidades públicas y privadas del país.

En esta parte del capítulo podemos afirmar que durante la investigación se ha desarrollado el contexto de la organización en donde se detalla de cómo la dirección de informaciones realiza el PLAN DE SEGURIDAD, en dicho plan se hace el análisis orientado a seguridad física, involucrando otros campos de seguridad como el de armamento, de accidentes, desastres naturales, entre otros que no favorecen adecuadamente en los procesos de gestión de riesgos de seguridad de información. Por ello, se plantea mejorar en específico el proceso de la seguridad de informaciones aplicando la NTP-ISO/IEC 27001 que permita plantear políticas de seguridad de la información previa identificación de activos, riesgos y amenazas que afectan el desarrollo normal de las actividades y en

cumplimiento de los objetivos trazados.

Los controles aplicados de acuerdo a la verificación y registro (directivas, fax, orden interna, y reglamentos) no son suficientes, carentes de metodología y procesos establecidos que permitan el adecuado cumplimiento de las políticas de control interno; frente a ello se ha planteado los controles propuestos por la NTP ISO/IEC 27001 estableciendo controles de acuerdo a la aplicabilidad de los mismos a la dirección.

El factor humano es algo que la dirección debería tener en cuenta, pues de ello depende mucho el correcto funcionamiento y manejo del sistema de información, ello debido a la alta rotación del personal en los puestos donde se requiere personal con alta formación, conocimiento y capacitación en temas de seguridad de información que pueda garantizar (confidencialidad, integridad y disponibilidad) la adecuada administración de información clasificada de la dirección.

VI. CONCLUSIONES

En relación con el objetivo general de este trabajo de investigación, se concluye que; la implementación del Sistema de Gestión de Seguridad de Información aplicando la NTP ISO/IEC 27001, mejora los procesos de seguridad de información en el Ejército del Perú, garantizando la confidencialidad, integridad y disponibilidad. Los procesos que se aplican de acuerdo al ciclo Deming Plan-Do-Check-Act (PDCA) permiten el desarrollo y la mejora continua.

La identificación de activos aplicando la NTP ISO/IEC 27001, permite a la dirección realizar el análisis adecuado de los activos críticos de seguridad de información, al identificar los activos críticos respecto a la administración propia de la seguridad de la información, permitiendo que los procesos para identificar los activos sean claros y precisos.

La gestión de riegos aplicando la metodología de gestión de riesgos, permite evaluar, analizar y valorar cualitativa y cuantitativamente los riesgos permitiendo la identificación y el grado de impacto que pueden ocasionar en cuanto se materialicen las amenazas, afectando la imagen institucional y la seguridad nacional.

La implementación de los controles de acuerdo a la NTP ISO/IEC 27001, permiten el desarrollo integral de políticas de seguridad de información en la dirección, por lo que se concluye que también mejoran los procesos de seguridad de información en compatibilidad de la implementación de gestión por procesos del Ejército.

Frente al factor humano la dirección debe evaluar personal con capacidad y altos conocimientos en seguridad de información para cubrir los puestos claves de área TI de la dirección y evitar la rotación permanente del personal.

VII. RECOMENDACIONES

Recomendaciones luego de la presente investigación son las siguientes:

Es de gran importancia la implementación del sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001 que permita la mejora en el proceso de seguridad de información en la dirección. También se recomienda la capacitación del personal en cada uno de los procesos implementados.

En relación a los activos críticos de la dirección, se recomienda que en las próximas investigaciones se identifique activos de información a nivel Ejército del Perú en coordinación de la Inspectoría General de Ejército (IGE) para el respectivo control en las inspecciones rutinarias programadas por el comando del Ejército. Asimismo, para la administrar activos e identificar riesgos, amenazas y vulnerabilidades se recomienda el uso de gestión libre del parque informático que facilita en la administración de los activos de la información para la correcta y oportuna toma de decisiones del comando del Ejército respecto a riesgos o amenazas.

Para la gestión de riesgos se recomienda que personal encargado de temas de seguridad puedan tomar de referencia la presente investigación para tener fundamentos sólidos de acuerdo a la NTP-ISO/IEC 27001 que establece pautas generales sobre gestión de riesgo aplicando la metodología del ciclo Deming que consiste en planificar, hacer, verificar y actuar garantizando en la medida de lo posible la confidencialidad, integridad y disponibilidad de la información que es activo crítico principal de la organización.

Se recomienda que los controles implementados como políticas de seguridad de la información en base a la NTP ISO/IEC 27001, debe ser de estricto cumplimiento por parte de todo personal que labora en la institución. Asimismo, se recomienda actualizar las políticas de seguridad de información cada vez que ocurran cambios considerables y obligatoriamente cada año.

REFERENCIAS BIBLIOGRÁFICAS

27000:2014, I. S. (2014). *Information technology — Security techniques — Information security management systems — Overview and.*

27001:2014, I. (20 de Noviembre de 2014). *Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.* Recuperado el 02 de Julio de 2018, de https://www.iso.org/

73:2002, I. G. (20 de Enero de 2002). *Risk Management - Vocabulary - Guidelines four use in standards EEUU.* Recuperado el 05 de Julio de 2018, de https://www.iso.org/

Aguirre Mollehuanca, D. A. (2014). *Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A, Pontificia Universidad Católica del Perú.* Lima.

Alexander, A. G. (2012). Análisis del riesgo y el sistema de gestión de seguridad de la información - El enfoque ISO 27001. *EGP S.A.*, 06.

Aliaga Flores, L. C. (2017). *Diseño de un sistema de gestión de seguridad de la información para un instituto educativo - Pontificia Universidad Católica del Perú.* Lima.

Arias, F. G. (2012). *El proyecto de Investigación - Introducción a la metodología científica.* Caracas: Episteme C.A.

Bojórquez Zapata, M. I., & Pérez Brito, A. E. (2013). La planeación estratégica. Un pilar en la gestión empresarial. *El Buzón de Pacioli*, 55.

Bravo Carrasco, J. (2013). *Gestión de Procesos.* Santiago: Editorial Evolución S.A.

Camisón, C., Cruz, S., & González, T. (2006). *Gestión de la calidad conceptos, enfoques, modelos y sistemas.* Madrid: Pearson Educación S.A.

Contreras Esgerra, L. C. (2017). *Diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para la dirección de*

sistemas de la gobernación de Boyacá, Universidad Nacional de Ciencias Básicas e Ingeniería. Boyacá.

Dominguez Coutiño, L. A. (2012). *Análisis de sistemas de información.* México: Tercer Milenio S.C.

Doria Corcho, A. F. (2015). *Diseño deun sistema de gestión de seguridad de la información mediante la aplicación de lanorma internacional ISO/IEC 27001:2013 en la oficina de sistemas de información y telecomunicaciones de la universidad de Córdoba, Universida Nacional Abierta de C.* Córdoba.

Fernández Peñaloza, D. A., & Pacheco Vargas, O. A. (2014). *Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP - ISO/IEC 27001.* Lima.

Fernández Sánchez, C. M. (2012). La norma ISO 27001 del sistema de gestión de seguridad de la información. *AENOR*, 5.

Figoberto Gonzalo, Ñ. B. (2017). *Plan de seguridad informática para mejorar la gestión de lainformación en la sociedad financiera visionfound-FODEMI de la ciudad de Ibarra, Universidad Regional Autónoma de los Andes.* Ibarra.

Gambetta, M. (2015). Estrategia de capacitación desarrolladas en el entorno corporativo estatal Uruguay. 18.

Heinemann, K. (2003). *Introducción a la metodologia de la investigación empírica en las ciencias.* Barcelona - España: Paidotribo.

Horacio Saroka, R. (2002). *Sistema de información en la era digital.* Argentina.

Leiva. (2015). Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Estrategias Nacionales de Ciberseguridad*, 16.

Martínez P., J., Espinosa T., D., & Amador D., S. (2014). Gestión del riesgo en la seguridad de la información con base en la norma ISO/IEC27005 proponiendo una adaptación de la metodologia OCTAVE-S. *ISSN*, 11.

Mercado Rojas, J. E. (2016). *Modelo de gestión de seguridad de la información para el E-Gobierno, Universidad Nacional Mayor de San Marcos .* Lima.

Murray, p. (2012). Gestión-Información-Conocimiento. *Redalyc*, 12.

Nuñez Sarmiento, L. I., Vélez Ramírez, M., & Berdugo Correa, C. R. (2004). Aplicación de una metodología de mejora de procesos basada en el enfoque de gestión de procesos, en los modelos de excelencia y el QFD en una empresa del sector de confecciones de Barranquilla. *Redalyc*, 16.

ONGEI, O. N. (10 de Julio de 2013). *Decreto Supremo N° 081-2013-PCM.* Recuperado el 01 de Julio de 2018, de diario el peruano: https://elperuano.pe/

Parra Alvernia, H., Contreras Navarro, J., Diaz Pacheco, D. Y., & López Ovalle, E. J. (2015). *Diseño de las políticas de seguridad de la información para la empresa comunitaria de acueducto de Rio de Oro, CESAR "EMCAR", Universidad Francisco de Paula Santander Ocana-OCONA.* Rio de Oro.

PCM, P. d. (08 de Enero de 2016). *Resolución Ministerial 004-2016-PCM.* Recuperado el 01 de Julio de 2018, de www.elperuano.pe/

Sánchez Ruipérez, G. (2011). Diseño e implementación de un sistema de gestión de seguridad de la información. *Fundación Germán Sánchez*, 1-8.

Sclén Arana, J. A. (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 - Universidad Nacional Mayor de San Marcos.* Lima.

Tupia, M. (2009). Principios de auditoría y control de sistemas de información. *Tipia Consultores y Auditores S.A.C*.

Vera Rodriguez, J. M., & Albarracín Calderón, A. P. (2017). Metodología para el análisis de vulnerabilidad ante amenazas de inundación, remosión en masa y flujo torrenciales de cuencas hidrográficas. *Ciencia e ingeniería Neogranadina*, 28.

Villena Aguilar, M. A. (2006). *Sistema de gestión de seguridada de información para una institución financiera, Pontificia Universidad Católica del Perú.* Lima.

ANEXOS

ANEXO 01: MATRIZ DE CONSISTENCIA

"IMPLEMENTACIÓN DE SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NTP ISO/IEC 27001 PARA MEJORAR EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO DEL PERÚ"

PROBLEMA GENERAL	OBJETIVO GENERAL	HIPÓTESIS PRINCIPAL	VARIABLES
¿De qué manera se implementación de un sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 mejorará el proceso de la seguridad de la información en el Ejército del Perú?	Implementar el sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de seguridad de la información en el Ejército del Perú.	La implementación del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 mejora el proceso de seguridad de la información en el Ejército del Perú.	**Variable predictora:** Influencia del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 en la mejora del proceso de la seguridad de la información en el Ejército del Perú. **Variable de criterio:** Mejorar el proceso de la seguridad de la información en una institución del Estado **Variable Independiente:** Sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 **Variable Dependiente** Procesos de la seguridad de la información en el Ejército de Perú.
PROBLEMAS ESPECÍFICOS	**OBJETIVOS ESPECÍFICOS**	**HIPÓTESIS ESPECÍFICOS**	
1) ¿De qué manera la identificación de activos críticos aplicando la NTP ISO/IEC 27001 mejorará el proceso de la seguridad de la información en el Ejército del Perú?	1) Identificar activos críticos aplicando la NTP ISO/IEC 27001 con la finalidad de mejorar el proceso de la seguridad de la información en el Ejército del Perú.	1) La identificación de activos críticos aplicando la NTP ISO/IEC 27001 mejora el proceso de seguridad de la información en el Ejército del Perú.	
2) ¿De qué manera la gestión de riesgos aplicando la NTP ISO/IEC 27001 permitirá mejorar el proceso de seguridad de la información en el Ejército del Perú?	2) Identificar oportunamente riesgos aplicando la NTP ISO/IEC 27001 para mejorar el proceso de la seguridad de la información en el Ejército del Perú.	2) La identificación oportuna de riesgos aplicando la NTP ISO/IEC 27001 permite mejorar el proceso de la seguridad de la información en el Ejército del Perú.	
3) ¿De qué manera los controles del sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001 permitirán mejorar el proceso de la seguridad de la información en el Ejército del Perú?	3) Establecer controles de acuerdo al sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de la seguridad de la información en el Ejército del Perú.	3) Los controles del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 mejoran el proceso de la seguridad de la información en el Ejército del Perú.	

Figura 29: Matriz de consistencia
Fuente: Elaboración propia

ANEXO 02: TABLA DE OPERACIONALIZACIÓN DE VARIABLES

SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NTP/ISO 27001

VARIABLES	DIMENSIONES	INDICADORES	ITEMS/ FORMULA	ESCALA DE MEDICIÓN	INSTRUMENTO
I: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN APLICANDO LA NTP ISO/IEC 27001	SGSI	Activos	¿La organización cuenta con información de activos críticos? ¿La organización cuenta con información de análisis de riesgo de los activos críticos? ¿La entidad cuenta con personal capacitado para realizar análisis de riesgos? ¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo? ¿Se han definido acciones para establecer niveles de riesgo? ¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos? ¿Existe algún software para la gestión de incidentes?	Si/No	ENCUESTA
		Riesgos	¿Se cuenta con personal capacitado para la gestión de incidentes? ¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto? ¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red? ¿Los encargados de Auditoría llevaron a cabo revisiones de seguridad en el pasado? ¿Los encargados de Auditoría participan en la elaboración de los planes de mejora? ¿Área de Auditoría tiene personal capacitado para llevar adelante las auditorías técnicas?		
		Controles	¿Existe planificación para realizar auditorías con el fin de controlar el SGSI? ¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control? ¿Se han documentado las mejoras en la organización? ¿Existe una planificación para establecer políticas de seguridad de la información en la organización? ¿Las políticas y procedimientos están documentados? ¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)? ¿Los encargados de TI participan en la elaboración de los planes de mejora?		

Figura 30: Matriz de Operacionalización
Fuente: Elaboración propia

TABLA DE OPERACIONALIZACIÓN DE VARIABLES

PROCESO DE SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO DEL PERÚ

D: PROCESOS DE SEGURIDAD DE LA INFORMACIÓN	Identificación de activos	Tiempo de identificación de activos	TIA= DRt + PTt + APt + ETt + EAt + RVt TIA= tiempo total del proceso de identificación de activos DRt= designación de los responsables PTt= elaboración del plan de trabajo APt= aprobación del plan de trabajo ETt= ejecución del trabajo EAt= elaboración de acta de activos RVt= revisión y visto bueno por el director t = tiempo	$\sum_{n=t}^{6} TIA_t$	FICHA DE OBSERVACIÓN
	Gestión de riesgos	Nivel de riesgo	Ri = Pr x Im Ri = Riesgo Pr = Probabilidad Im = Impacto	Ri=Pr x Im	
	Aplicabilidad de controles	Controles de la NTP	CA = TC – NA CA = Controles aplicables de la NTP ISO/27001 en la dirección TC = Total de controles NA = Controles no aplicables	CA =TC -NA	

Figura 31: Matriz de Operacionalización
Fuente: Elaboración propia

ANEXO 03: ENCUESTA

INSTRUCCIONES:

Se está realizando una investigación para conocer tus opiniones e intereses sobre la IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO DEL PERÚ, APLICANDO LA NTP ISO/IEC 27001, 2018.

Responde todas las preguntas con la mayor sinceridad posible. Este es un cuestionario anónimo, por favor no escribas tu nombre ni tus apellidos. Toda la información que nos brinden tendrá carácter RESERVADO.

Lea detenidamente cada pregunta responda y/o marque con una (X) la alternativa de su elección.

Marque solamente una opción de las que se le ofrecen en cada caso.

Nº	Dimensiones	ítems	Si	No
1	Activos	¿La organización cuenta con información de activos críticos?		
2		¿La organización cuenta con información de análisis de riesgo de los activos críticos?		
3		¿La entidad cuenta con personal capacitado para realizar análisis de riesgos?		
4		¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo?		
5		¿Se han definido acciones para establecer niveles de riesgo?		
6		¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos?		
7		¿Existe algún software para la gestión de incidentes?		
8	Riesgos	¿Se cuenta con personal capacitado para la gestión de incidentes?		
09		¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto?		
10		¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red?		
11		¿Los encargados de Auditoría llevaron a cabo revisiones de seguridad en el pasado?		
12		¿Los encargados de Auditoría participan en la elaboración de los planes de mejora?		
13		¿Área de Auditoría tiene personal capacitado para llevar adelante las auditorías técnicas?		
14	Controles	¿Existe planificación para realizar auditorías con el fin de controlar el SGSI?		
15		¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control?		
16		¿Se han documentado las mejoras en la organización?		
17		¿Existe una planificación para establecer políticas de seguridad de la información en la organización?		
18		¿Las políticas y procedimientos están documentados?		
19		¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)?		
20		¿Los encargados de TI participan en la elaboración de los planes de mejora?		

ANEXO 04: INSTRUMENTO: ENCUESTA ANTES DE LA IMPLEMENTACIÓN DE LA NTP ISO/IEC 27001

INSTRUCCIONES:

Se está realizando una investigación para conocer tus opiniones e intereses sobre la IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO DEL PERÚ, APLICANDO LA NTP ISO/IEC 27001, 2018.

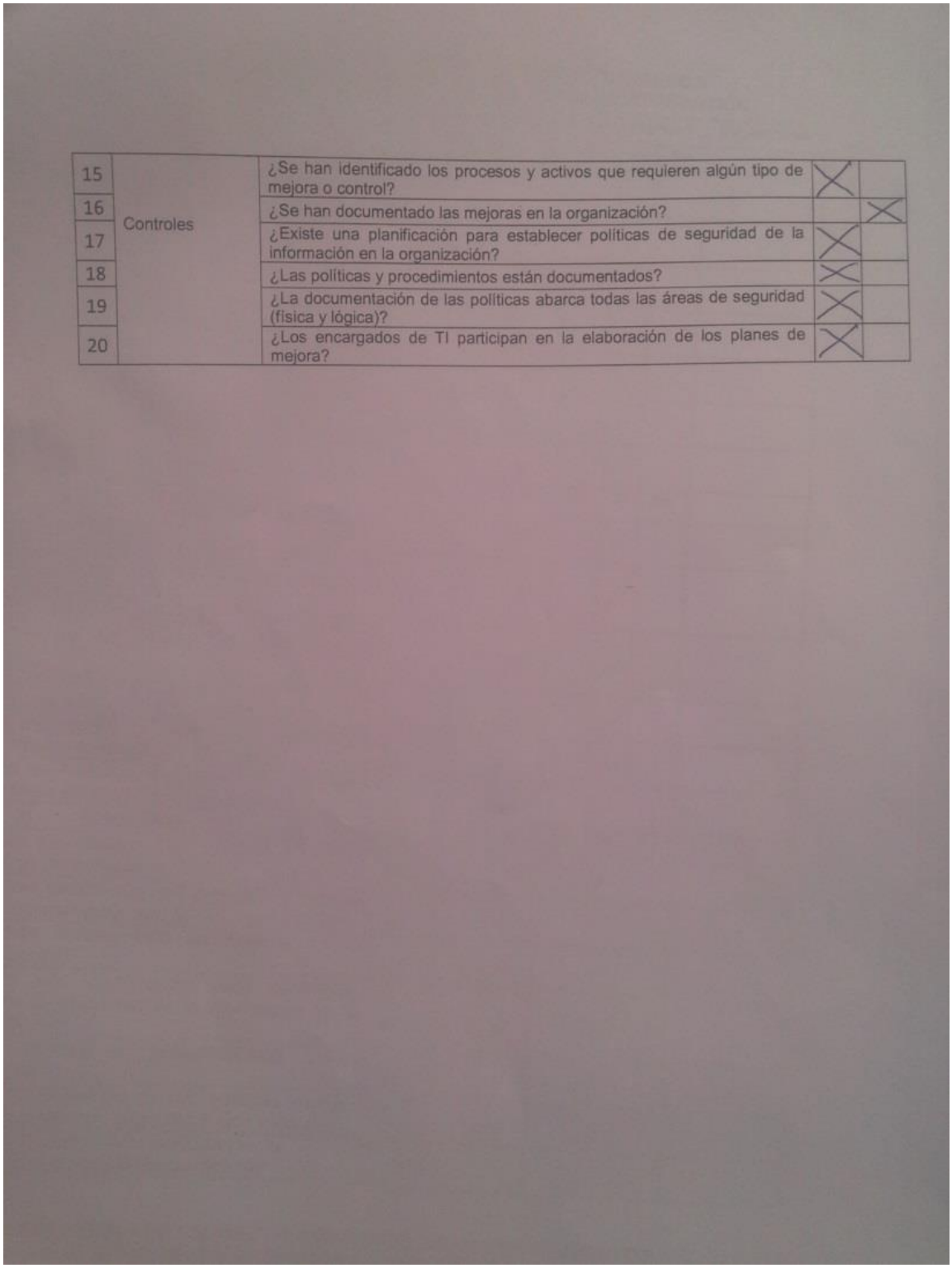
Responde todas las preguntas con la mayor sinceridad posible. Este es un cuestionario anónimo, por favor no escribas tu nombre ni tus apellidos. Toda la información que nos brinden tendrá carácter RESERVADO.

Lea detenidamente cada pregunta responda y/o marque con una (X) la alternativa de su elección.

Marque solamente una opción de las que se le ofrecen en cada caso.

Nº	Dimensiones	Ítems	Si	No
1	Activos	¿La organización cuenta con información de activos críticos?		X
2		¿La organización cuenta con información de análisis de riesgo de los activos críticos?		X
3		¿La entidad cuenta con personal capacitado para realizar análisis de riesgos?		X
4		¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo?		X
5		¿Se han definido acciones para establecer niveles de riesgo?		X
6		¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos?	X	
7		¿Existe algún software para la gestión de incidentes?		X
8	Riesgos	¿Se cuenta con personal capacitado para la gestión de incidentes?		X
09		¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto?		X
10		¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red?		X
11		¿Los encargados de Auditoria llevaron a cabo revisiones de seguridad en el pasado?		X
12		¿Los encargados de Auditoria participan en la elaboración de los planes de mejora?	X	
13		¿Área de Auditoría tiene personal capacitado para llevar adelante las auditorías técnicas?		X
14		¿Existe planificación para realizar auditorías con el fin de controlar el SGSI?		X

Figura 31: Encuesta antes de implementar SGSI
Fuente: Encuesta realizada al personal de la Dirección



15	Controles	¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control?	X	
16		¿Se han documentado las mejoras en la organización?		X
17		¿Existe una planificación para establecer políticas de seguridad de la información en la organización?	X	
18		¿Las políticas y procedimientos están documentados?	X	
19		¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)?	X	
20		¿Los encargados de TI participan en la elaboración de los planes de mejora?	X	

Figura 32: Resultados de encuesta antes de implementación de SGSI
Fuente: Encuesta realizada al personal de la Dirección

INSTRUMENTO: ENCUESTA DESPUÉS DE LA IMPLEMENTACIÓN DE LA NTP ISO/IEC 27001

INSTRUCCIONES:

Se está realizando una investigación para conocer tus opiniones e intereses sobre la IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA MEJORAR EL PROCESO DE SEGURIDAD DE LA INFORMACIÓN EN EL EJÉRCITO DEL PERÚ, APLICANDO LA NTP ISO/IEC 27001, 2018.

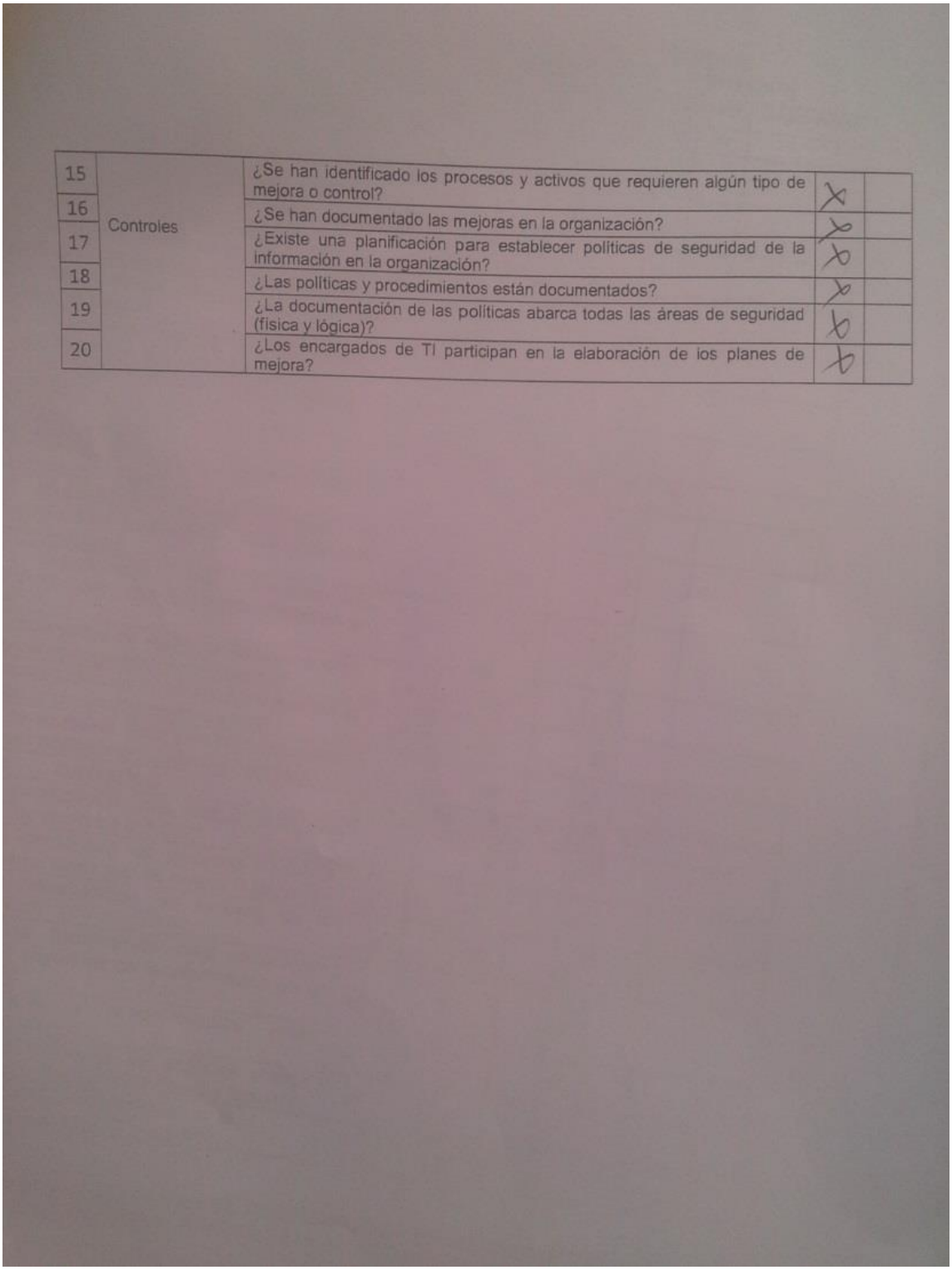
Responde todas las preguntas con la mayor sinceridad posible. Este es un cuestionario anónimo, por favor no escribas tu nombre ni tus apellidos. Toda la información que nos brinden tendrá carácter RESERVADO.

Lea detenidamente cada pregunta responda y/o marque con una (X) la alternativa de su elección.

Marque solamente una opción de las que se le ofrecen en cada caso.

Nº	Dimensiones	ítems	Si	No
1	Activos	¿La organización cuenta con información de activos críticos?	X	
2		¿La organización cuenta con información de análisis de riesgo de los activos críticos?	X	
3		¿La entidad cuenta con personal capacitado para realizar análisis de riesgos?	X	
4		¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo?	X	
5		¿Se han definido acciones para establecer niveles de riesgo?	X	
6		¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos?	X	
7		¿Existe algún software para la gestión de incidentes?		X
8	Riesgos	¿Se cuenta con personal capacitado para la gestión de incidentes?	X	
09		¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto?	X	
10		¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red?	X	
11		¿Los encargados de Auditoria llevaron a cabo revisiones de seguridad en el pasado?		X
12		¿Los encargados de Auditoria participan en la elaboración de los planes de mejora?	X	
13		¿Área de Auditoria tiene personal capacitado para llevar adelante las auditorias técnicas?		X
14		¿Existe planificación para realizar auditorias con el fin de controlar el SGSI?	X	

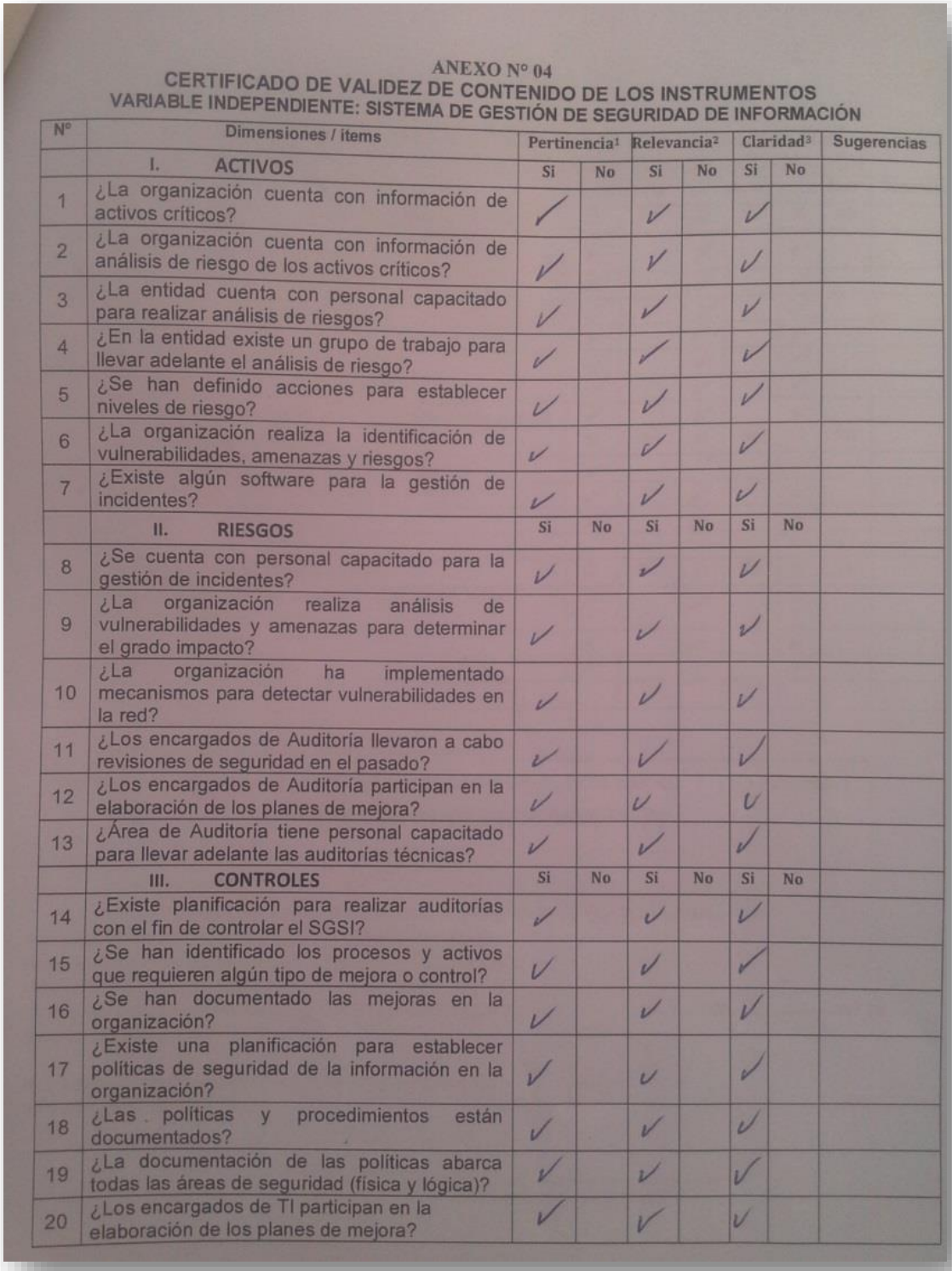
Figura 33: Resultados de encuesta despues de la implementación de SGSI
Fuente: Encuesta realizada al personal de la Dirección



15	Controles	¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control?	X	
16		¿Se han documentado las mejoras en la organización?	X	
17		¿Existe una planificación para establecer políticas de seguridad de la información en la organización?	X	
18		¿Las políticas y procedimientos están documentados?	X	
19		¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)?	X	
20		¿Los encargados de TI participan en la elaboración de los planes de mejora?	X	

Figura 34: Resultados de encuesta despues de la implementacion de SGSI
Fuente: Encuesta realizada al personal de la Dirección

ANEXO 05: VALIDACIÓN DEL INSTRUMENTO



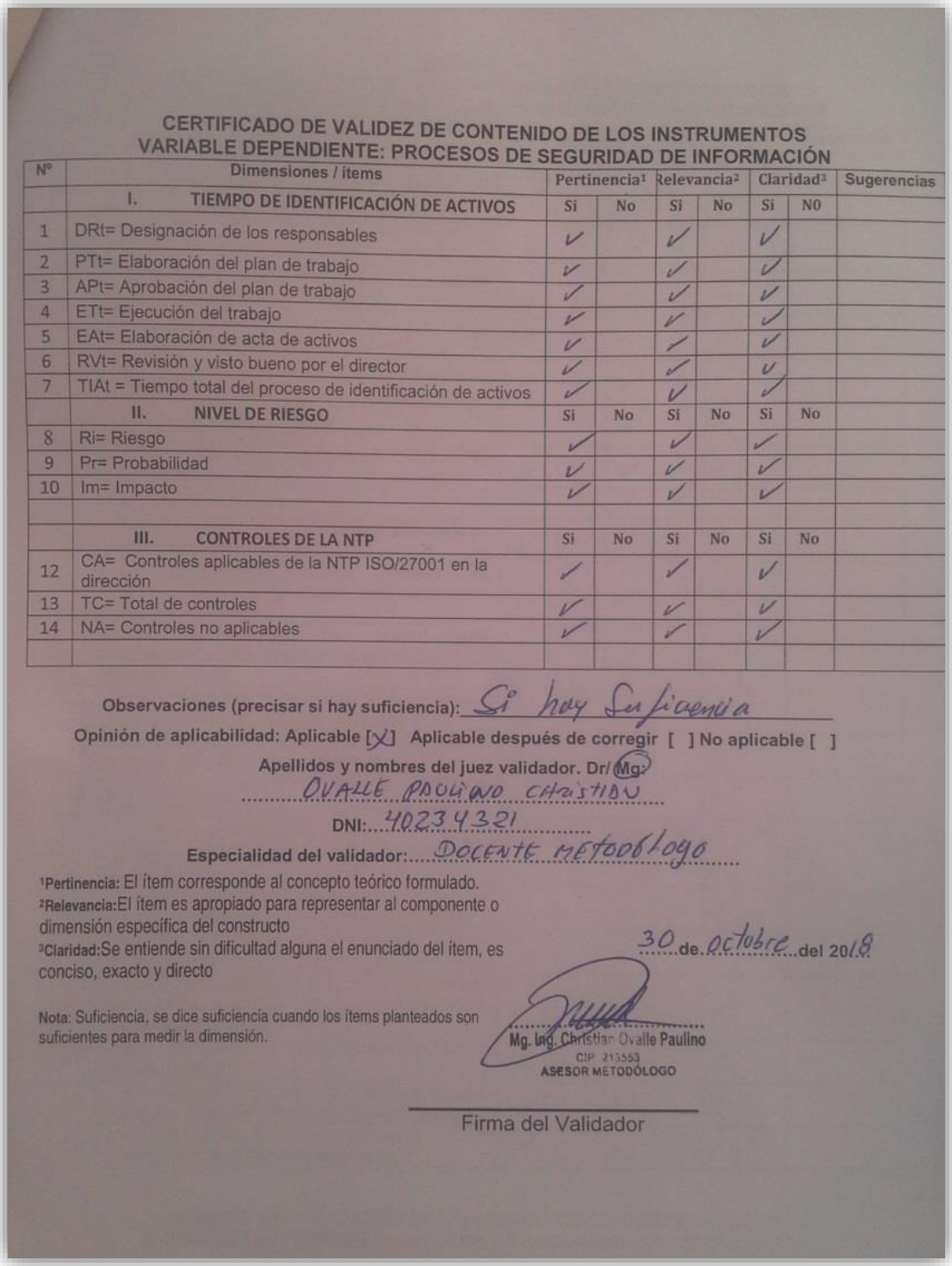
ANEXO N° 04

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS

VARIABLE INDEPENDIENTE: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

N°	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. ACTIVOS	Si	No	Si	No	Si	No	
1	¿La organización cuenta con información de activos críticos?	✓		✓		✓		
2	¿La organización cuenta con información de análisis de riesgo de los activos críticos?	✓		✓		✓		
3	¿La entidad cuenta con personal capacitado para realizar análisis de riesgos?	✓		✓		✓		
4	¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo?	✓		✓		✓		
5	¿Se han definido acciones para establecer niveles de riesgo?	✓		✓		✓		
6	¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos?	✓		✓		✓		
7	¿Existe algún software para la gestión de incidentes?	✓		✓		✓		
	II. RIESGOS	Si	No	Si	No	Si	No	
8	¿Se cuenta con personal capacitado para la gestión de incidentes?	✓		✓		✓		
9	¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto?	✓		✓		✓		
10	¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red?	✓		✓		✓		
11	¿Los encargados de Auditoría llevaron a cabo revisiones de seguridad en el pasado?	✓		✓		✓		
12	¿Los encargados de Auditoría participan en la elaboración de los planes de mejora?	✓		✓		✓		
13	¿Área de Auditoría tiene personal capacitado para llevar adelante las auditorías técnicas?	✓		✓		✓		
	III. CONTROLES	Si	No	Si	No	Si	No	
14	¿Existe planificación para realizar auditorías con el fin de controlar el SGSI?	✓		✓		✓		
15	¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control?	✓		✓		✓		
16	¿Se han documentado las mejoras en la organización?	✓		✓		✓		
17	¿Existe una planificación para establecer políticas de seguridad de la información en la organización?	✓		✓		✓		
18	¿Las políticas y procedimientos están documentados?	✓		✓		✓		
19	¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)?	✓		✓		✓		
20	¿Los encargados de TI participan en la elaboración de los planes de mejora?	✓		✓		✓		

Figura 35: Validación de instrumento de SGSI



CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS
VARIABLE DEPENDIENTE: PROCESOS DE SEGURIDAD DE INFORMACIÓN

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. TIEMPO DE IDENTIFICACIÓN DE ACTIVOS	Si	No	Si	No	Si	N0	
1	DRt= Designación de los responsables	✓		✓		✓		
2	PTt= Elaboración del plan de trabajo	✓		✓		✓		
3	APt= Aprobación del plan de trabajo	✓		✓		✓		
4	ETt= Ejecución del trabajo	✓		✓		✓		
5	EAt= Elaboración de acta de activos	✓		✓		✓		
6	RVt= Revisión y visto bueno por el director	✓		✓		✓		
7	TIAt = Tiempo total del proceso de identificación de activos	✓		✓		✓		
	II. NIVEL DE RIESGO	Si	No	Si	No	Si	No	
8	Ri= Riesgo	✓		✓		✓		
9	Pr= Probabilidad	✓		✓		✓		
10	Im= Impacto	✓		✓		✓		
	III. CONTROLES DE LA NTP	Si	No	Si	No	Si	No	
12	CA= Controles aplicables de la NTP ISO/27001 en la dirección	✓		✓		✓		
13	TC= Total de controles	✓		✓		✓		
14	NA= Controles no aplicables	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Sí hay Suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg: OVALLE PAULINO CHRISTIAN

DNI: 40234321

Especialidad del validador: DOCENTE METODÓLOGO

[1]Pertinencia: El ítem corresponde al concepto teórico formulado.
[2]Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

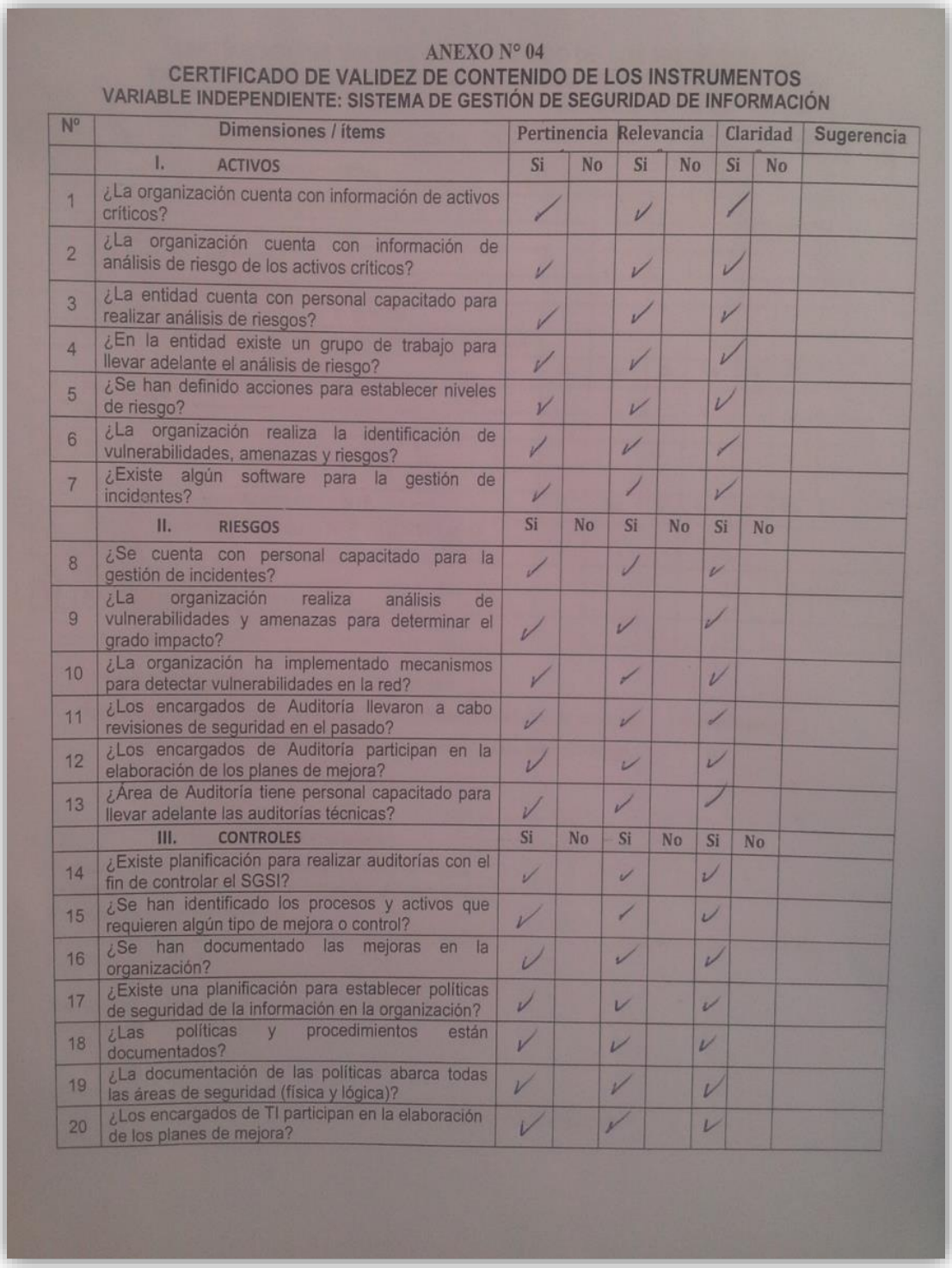
Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

30 de octubre del 2018

Mg. Ing. Christian Ovalle Paulino
CIP 213553
ASESOR METODÓLOGO

Firma del Validador

Figura 36: Validación de instrumento de proceso de seguridad de información



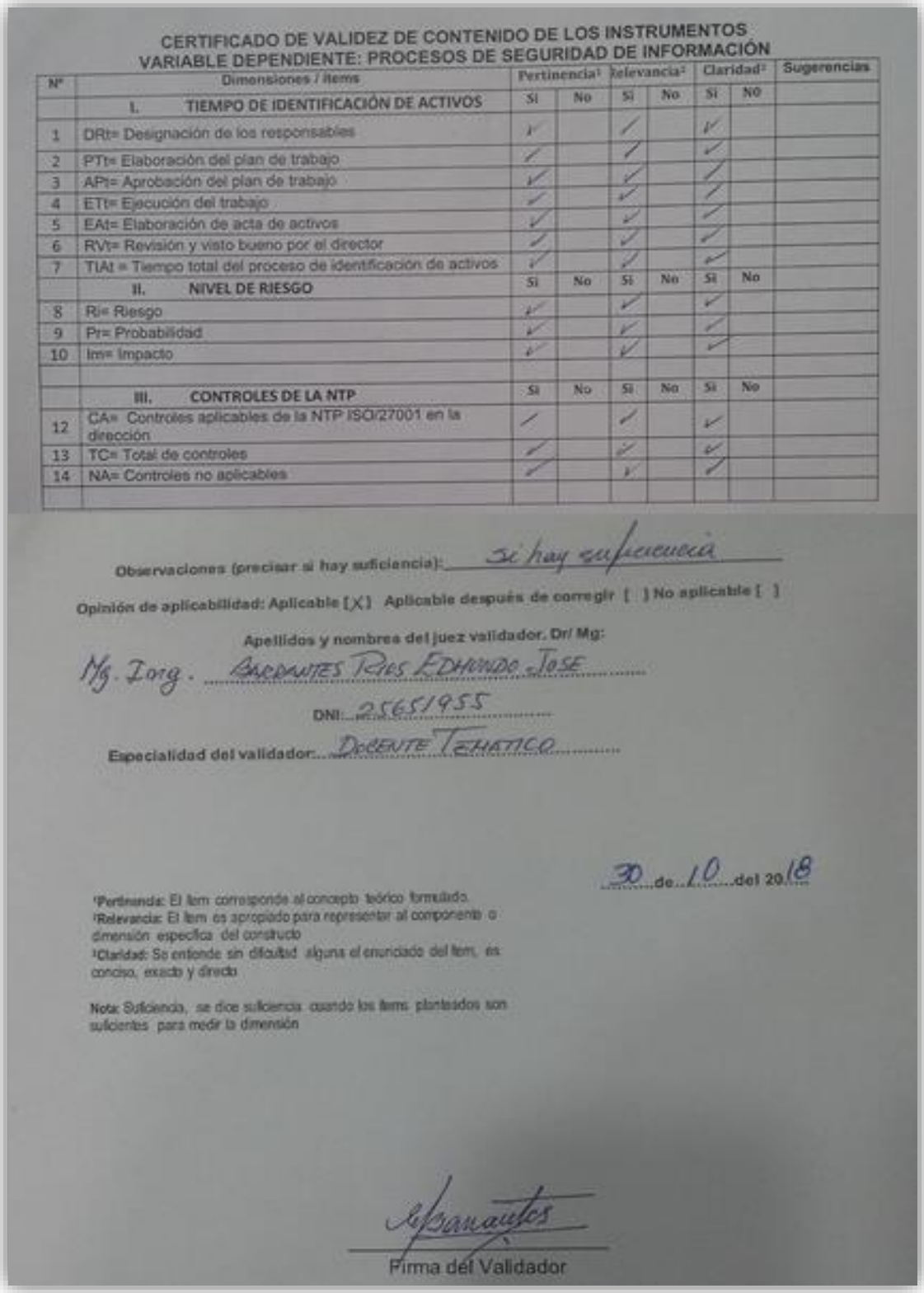
ANEXO N° 04

CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS

VARIABLE INDEPENDIENTE: SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN

N°	Dimensiones / ítems	Pertinencia		Relevancia		Claridad		Sugerencia
	I. ACTIVOS	Si	No	Si	No	Si	No	
1	¿La organización cuenta con información de activos críticos?	✓		✓		✓		
2	¿La organización cuenta con información de análisis de riesgo de los activos críticos?	✓		✓		✓		
3	¿La entidad cuenta con personal capacitado para realizar análisis de riesgos?	✓		✓		✓		
4	¿En la entidad existe un grupo de trabajo para llevar adelante el análisis de riesgo?	✓		✓		✓		
5	¿Se han definido acciones para establecer niveles de riesgo?	✓		✓		✓		
6	¿La organización realiza la identificación de vulnerabilidades, amenazas y riesgos?	✓		✓		✓		
7	¿Existe algún software para la gestión de incidentes?	✓		✓		✓		
	II. RIESGOS	Si	No	Si	No	Si	No	
8	¿Se cuenta con personal capacitado para la gestión de incidentes?	✓		✓		✓		
9	¿La organización realiza análisis de vulnerabilidades y amenazas para determinar el grado impacto?	✓		✓		✓		
10	¿La organización ha implementado mecanismos para detectar vulnerabilidades en la red?	✓		✓		✓		
11	¿Los encargados de Auditoría llevaron a cabo revisiones de seguridad en el pasado?	✓		✓		✓		
12	¿Los encargados de Auditoría participan en la elaboración de los planes de mejora?	✓		✓		✓		
13	¿Área de Auditoría tiene personal capacitado para llevar adelante las auditorías técnicas?	✓		✓		✓		
	III. CONTROLES	Si	No	Si	No	Si	No	
14	¿Existe planificación para realizar auditorías con el fin de controlar el SGSI?	✓		✓		✓		
15	¿Se han identificado los procesos y activos que requieren algún tipo de mejora o control?	✓		✓		✓		
16	¿Se han documentado las mejoras en la organización?	✓		✓		✓		
17	¿Existe una planificación para establecer políticas de seguridad de la información en la organización?	✓		✓		✓		
18	¿Las políticas y procedimientos están documentados?	✓		✓		✓		
19	¿La documentación de las políticas abarca todas las áreas de seguridad (física y lógica)?	✓		✓		✓		
20	¿Los encargados de TI participan en la elaboración de los planes de mejora?	✓		✓		✓		

Figura 37: Validación de instrumento de SGSI



CERTIFICADO DE VALIDEZ DE CONTENIDO DE LOS INSTRUMENTOS
VARIABLE DEPENDIENTE: PROCESOS DE SEGURIDAD DE INFORMACIÓN

Nº	Dimensiones / ítems	Pertinencia[1]		Relevancia[2]		Claridad[3]		Sugerencias
	I. TIEMPO DE IDENTIFICACIÓN DE ACTIVOS	Si	No	Si	No	Si	No	
1	DRt= Designación de los responsables	✓		✓		✓		
2	PTt= Elaboración del plan de trabajo	✓		✓		✓		
3	APt= Aprobación del plan de trabajo	✓		✓		✓		
4	ETt= Ejecución del trabajo	✓		✓		✓		
5	EAt= Elaboración de acta de activos	✓		✓		✓		
6	RVt= Revisión y visto bueno por el director	✓		✓		✓		
7	TIAt = Tiempo total del proceso de identificación de activos	✓		✓		✓		
	II. NIVEL DE RIESGO	Si	No	Si	No	Si	No	
8	Ri= Riesgo	✓		✓		✓		
9	Pr= Probabilidad	✓		✓		✓		
10	Im= Impacto	✓		✓		✓		
	III. CONTROLES DE LA NTP	Si	No	Si	No	Si	No	
12	CA= Controles aplicables de la NTP ISO/27001 en la dirección	✓		✓		✓		
13	TC= Total de controles	✓		✓		✓		
14	NA= Controles no aplicables	✓		✓		✓		

Observaciones (precisar si hay suficiencia): Si hay suficiencia

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador. Dr/ Mg:

Mg. Ing. ESCRIVENS PEREZ EDMUNDO JOSE

DNI: 25651955

Especialidad del validador: DOCENTE TEMATICO

30 de 10 del 2018

[1]Pertinencia: El ítem corresponde al concepto teórico formulado.
[2]Relevancia: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]Claridad: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Validador

Figura 38: Validación de instrumento de proceso de seguridad de información

ANEXO 06: MATRIZ DE DATOS

MATRIZ DE DATOS – PRE IMPLEMENTACIÓN DE LA NTP ISO/IEC 27001

Tabla 28: Matriz de datos pre implementación de la NTP ISO/IEC 27001

	V. I. SISTEMA DE INFORMACION DE SEGURIDAD DE INFORMACION																					
N°	ACTIVOS							RIESGOS						CONTROLES							TOTAL	
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	SI	NO
01	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
02	si	no	si	si	no	si	no	si	no	no	no	no	no	no	no	no	no	si	no	si	07	13
03	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
04	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	si	si	04	16
05	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	no	si	si	12	08
06	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
07	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	no	si	si	12	08
08	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
09	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
10	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
11	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
12	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
13	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
14	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
15	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
16	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
17	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
18	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
19	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
20	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
21	si	no	si	si	no	si	no	si	no	no	no	no	no	no	no	no	no	si	no	si	07	13
22	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
23	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	si	si	04	16
24	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	no	si	si	12	08
25	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
26	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	no	si	si	12	08
27	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
28	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
29	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
30	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
31	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
32	si	si	si	si	si	si	si	no	no	si	no	no	no	no	si	no	si	si	si	si	13	07
33	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
34	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
35	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17
36	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
37	no	no	no	no	no	si	no	no	no	no	no	si	no	no	si	no	si	si	si	si	07	13
38	no	no	no	no	no	si	no	no	no	no	no	no	no	no	no	no	no	si	no	si	03	17

Tabla 29: Matriz de datos de procesos de seguridad de información - Pre

V. D. PROCESOS DE SEGURIDAD DE INFORMACIÓN			
N° DE REGISTRO	ÁREA	TIEMPO DE IDENTIFICACIÓN DE ACTIVOS	
		PRE	POST
1	Administración	33:56	9:06
2	Mesa de partes	50:00	11:30
3	Criptologia	37:17	12:07
4	Informaciones	28:48	13:38
5	Planeamiento	25:15	10:50
6	Presupuesto	36:40	10:20
7	Organización	36:09	13:20
8	Inteligencia	28:10	12:30
9	Jurídico	3914	09:47
10	Economía	48:28	13:32
11	Control interno	53:43	17:01
12	Seguridad	55:58	09:08
13	Área TI	27:08	07:28
14	Personal	36:56	10:46
15	Inspectoría	35:35	08:22
TOTAL		573:28	169:42

Fuente: Elaboración propia

MATRIZ DE DATOS – POST IMPLEMENTACIÓN DE LA NTP ISO/IEC 27001

	V. I. SISTEMA DE INFORMACION DE SEGURIDAD DE INFORMACION																				
N°	ACTIVOS							RIESGOS						CONTROLES							TOTAL	
	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16	P17	P18	P19	P20	SI	NO
01	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
02	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
03	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
04	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
05	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
06	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
07	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
08	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
09	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
10	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
11	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
12	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
13	si	si	si	si	si	si	no	si	si	si	si	si	si	si	si	si	si	si	si	si	19	01
14	si	si	si	si	si	si	no	si	si	si	si	si	si	si	si	si	si	si	si	si	19	01
15	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
16	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
17	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
18	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
19	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
20	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
21	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
22	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
23	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
24	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
25	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
26	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
27	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
28	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
29	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
30	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
31	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
32	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
33	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
34	si	si	si	si	si	si	no	si	si	si	no	si	si	si	si	si	si	si	si	si	18	02
35	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
36	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03
37	si	si	no	si	si	si	no	no	si	si	no	no	no	si	si	si	si	si	si	si	14	06
38	si	si	si	si	si	si	no	si	si	si	no	si	no	si	si	si	si	si	si	si	17	03

Fuente: Elaboración propia

Tabla 30: Matriz de datos de procesos de seguridad de información - Post

V. D. PROCESOS DE SEGURIDAD DE INFORMACIÓN			
N° DE REGISTRO	ÁREA	TIEMPO DE IDENTIFICACIÓN DE ACTIVOS	
		PRE	POST
1	Administración	33:56	9:06
2	Mesa de partes	50:00	11:30
3	Criptologia	37:17	12:07
4	Informaciones	28:48	13:38
5	Planeamiento	25:15	10:50
6	Presupuesto	36:40	10:20
7	Organización	36:09	13:20
8	Inteligencia	28:10	12:30
9	Jurídico	3914	09:47
10	Economía	48:28	13:32
11	Control interno	53:43	17:01
12	Seguridad	55:58	09:08
13	Área TI	27:08	07:28
14	Personal	36:56	10:46
15	Inspectoría	35:35	08:22
TOTAL		573:28	169:42

Fuente: Elaboración propia

ANEXO 07: PROPUESTA DE VALOR

FASE PLANIFICACIÓN

Cronograma del proyecto

En la tabla se observa el cronograma del proyecto de “Implementación de sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001 para la mejora de los procesos de seguridad de información en el Ejército del Perú”.

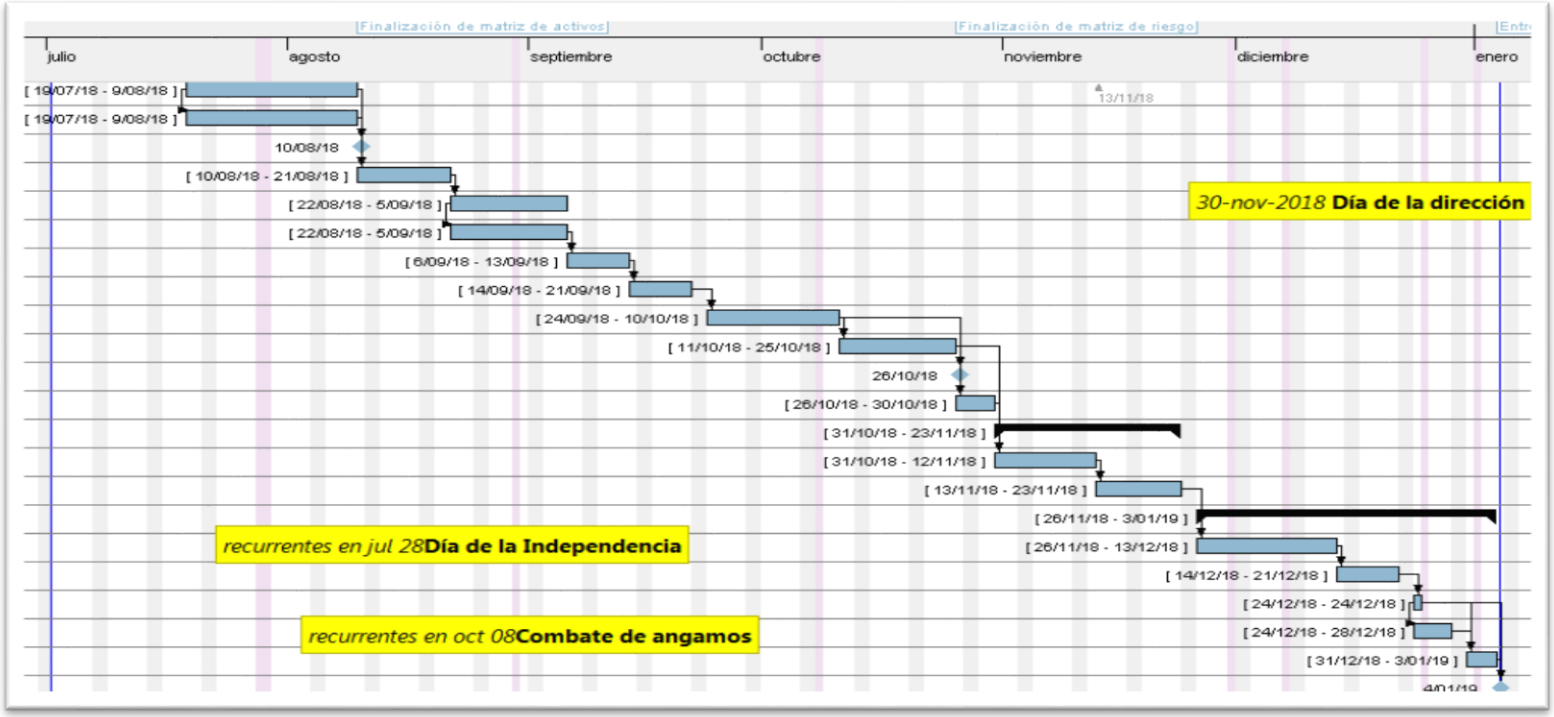


Figura 39: Cronograma de actividades de implementación del SGSI
Fuente: Elaboración propia

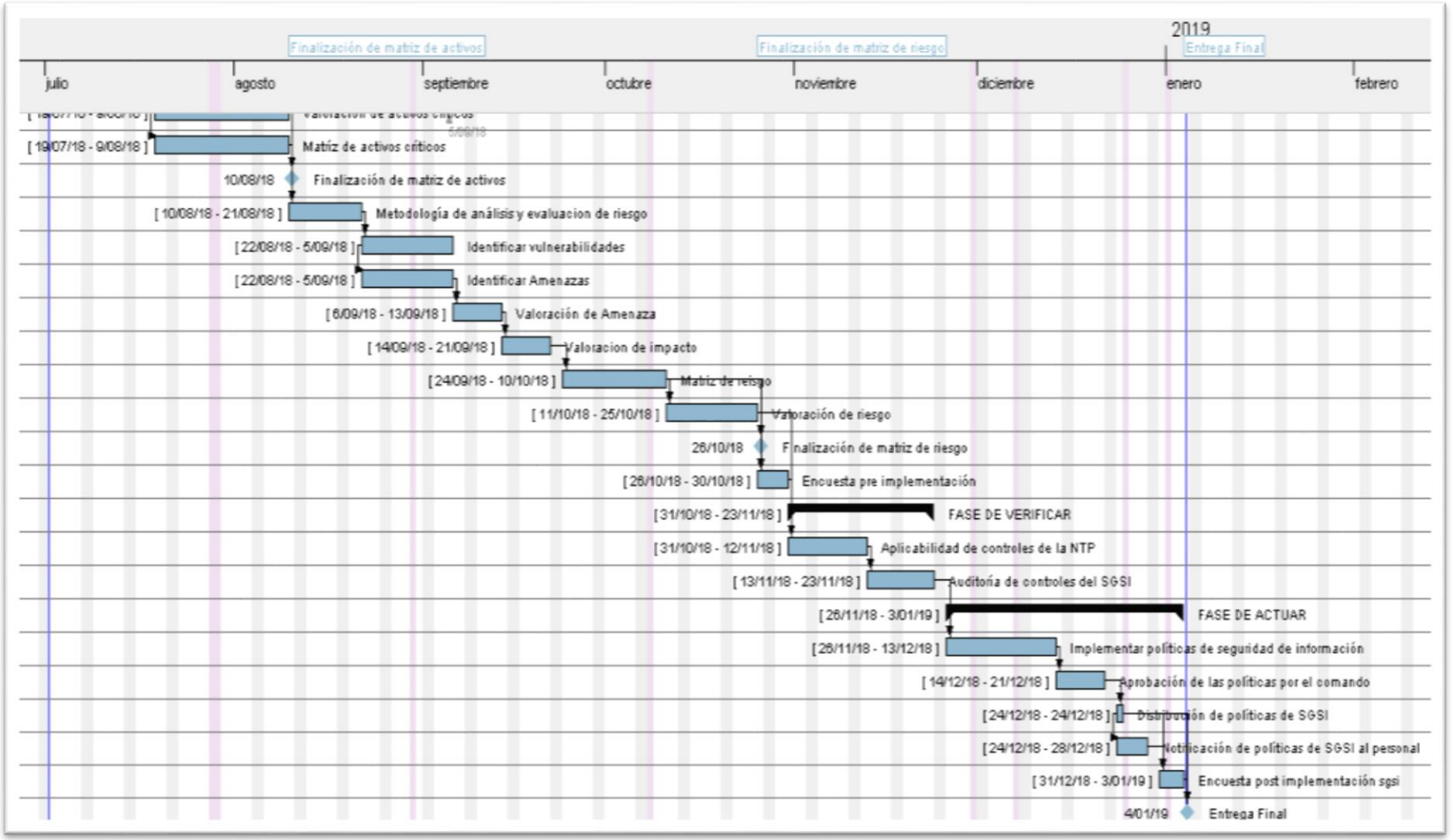


Figura 40: Cronograma que muestra las tareas y fechas correspondientes de implementación del SGSI
Fuente: Elaboración propia

Presupuesto

En la tabla se observa el presupuesto del proyecto de “Implementación de sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001 para la mejora de los procesos de seguridad de información en el Ejército del Perú”.

BIENES

Tabla 31: Presupuesto de bienes

Cantidad	Descripción	P. Unit (S/.)	Total (S/.)
1	Laptop	2000.00	2000.00
1	Antena wifi	100.00	100.00
1	Millar de hojas	25.00	25.00
2	Memoria USB 32 GB	60.00	120.00
1	Tinta para impresora HP 1002	200.00	200.00
Global	Otros útiles de escritorio, fólderes, minas, lapiceros	35.00	35.00
		Total	**2,480.00**

Fuente: Elaboración propia

SERVICIOS

Tabla 32: presupuesto de servicios

Descripción	Total (S/.)	Total (S/.)
Internet	300.00	300.00
Luz	150.00	150.00
Celular	100.00	100.00
Transporte	300.00	300.00
	Total	**850.00**

Fuente: Elaboración propia

RECURSOS HUMANOS

Tabla 33: Presupuesto de recursos humanos

Cantidad	Descripción	Total (S/.)
1	Especialista temático	5000.00
1	Especialista en planeamiento e indicadores	3000.00
1	Trabajo de campo	2000.00
	Total	**10.000.00**

Fuente: Elaboración propia

RESUMEN

Tabla 34: Resumen de presupuesto

Descripción	Total (S/.)
Bienes	2480.00
Servicios	850.00
Recursos Humanos	10.000.00
Total	**13,330.00**

Fuente: Elaboración propia

Nombre y descripción del Sistema de Gestión

Implementación del sistema de gestión de seguridad de información aplicando la norma técnica peruana ISO/IEC 27001 para mejorar el proceso de seguridad de información en el Ejército del Perú.

Para mejorar procesos de seguridad de información en la dirección se requiere la identificación de activos, gestión de riesgos y posteriormente establecer controles en este caso de acuerdo a la norma técnica peruana ISO/iec 27001 que precisamente aplica la metodología de ciclo Deming que consiste en el Plan-Do-Check-Act (PDCA) de mejora continua. En consecuencia, el presente trabajo de investigación se desarrolla fase por fase (Planear-Hacer-Verificar-Actuar), mediante la aplicación de la misma se identifica los riesgos de la seguridad de la información, realizar una correcta estimación de los tiempos en el proceso de identificación de activos críticos, que permitirá el análisis correspondiente de los riesgos de seguridad de la información; además, lograr una participación activa y el trabajo en equipo, hasta obtener el producto esperado, sin que ello implique el final del proyecto porque la metodología empleada PDCA es cíclico es decir en desarrollo permanente debiendo hacer los ajustes necesarios e implementar en otras direcciones de la entidad permitiendo la continuidad del producto y aplicando el SGSI de acuerdo al contexto.

Descripción del proyecto

El departamento de TI de la DIE, realiza la vigilancia y monitoreo permanente de los accesos a la red de la DIE, teniendo en cuenta de los incidentes relacionados a la seguridad de informaciones que ocurran en la entidad. Dichos incidentes son debidamente registrados para el análisis posterior con el fin de establecer las causas u orígenes del incidente.

La finalidad del proyecto es obtener la gestión de seguridad de información en el cual se pueda plasmar los procesos de seguridad de información que puedan mejorar en los controles de las vulnerabilidades, amenazas y riesgos, utilizando en este caso particular software libre para realizar las auditorias correspondientes.

Componentes del Sistema de Gestión

Recursos Humanos

Constituidos por personal que labora en área de TI de la dirección, quienes trabajan e interactúan a diario con información clasificada de alto valor para la organización y la seguridad del país.

Hardware

En la dirección se comprende por hardware todos los dispositivos o elementos físicos que componen una computadora, incluyendo los elementos mecánicos, electrónicos y eléctricos. Los teclados, monitores, impresoras, microprocesadores, unidades de disco, ratón, escáner y demás periféricos, son hardware. Se clasifica generalmente en básico y complementario, entendiendo por básico todo aquel dispositivo necesario para iniciar la computadora y el complementario que sirve para realizar funciones específicas.

Software

Es el conjunto de datos que necesita la computadora para poder trabajar. Los datos varían según el tipo de operación que deba realizar la computadora, y por eso se agrupan formando programas distintos. Se clasifican en:

- De sistema operativos.
- De aplicación.
- De desarrollo.

Al respecto la dirección emplea software para realizar sus labores cotidianas; sin embargo, carece de una aplicación para administrar los activos de la dirección la misma que facilitaría la gestión de riesgos de seguridad de información de la dirección.

Datos

Los datos que viene administrando la dirección son muchas formas, incluyendo datos alfanuméricos (compuesto de letras y números), de textos, imágenes, audio y video en su mayoría de carácter RESERVADO y de alto interés para las agencias de inteligencia de otros países.

Objetivo del Sistema de Gestión

En la presente investigación los objetivos del sistema de gestión son los siguientes:

Objetivo general:

- Implementar el sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de seguridad de la información en el Ejército del Perú.

Objetivos específicos:

- Identificar activos críticos aplicando la NTP ISO/IEC 27001 con la finalidad de mejorar el proceso de la seguridad de la información en el Ejército del Perú.

- Identificar oportunamente riesgos aplicando la NTP ISO/IEC 27001 para mejorar el proceso de la seguridad de la información en el Ejército del Perú.

- Establecer controles de acuerdo al sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001 para mejorar el proceso de la seguridad de la información en el Ejército del Perú.

Alcance del Sistema de Gestión

El sistema de gestión de seguridad de la información involucra todas las áreas o subdirecciones de la Dirección de Informaciones del Ejército del Perú y terceros que tengan alguna relación de contrato, proveedor o servicios que involucren algún proceso de seguridad de información de la institución.

Restricciones del Sistema de Gestión

Actualmente, la Dirección en estudio carece de software que permita gestionar riesgos bajo las normas internacionales que garanticen la seguridad de la información de la dirección de acuerdo a la implementación de controles del SGSI de la NTP ISO/IEC 27001.

Estudio de Factibilidad del Sistema de Gestión

El estudio de factibilidad para la implementación de un sistema de gestión de seguridad de información aplicando la NTP ISO/IEC 27001 para mejorar los procesos de seguridad de información en la dirección de informaciones del

Ejército del Perú, se desarrolla en tres aspectos básicos: operativa, técnica y económica.

Factibilidad Operativa

La factibilidad operativa de la investigación, fue posible por el apoyo del personal encargado de administrar la seguridad de manera general que incluye la seguridad de la información y la necesidad de contar con un sistema de gestión de seguridad de la información para mejorar los procesos de la seguridad de la información en el Ejército del Perú, aplicando la NTP/ISO 27001. La misma que permite gestionar riesgos identificando los activos críticos de la dirección para mitigar las vulnerabilidades y amenazas que de materializarse generarían perdidas de información clasificada, afectando la imagen institucional e incluso puede comprometer la seguridad nacional.

Factibilidad Técnica

La factibilidad técnica se sustenta en los recursos informáticos de la dirección para poder implementar el sistema de gestión de seguridad de la información; existe la experiencia para el análisis, planeamiento e implementación del sistema en base a la Norma Técnica Peruana. Se ha priorizado su desarrollo por ser procesos críticos de la dirección y se ha identificado la metodología más adecuada para lograr los objetivos de la problemática de estudio, El presente proyecto responde a la necesidad inmediata de implementación del SGSI, que involucra identificar los riegos, vulnerabilidades y amenazas para tomar previsiones relacionados a la seguridad de la información de la dirección.

Factibilidad económica

La factibilidad económica del presente proyecto, es el análisis que se realiza del costo-beneficio la administración de la seguridad de la información en la dirección, recordemos que la finalidad principal de la implementación en proteger o garantizar la disponibilidad, confidencialidad e integridad de la información en la dirección, por lo cual la información juega un papel preponderante y el monto que propuesto es factible en vista que la implementación de las políticas de seguridad de la información y su estricto control reducen los riesgos a la que está expuesto

la información.

En la tabla de presupuesto que se presenta se identifican los costos de papelería, del hardware, del software, de los recursos humanos necesarios para la implementación del SGSI en la dirección. A continuación se muestra el cuadro de resumen.

Tabla 35: Presupuesto de bienes, servicios y recursos humanos

Descripción	Total (S/.)
Bienes	2480.00
Servicios	850.00
Recursos Humanos	10.000.00
Total	**13,330.00**

Fuente: Elaboración propia

Metodología Aplicada

Descripción de la metodología aplicada

La Metodología aplicada es el PDCA en la cual se desarrolla el proyecto fase por fase, mediante la aplicación de la misma se pretende identificar los riesgos de la seguridad de la información, realizar una correcta identificación de riesgos, amenazas y vulnerabilidades, lograr una participación activa del equipo de trabajo, desarrollar un incremento funcional en las medidas de seguridad, revisar los planes elaborados contrastando con la meta para entregar los avances del producto hasta finalmente obtener los entregables, lo cual no implica el fin del proyecto porque se deberá hacer los ajustes necesarios para implementar en otras direcciones de la entidad permitiendo la continuidad del producto.

Se requiere de un sistema de gestión de seguridad de la información para tener los controles adecuados en los procesos de recolección de datos, almacenamiento, procesamiento, transmisión y exhibición de la información de que administra y produce la organización.

Implementación del Sistema de Gestión

Se inició con una reunión en la Sala de Reuniones de la Dirección, a las 08:30 horas con la participación de los responsables de la toma decisiones de la dirección entre ellos el Director, el Jefe de TI, el Jefe de Planeamiento, Presupuesto, y el encargado del proyecto; en dicha reunión se explicó ampliamente de la implementación del sistema de gestión de seguridad de la información aplicando la NTP ISO/IEC 27001, en vista de cumplir también con la Resolución Ministerial de la ONGEI.

Se determinó el alcance del proyecto la misma que sería en el ámbito de la dirección de informaciones.

Se estableció el cronograma de trabajo a realizarse durante la implementación del proyecto.

FASE HACER

Identificación de activos críticos

Se identifican los activos que de la dirección que están involucrados en diferentes procesos de seguridad de información, de acuerdo al ISO 27001, se pueden identificar dos tipos de activos: los primarios y los de soporte. Los primarios, son los procesos e información más sensibles para la dirección. Los activos de soporte, son los que dan el soporte adecuado a los activos primarios.

Valoración de los Activos: Los activos que generan valor son aquellos que se necesitan proteger, y cada activo tiene una importancia mayor o menor en la dirección. MAGERIT establece dos (2) tipos de valoraciones: Cualitativa que es aquella que permite calcular el valor de un activo en base al impacto que pueda tener en la organización y la Cuantitativa que estima el costo del activo (incluyendo costo de compra, de reparación, configuración, mantenimiento, etc.).

Se determina la valoración de los activos de acuerdo a la dimensión de seguridad (confidencialidad, integridad y disponibilidad) de la información para ello se establece el siguiente cuadro:

Tabla 36: Dimensión de seguridad

Dimensión de seguridad	Nomenclatura	Definición
Disponibilidad	D	Propiedad o característica de los activos consistente en que las sub direcciones o procesos autorizados tienen acceso a los mismos cuando lo requieran
Integridad	I	Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada
Confidencialidad	C	Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados

Fuente: Elaboración propia

Tabla 37: Valoración y criterio de dimensión de seguridad

Disponibilidad (D)		Integridad (I)		Confidencialidad (C)	
Valor	Criterio	Valor	Criterio	Valor	Criterio
3	Información disponible en todo momento para la toma de decisiones	3	Información que de ser modificada altera por completo el proceso de seguridad de la información	3	Información clasificada que solo puede ser accedida con autorización del Director
2	Información requerida para la toma de decisiones de la organización	2	Información que de ser modificada afecta en parte el resultado del proceso de seguridad de información	2	Información reservado que requiere cierta medida de seguridad de información
1	Información no es vital para la toma de decisiones	1	Información que de ser modificada no impacta en la imagen de la institución	1	Información disponible al público

Fuente: Elaboración propia

A continuación, se muestra el inventario de todos los activos identificados en la dirección, consecuentemente se realiza la valoración de los activos identificados que están involucrados en los procesos de la seguridad de la información.

Matriz de activos críticos

Id	Activo de información			Proceso	Ubicación del activo		Propietario	Clasificación	Valoración		
	Activo	Descripción	Tipo	Actividad	Físico	Lógico			D	I	C
01	Orden de servicio	Documentos donde se establece el rol de servicio de la semana	Primario	Recibir la notificación	Legajo		Administración	Reservado	3	2	3
02	Guía de remisión	Documento donde se lleva el registro de remisión de la producción.	Primario	Firmar cargo	Archivo de guías		Agente	Reservado	2	2	2
03	Computador de escritorio	Computadoras utilizada por el personal para realizar labores de búsqueda de información y elaboración de documentos y otros	Soporte	Formular documentos	Sub direcciones		DIE		1	2	3
04	Módulo PNP	Módulo que sirve para coordinación con la PNP	Soporte	Realizar coordinación	Secretaría		Agente PNP		2	2	2
05	Cuaderno de registro – remitido	Cuaderno donde se realizan los registros de	Primario	Registrar documentos remitidos	Mesa de partes		Jefe de mesa de partes	Confidencial	2	2	2
06	Cuaderno de registro – recibido	Cuaderno donde se realizan los registros de documentos que se reciben de otras instituciones o unidades del EP	Primario	Registrar documentos recibidos	Mesa de partes		Jefe de mesa de partes	Confidencial	2	2	2
07	Formatos para redacción de documentos clasificados	Formatos donde se elaboran documentos de carácter clasificado	Primario	Utilizar formato	Sub direcciones		DIE	Secreto	3	3	3
08	Impresoras	Herramienta utilizada para imprimir	Soporte	Imprimir documentos	Subdirecciones		DIE		1	1	1
09	Correo institucional	Correos enviados y recibidos de otros organismos del estado y otras unidades EP	Primario	Enviar y recibir correos	Sub dirección de TI	Servidor	Jefe de área TI		3	3	3

Id	Activo de información			Proceso	Ubicación del activo		Propietario	Clasificación	Valoración		
	Activo	Descripción	Tipo	Actividad	Físico	Lógico			C	I	D
10	Backup de correos	Backup generado tras archivar los correos recibidos de las entidades o unidades del EP	Primario	Archivar correos recibidos	Servidor	Base de datos	Jefe de TI	Confidencial	3	2	2
11	Carpeta compartida	Carpeta compartida por todas las subdirecciones de la DIE para compartir información de interés	Soporte	Importar formatos	Área de TI	En el servidor	Jefe de TI	Confidencial	3	3	3
12	Base de datos del personal	Almacenamiento de datos del personal que labora en la institución	Primario	Almacenar datos	Servidor	En el servidor DB	Jefe del TI	Secreto	3	3	3
13	Reporte de síntesis de información	Documento de síntesis de información que se distribuye a otras dependencias y órganos del EP para toma de decisiones	Primario	Impresión y distribución del reporte	subdirecciones	Servidor	Jefes de sub direcciones	Confidencial	3	3	2
14	Plan operativo institucional	Documento de planes de operaciones a realizarse en el año 2018	Primario	Realizar el POI	Planeamiento		Jefe de planeamiento	Reservado	3	3	3
15	Reporte de informes de las unidades de las regiones	Documento donde se detalla la situación actual de cada región en el ámbito económico, social y político	Primario	Realizar informes	Área Informaciones		Jefe de área de informaciones	Reservado	3	3	2
16	Directivas	Documento donde se plasma los lineamientos sobre funciones y obligaciones de la organización	Primario	Recepción y explotación de directivas	Sub direcciones		DIE	Reservado	3	2	2
17	Memorándum	Memorándum de asignación de responsabilidades según sea el caso y área de responsabilidad	Primario	Formular memorándum	Sub direcciones	servidor	Jefes de sub direcciones	Reservado	2	2	2
18	Escáner	Herramienta para escanear documentos para su envío	Soporte	Escanear documentos	Sub DIE		Encargado		1	1	1

Id	Activo de información			Proceso	Ubicación del activo		Propietario	Clasificación	Valoración		
	Activo	Descripción	Tipo	Actividad	Físico	Lógico			C	I	D
19	Servidor de correo	Realiza la administración de correos (envíos y recepción)	Primario	Administrar correos	servidor		Jefe de TI		3	3	2
20	CD	CD con imágenes, videos, documento y exposición de planes de seguridad	Soporte	Grabar imágenes y videos	Sub direcciones		Jefes de sub direcciones	Reservado	3	2	2
21	CD con backup	CD con backup de síntesis de información mensual	Soporte	Gravar SID	Área de informaciones		Jefe de informaciones	Reservado	3	2	2
22	Sistema de cámaras de seguridad	Cámara que graban en ingreso y salida por la puerta principal y áreas comunes de la DIE	Soporte	Gravar permanentemente	Área de CCTV		Jefe de CCTV		2	2	2
23	Base de datos de producción	Base de datos ubicado en el área de TI contiene información utilizada por los usuarios para el trabajo diario	Soporte	Almacenar base de datos	Área de TI		Jefe de TI		3	3	3
24	Archivo	Área donde se almacena informaciones clasificada en físico	Primario	Almacenar información clasificada	Área de archivo		Jefe de archivos	Secreto	2	2	2
25	UPS power ware	3 UPS utilizado para mantener la operatividad de los servidores y base de datos del data center	Soporte	Mantener la operatividad	Área de TI		Jefe de TI		1	1	1
26	Cableado estructural	Red de cables Cat5e en todas las áreas Dirección según necesidad	Soporte	Mantener en red a los usuarios	Áreas de la DIE		Jefe de TI		2	2	2
27	Firewalls	Cortafuego que permite reducir los riesgos de internet	Soporte	Proteger la red	Área de TI		Jefe de TI		2	2	3

Id	Activo de información			Proceso	Ubicación del activo		Propietario	Clasificación	Valoración		
	Activo	Descripción	Tipo	Actividad	Físico	Lógico			C	I	D
28	Dispositivos móviles	Dispositivos que permiten la comunicación de los usuarios de la organización	Soporte	Comunicación de usuarios	Prevención – guardia		Oficial de guardia		2	2	2
29	Routers	Dispositivo que permite la interconexión de la internet con los usuarios	Soporte	Interconectar	Área de TI		Jefe de TI		2	2	3
30	Telefonía fija	Dispositivo que permite la comunicación vía teléfono	Soporte	Realizar o recepcionar llamadas	Secretaría de la DIE		Secretarios		2	2	1
31	Sistema operativo	Plataforma que permite la interacción del hardware con el usuario	Primario	Interfaz de conexión del computador con el usuario	PCs de la DIE	Computador	La DIE		1	2	3
32	Control de accesos	Documento donde establece las políticas y lineamientos de seguridad para la organización	Primario	Controlar accesos	Prevención - Guardia		Oficial de guardia	Reservado	3	3	3
33	Instalación	Lugar, área donde está ubicada la dirección	Soporte	Alojamiento de activos	DIE		Director		2	2	2
34	Electricidad	Fluido eléctrico que permite el funcionamiento de los equipos de la organización	Soporte	Mantener con fluido eléctrico la dirección	DIE		Sub director		2	2	3
35	Políticas de la organización	Documento que establece las políticas y lineamientos de la organización	Primario	Implementar políticas de seguridad	Área de administración		Jefe de administración	Confidencial	3	3	3
36	Calves criptográficas	Son aquellos que permiten cifrar la información. Incluye los algoritmos de encriptación	Primario	Cifrar la información clasificada de la organización	Área de criptografía	Aplicativo	Jefe de criptografía	Secreto	3	3	3

Metodología de Análisis y Evaluación de Riesgo

Metodología MAGERIT, es una Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información elaborado por el CSAE (Consejo Superior de Administración Electrónica) que supone los beneficios evidentes de emplear las tecnologías de información, pero gestionando los riesgos inherentes a ella.

El objetivo principal de MAGERIT es proteger los activos informáticos en pro de ayudar el alcance de la misión de la organización de acuerdo a las Dimensiones de Seguridad propuestas.

Identificación de Amenazas: Las amenazas son los eventos que ocurren sobre un activo que podría causarle daño a la dirección. MAGERIT emplea un catálogo de amenazas posibles sobre los activos de un sistema de información, los cuales están clasificados de la siguiente manera:

Tabla 38: Identificación de amenaza y definición

Tipo de amenaza	Definición
Ataques intencionados	Fallos deliberados causados por personas
Desastres naturales	Sucesos que pueden ocurrir sin intervención de seres humanos
De origen industrial	Sucesos que pueden ocurrir de manera accidental o deliberada
Errores y fallos no intencionados	Errores o fallos causados por personas

Fuente: MAGERIT

Valoración de Amenazas: Para establecer la valoración de las amenazas es necesario determinar la probabilidad de ocurrencia, la misma que se muestra en el siguiente cuadro:

Tabla 39: Rango, valor y probabilidad de ocurrencia de amenazas

Probabilidad	Valor	Rango
Muy alta	5	Una vez al día
Alta	4	Una vez a la semana
Media	3	Una vez al mes
Baja	2	Una vez en el semestre
Muy baja	1	Una vez al año

Fuente: Elaboración propia

Valoración del impacto: Se determina la valoración de los activos de la dirección de acuerdo al tipo Cualitativo que establece MAGERIT y el impacto que tiene en la institución, de acuerdo a la siguiente escala:

Tabla 40: Valoración del impacto y su descripción

Impacto	Valor	Descripción
Muy alto	5	El daño tienen consecuencias muy graves y podrían ser irreversibles
Alto	4	El daño tiene consecuencias muy graves para la dirección
Medio	3	El daño es relevante puede afectar algunos procesos de la dirección
Bajo	2	El daño tiene consecuencias relevantes, pero no afecta a la dirección
Muy bajo	1	El daño no contiene consecuencias relevantes para la dirección

Fuente: Elaboración propia

Riesgo: el riesgo es la medida probable de daño sobre un sistema el cual es posible determinar directamente conociendo la probabilidad de ocurrencia de una amenaza sobre un activo y el impacto. Por ende, el riesgo es calculado como:

Riesgo = Probabilidad (P) x Impacto (I)

Tabla 41: Nivel de riesgo

	Nivel de riesgo				
I \ P	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Fuente: Elaboración propia

Valoración del riesgo: Se establece la valoración de riesgo evaluando sobre los diferentes niveles de riesgo que determinan el grado de ocurrencia de una amenaza que puedan influir significativamente en la seguridad de la información de la dirección.

Tabla 42: Valoración de riesgo

Nivel de riesgo	Valor	Descripción
Muy alto	20,25	Riesgo con consecuencias muy graves y podrían ser irreversibles
Alto	12,15,16	Riesgo con consecuencias graves para la organización
Medio	6,8,9,10	Riesgo relevante que puede afectar algunos procesos de la organización
Bajo	3,4,5	Riesgo con consecuencias que no afectan la organización
Muy bajo	1,2	Riesgo irrelevante para la organización

Fuente: Elaboración propia

Matriz de Riesgo

Id Riesgo	Activo	Identificación de riesgo			Evaluación de riesgo			Tratamiento de riesgo
		Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Control
R01	Orden de servicio	Fuego	Falta de capacitación en uso de extintores al personal militar	Daño o deterioro debido al incendio,	3	3	9	Se debe capacitar al personal militar en el uso de equipos contraincendios, de debe tener resguardo de la información
R02	Guía de remisión	Hurto	Dejar la guía de remisión sobre el escritorio	Perdida de la guía de remisión	2	3	6	Se debe cumplir con las políticas de seguridad de la información
R03	Computador de escritorio	Acceso no autorizado a sistemas o redes	El personal no cierra sesión al dejar el puesto de trabajo	Riesgo de pérdida, hurto o modificación de la información	4	5	20	Se debe concientizar al personal en temas de seguridad de información
R04		Error en el uso	Uso incorrecto de software y hardware	Daño o deterioro de las computadoras por errores de uso y desconocimiento de herramientas de trabajo	2	4	8	Se debe establecer procedimientos adecuados de uso del computador
R05		Falla del equipo por tiempo de uso	Perdida de conexión a la red interna e internet	Pérdida de información debido a fallas repentinos de las PC	4	4	16	Se debe establecer procedimientos de reparación del PC
R06		Introducción de software malicioso, virus, troyanos	Falta de actualización de antivirus	Pérdida de la información, daño o deterioro de la PC	2	5	10	Se debe implementar un servicio para monitoreo permanente y detectar irregularidades
R07		Fuego	Falta de capacitación al personal militar en el uso de extintores	Daño o deterioro debido al incendio	2	2	4	Se debe capacitar al personal militar en el uso de equipos contraincendios
R08		Incumplimiento de mantenimiento de la PCs	Mantenimiento insuficiente o inapropiado	Daño o deterior de la computadora por falta de mantenimiento	2	2	4	Se debe establecer procesos, cronograma de mantenimiento
Id	Activo	Identificación de riesgo			Evaluación de riesgo			Tratamiento de

Riesgo								riesgo
		Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Control
R09	Módulo PNP	Incendio	Módulo de material inflamable	Daño o deterioro a causa del incendio	2	5	10	Reubicación del módulo por medidas de seguridad
R10	Cuaderno de registro – remitido	Hurto o modificación del cuaderno de registros	Falta de lugar adecuado para guardar el cuaderno de registro	Riesgo de pérdida, daño o modificación del cuaderno de registro	2	5	10	Se debe habilitar un lugar adecuado para su resguardo
R11	Cuaderno de registro – recibido	Hurto o modificación del cuaderno de registro	Falta de lugar adecuado para guardar el cuaderno de registro	Riesgo de pérdida, daño o modificación del registro	2	5	10	Se debe habilitar un lugar adecuado para su resguardo
R12	Formatos para documento clasificado	Hurto o modificación de formatos	Falta de protección con contraseñas	Riesgo de ser hurtado o modificado	3	3	9	Implementar políticas de seguridad de información
R13	Impresoras	Error de uso	Uso incorrecto de software y hardware	Daño o deterioro de la impresora por mal uso del dispositivo	2	2	4	Se debe contar con manuales que den a conocer sobre el uso correcto de la impresora
R14		Incumplimiento en el mantenimiento de la impresora	Insuficiente mantenimiento	Daño o deterioro de la impresora por falta de mantenimiento	2	3	6	Contar con procedimientos de mantenimiento por averías
R15		Pérdida de suministro de energía	Inactividad del equipo debido a la falta de energía eléctrica	Pérdida de disponibilidad de la impresora por falta de energía eléctrica	2	3	6	Activación del grupo electrógeno de la organización
R16	Correo institucional	Acceso no autorizado al correo	Falta de cierre de sesión cuando se abandona el área de trabajo	Sustracción de información debido a la falta de bloqueo	3	5	15	Se debe concientizar al personal sobre seguridad de la información
R17	Carpeta compartida	Acceso no autorizado al sistema o la red	Falta de cierre de sesión al retirarse del trabajo	Pérdida o sustracción de información	3	2	6	Concientizar al personal sobre seguridad de información

Id Riesgo	Activo	Identificación de riesgo			Evaluación de riesgo			Tratamiento de riesgo
		Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Control
R18	Backup de correos	Acceso de usuarios no autorizados al sistema o red	Falta de cierre de sesión al retirarse del área de trabajo	Borrado o perdida de backup de información del correo	3	5	15	Se debe concientizar al personal en seguridad de información
R19	Base de datos	Abuso de privilegios	Falta de auditorías o supervisiones inopinadas	Hurto de información de la base de datos	2	5	10	La organización debe almacenar logs para su análisis en la auditoría
R20		Usuario mal intencionado	Falta de pruebas de hacking ético	Riesgo de comprometer la información debido a los ataques mal intencionados	2	5	10	Establecer políticas de monitoreo para detectar ataques al sistema
R21	Reporte de síntesis de información	Hurto o modificación de información	Falta de lugar adecuado para guardar información	Pérdida o modificación de la información	1	5	5	Implementar y concientizar políticas d seguridad de información
R22	Plan operativo institucional	Hurto o modificación de información	Acceso de personal no autorizado al área de trabajo	Pérdida o modificación de la información	2	3	6	Implementar políticas de accesos a instalaciones
R23	Reporte de informes de las unidades de regiones	Interceptación física de los reportes de las unidades	Falta de seguridad en el transporte de la valija	Pérdida o reemplazo de la información	3	3	9	Establecer medidas de seguridad para el envío de los informes
R24		Interceptación en el correo o la red	Acceso no autorizado al correo, red	Pérdida de la información daño o cambio de datos del reporte	3	5	15	Establecer políticas de encriptamiento de la información
R25	Directivas	Hurto	Acceso no autorizado de personal de otras áreas	Perdida de las directivas	2	4	8	Establecer medidas se seguridad de información que eviten el hurto
R26	Memorándum	Hurto	Acceso no autorizado de personal de otra área	Perdida de memorándum	2	2	4	Establecer medidas de seguridad de información que eviten el hurto
R27	Escáner	Fuego	Falta de capacitación al personal en uso de extintores, degradación	Deterior del escáner debido al incendio	2	1	2	Se debe instalar equipos de contra incendio

			del activo					
Id Riesgo	**Activo**	**Identificación de riesgo**			**Evaluación de riesgo**			**Tratamiento de riesgo**
		Amenaza	**Vulnerabilidad**	**Riesgo**	**Probabilidad**	**Impacto**	**Nivel de riesgo**	**Control**
R28	Servidor de correo	Abuso de privilegios	Falta de auditorías inopinadas	Información comprometida por acceso de personas ajenas al servidor	2	5	10	Elaborar plan de auditoria para el control respectivo
R29		Usuario mal intencionado	Falta pruebas de hacking empleando ingeniería social	Riesgo de la información debido al ataque malintencionado	2	5	10	Desarrollar plan de análisis de vulnerabilidad
R30	CD con backup	Hurto	Pérdida de CD con backup	Riesgo de perder información clasificada en el CD de backup	2	5	10	Implementar políticas de seguridad para el resguardo adecuado
R31	Sistema de cámaras de seguridad	Pérdida de suministro de energía	Las cámaras conectados directamente al suministro de energía	Riesgo de comprometer la información y activo de la organización	1	2	2	Se debe solicitar compra de UPS
		Usuarios mal intencionados	Borrado de imágenes por el usuario mal intencionado	Riesgo de pérdida de la grabación	2	1	2	Tener copias de respaldo para evitar el borrado de la grabación por ataques al sistema
R32	Base de datos de producción	Abuso de privilegios	Falta de auditorías programadas e inopinadas	Riesgo de comprometer la información debido al no autorizado a la base de datos	2	4	8	La organización debe producir y almacenar los log para su posterior análisis
R33		Usuario mal intencionado	Falta de pruebas de hacking ético	Riesgo de comprometer la información debido a un ataque malintencionado	3	5	15	Debe desarrollar un plan de análisis de vulnerabilidad que permita identificar el problema
R34	Archivo	Incendio	Material altamente inflamable	Pérdida de información clasificada por incendio	3	3	9	Contar con plan de evacuación de los archivos clasificados
R35	UPS power ware	Incumplimiento en el mantenimiento del sistema	Mantenimiento insuficiente	Deterioro de los equipos UPS por falta de mantenimiento	2	1	2	Se debe documentar los procedimientos para el mantenimiento de la UPS

Id Riesgo	Activo	Identificación de riesgo			Evaluación de riesgo			Tratamiento de riesgo
		Amenaza	Vulnerabilidad	Riesgo	Probabilidad	Impacto	Nivel de riesgo	Control
R36	Dispositivos móviles	Dispositivos con software malicioso	Uso de dispositivos móviles en centro de labores	Ataques al sistema desde los dispositivos móviles	3	4	12	Implementar políticas de uso de dispositivos móviles
R37	Routers	Cambio de DNS	Falta de adecuada configuración del router	Ataques al sistema interno o externo	2	4	8	Generar políticas para el permanente de ataques al sistema
R38	Telefonía fija	Interceptación telefónica	Tener la ruleta de conexión en el exterior de la unidad	Revelar información clasificada de	3	5	15	Establecer la revisión periódica de la línea
R39	Sistema operativo	Instalación de software malicioso	Falta de cierre de sesión al alejarse del área de trabajo	Pérdida de información, daños a la PC y apertura de puertas traceras	2	4	8	Realizar auditoria de los software instalados en la PC
R40	Red LAN	Ingreso de personal no autorizado a la red LAN	Falta de monitoreo de la red LAN	Denegación de servicios, robo de información, daños a la red LAN	3	5	15	Implementar monitoreo permanente de la red LAN
R41	Electricidad	Corte intempestivo	Pérdida de información, interrupción del trabajo retrasando los resultados	Daño de los equipos informáticos y pérdida de información	1	2	2	Recomendar la reparación del electrógeno para su uso
R42	Políticas de la organización	Alteración de las políticas de la organización	Cambios sin autorización de la alta dirección	Tergiversación en la toma de decisiones del alto mando	2	2	4	Implementar medidas de seguridad para el resguardo del documento

FASE VERIFICAR

Aplicabilidad de controles de la NTP ISO/IEC 27001:2014

Se ha desarrollado la aplicabilidad de los controles conforme establece la NTP ISO/IEC 27001:2014, para posteriormente desarrollar las políticas de seguridad de la información como parte de la implementación de SGSI.

FICHA DE APLICABILIDAD DE CONTROLES DE LA NTP ISO/IEC 27001

N°	POLÍTICAS	CONTROLES DE LA NTP ISO 27001	APLICA	
			SI	NO
A.5.1	seguridad de información	Definir, aprobar y comunicar de políticas para la seguridad de la información por el comando de la dirección	X	
A.5.2	Revisión	Verificar las políticas para la seguridad de la información a intervalos planificados y asegurar su efectividad continúa.	X	
A.6.1	Roles y responsabilidades	Definir y asignar las responsabilidades de seguridad de la información.	X	
A.6.2	Segregación de funciones	Segregar las funciones y áreas de responsabilidad reduciendo el mal uso de los activos de la dirección.	X	
A.6.3	Contacto con autoridades	Mantener los contactos apropiados con autoridades relevantes.	X	
A.6.5	Gestión de proyectos	De debe mantener la seguridad de la información en la gestión de proyectos.	X	
A.6.7	Dispositivos móviles	Adoptar medidas de seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles.	X	
A.6.7	Teletrabajo	Implementar medidas de seguridad para proteger información a la que se accede, se procesa o almacena en sitios de teletrabajo.		X
A.7.1	Selección	Verificación de antecedentes de los empleados, la clasificación de la información a la que se tendrá acceso y los riesgos percibidos.	X	
A.7.2	Capacitación	Recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización.	X	
A.7.3	Proceso disciplinario	Tomar acción contra empleados que hayan cometido una infracción a la seguridad de la información.	X	

Tabla 43: Aplicabilidad de controles de NTP ISO/IEC 27001

N°	POLÍTICAS	CONTROLES DE LA NTP ISO 27001	APLICA	
			SI	NO
A.7.4	Terminación o cambio del empleo.	Definir y comunicar las responsabilidades y deberes de seguridad de la información al empleado o contratista y forzar su cumplimiento.	X	
A.8.1	Inventario de activos	Identificar los activos asociados con información e instalaciones de procesamiento de información.	X	
A.8.2	Clasificación de la información	Clasificar la información en términos legales, valor y criticidad respecto a una divulgación o modificación no autorizada.	X	
A.8.3	Manejo de activos	Desarrollar e implementar procedimientos para el manejo de activos	X	
A.8.4	Medios removibles	Implementar procedimientos para la gestión de medios removibles.		X
A.9.1	Control de acceso	Establecer políticas de control de acceso, basada en seguridad de la información.	X	
A.9.2	Acceso a redes y servicios de red	Tener autorización para acceso a la red y servicios de red.	X	
A.9.3	Registro y baja de usuarios	Implementar un proceso formal de registro y baja de usuarios.	X	
A.9.4	Derechos de acceso de usuarios	Revisar los derechos de acceso de usuario a intervalos regulares.	X	
A.9.5	Acceso a la información	Restringir el acceso a la información en concordancia con la política de acceso.	X	
A.9.6	Gestión de contraseñas	Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	X	
A.10.1	Criptográficos	Desarrollar e implementar los controles criptográficos.	X	
A.10.2	Gestión de claves	Implementar políticas sobre el uso, protección y tiempo de vida de las claves criptográficas.	X	
A.11.1	Seguridad física	Definir áreas críticas de instalaciones de procesamiento de la información.	X	
A.11.2	Ingreso físico	Asegurar controles para permitir el acceso sólo al personal autorizado.	X	
A.11.3	Amenazas externas y ambientales	Diseñar y aplicar protección física contra desastres naturales, ataque malicioso o accidentes.	X	
A.11.4	Áreas de despacho y carga	Controlar las áreas de despacho, carga y otros puntos.		X
A.12.1	Entornos de desarrollo, operación y pruebas	Separar los entornos de desarrollo, pruebas y operaciones para reducir los riesgos de acceso no autorizado o cambios.		X
A.12.2	Códigos maliciosos	Implementar controles de detección, prevención y recuperación para proteger contra códigos maliciosos a los usuarios.	X	
A.12.3	Respaldo de la información	Realizar copias de respaldo de la información con regularidad en concordancia con una política de respaldo acordada.	X	

A.12.4	Registro de eventos	Revisar los registros (logs) de eventos de actividades de usuarios, fallas y eventos de seguridad de la información.	X	
A.12.5	Gestión de vulnerabilidades	Obtener información sobre vulnerabilidades técnicas de los sistemas de información para su posterior evaluación y el resolver el riesgo.	X	
A.12.6	Auditoría de sistemas de información	Planificar las auditorías y las actividades que involucran la verificación de sistemas operacionales.	X	
A.13.1	Controles de la red	Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	X	
A.13.2	Transferencia de la información	Aplicar políticas de seguridad de información para proteger la transferencia de información.	X	
A.13.3	Mensajes electrónicos	Proteger apropiadamente la información involucrada en mensajería electrónica.	X	
A.14.1	Servicios de aplicaciones	Proteger la información involucrada en servicios de aplicaciones que pasa sobre redes públicas.	X	
A.14.2	Transacciones en servicios de aplicación	Proteger la información involucrada en las transacciones de servicios de aplicación.		X
A.14.3	Ambiente de desarrollo seguro	Establecer y proteger apropiadamente los ambientes de desarrollo seguros para los esfuerzos de desarrollo e integración de sistemas.	X	
A.14.4	Desarrollo externo	Supervisar y monitorear la actividad de desarrollo de sistemas contratado externamente.		X
A.14.5	Protección de datos de prueba	Los datos de prueba deben ser seleccionados cuidadosamente, protegidos y controlados.		X
A.15.1	Relaciones con los proveedores	Mitigar los riesgos asociados con el acceso por parte del proveedor a los activos de la organización.	X	
A.15.2	Monitoreo y revisión de servicios	Monitorear, revisar y auditar regularmente la entrega de servicios por parte de los proveedores.	X	
A.16.1	Reporte de eventos	Reportar los eventos de seguridad de la información a través de canales de gestión apropiados.	X	
A.16.2	Reporte de debilidades	El personal y contratista debe reportar las debilidades observadas o de la sospecha en cuanto a seguridad de la información.	X	
A.16.3	Respuesta a incidentes	Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	X	
A.16.4	Evidencia	Definir y aplicar procedimientos para la identificación, recolección y preservación de información que pueda servir como evidencia.	X	
A.17.1	Planificación de continuidad	Determinar los requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información.	X	
A.17.2	Implementación de continuidad	Establecer, documentar, implementar y mantener procesos y controles para asegurar la continuidad de seguridad de la información en situaciones adversas.	X	
A.17.3	Verificación, revisión y evaluación de continuidad	Verificar los controles de continuidad de seguridad de la información establecidos para asegurarse que son válidos y efectivos en situaciones adversas.	X	

A.18.1	Derechos de propiedad intelectual	Implementar procedimientos regulatorios y contractuales relacionados a los derechos de propiedad intelectual.		X
A.18.2	Protección de registros	Proteger los registros de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada.	X	
A.18.3	Protección de datos personales.	Asegurar la privacidad y la protección de datos personales de acuerdo a la legislación y regulación donde sea aplicable.	X	
A.18.4	Cumplimiento de políticas y normas de seguridad	Revisar regularmente el cumplimiento del procesamiento de la información y de los procedimientos dentro de su área de responsabilidad.	X	
TOTAL			47	8

Fuente: NTP ISO/IEC 27001-Elaboración propia

FASE ACTUAR

POLÍTICAS DE SEGURIDAD DE LA DIRECCIÓN DE INFORMACIONES DEL EJÉRCITO

La institución como parte del Ejército del Perú, claramente comprometido con la seguridad de la información y por recomendación, implementó el sistema de gestión de seguridad de la información (SGSI), sustentado en los lineamientos de la Norma Técnica Peruana ISO/IEC 27001:2014 y en cumplimiento de la Resolución Ministerial N° 004-2016-PCM.

1. **Objetivos**

   Dar a conocer al personal de la Dirección de Informaciones del Ejército del Perú la importancia de la gestión de seguridad de información en la institución toda vez que administra información clasificada.

   Establecer e indicar el conjunto de instrucciones o normas generales necesarias para la operación y buscar mejorar la disponibilidad, integridad y confiabilidad de la información procesada por los diferentes órganos o unidades del Ejército.

   Este documento describe el uso adecuado de los servicios, aplicativos, equipos de cómputo y la red.

2. **Alcance**

   Las políticas de seguridad de información son de carácter obligatorio para todo el personal de la Dirección de Informaciones del Ejército del Perú y terceros que tengan alguna relación de contrato, proveedor o servicios que involucren algún proceso de seguridad de información de la institución.

3. **Responsabilidades**

   Se cuenta con las siguientes responsabilidades relacionadas a la seguridad de información en el proceso de sistema de gestión de seguridad de la información (SGSI):

   a. **Comité de seguridad de información**. La responsabilidad es asumido por un jefe del área TI de la Dirección y otros miembros que representan a las principales áreas involucradas en el SGSI (Jefe de

Planeamiento y Presupuesto, Jefe de Operaciones y el Oficial de Seguridad de Información, como secretario), El comité de seguridad de información ha implementado y realizado las actividades siguientes:

- Recomendar al Director de informaciones la aprobación del cronograma de las actividades para identificar activos, vulnerabilidades y amenazas con el objetivo de implementar controles del SGSI.
- Formular la documentación de políticas de seguridad de información y alcance del SGSI.
- Participar de la auditoría interna verificando los controles de acuerdo a la norma técnica peruana.
- Designar los recursos entre ellos al personal, equipos y servicios necesarios para desarrollar la identificación de activos, vulnerabilidades, amenazas y riesgos.
- Elaboración de la documentos (planes, informes y procedimientos) requeridos para las actividades de implementación del SGSI en la dirección.

b. **Oficial de seguridad de información.** Responsabilidad asumida por el autor del trabajo de investigación como parte del desarrollo de las funciones como encargado del “Departamento de Seguridad” lo que facilita en desarrollo del trabajo de investigación de Seguridad de Información; se realiza las siguientes actividades:

- Elaborar memorándums internos para desarrollar y coordinar sobre la implementación del SGSI en la dirección.
- Brindar asesoramiento al comando de la dirección sobre la gestión de riesgos de seguridad de información.
- Gestionar la realización de las charlas y capacitaciones de seguridad de información planteadas por la NTP ISO/IEC 27001
- Gestionar la identificación de activos críticos de la dirección de acuerdo a la norma técnica peruana de seguridad de información.
- Realizar análisis de gestión de riesgos empleando la metodología del ciclo Deming PDCA.

- Establecer la aplicabilidad de los controles de la NTP ISO/IEC 27001 de seguridad de información

c. **Auditor informático.** La responsabilidad es asumido por el Auditor designado por la dirección y participa de las siguientes actividades:
   - Elabora el Plan de Auditoría Interna, basado en los controles de la NTP ISO/IEC 27001.
   - Realiza inspecciones, pruebas y revisión de evidencias relacionadas a la auditoría interna del sistema de gestión de seguridad de información.
   - Elabora los informes de resultados de la auditoría interna de la dirección.

4. Normas legales

a. En la dirección el responsable de identificar las normas de legislación aplicables a la organización que puedan afectar a la seguridad de información es el Jefe del Departamento Jurídico, en coordinación con el Oficial de Seguridad de Información.
b. Como parte de la seguridad de la información la dirección reconoce, entre otros las siguientes normas legales “Ley de Protección de Datos Personales, Ley de Derecho del Autor, Ley de Delitos Informáticos, Ley de Firmas Digitales”.

5. Riesgos e incidentes

a. Establecer los activos críticos de la dirección mejorando en los procesos
b. Gestión de riesgos comprende la identificación, análisis, evaluación y tratamiento de los riesgos relacionados a la seguridad de la información.
c. Para realizar la gestión de riesgos, se empleará la Metodología de Gestión de Riesgos.

d. Personal que trabaja en la dirección, está obligado a reportar los incidentes relacionados a la seguridad de la información o eventos que tengan relación con los activos críticos de seguridad de información.
e. El Oficial de seguridad de información de la dirección es responsable de mantener el contacto con el Departamento de Cyberdefensa del EP, para atender los incidentes que no pudiera resolver el personal de TI de la dirección.

6. Consideraciones generales de seguridad de información

La Dirección dispone consideraciones generales de seguridad de información las cuales deben ser acatadas de forma **obligatoria** por todo el personal que labora en la dirección, siendo según se indica a continuación:

a. Institucional

- El activo que contenga información de la Dirección y que requiera ser trasladado fuera de institución, debe estar autorizado por el comando.
- Los cambios en los procesos, personal o infraestructura debe ser autorizado por el comando de la Dirección.
- Los proyectos a desarrollarse están bajo responsabilidad de las subdirecciones involucradas, en todo momento se deban tomar las medidas de seguridad de la información frente a riesgos que puedan involucrar su ejecución.

b. Personales

- El personal que labora en la dirección cuando se retira del trabajo de manera temporal debe bloquear la pantalla de su equipo o apagar en caso se retire del trabajo.
- El personal es responsable de la información sensible expuesta en su escritorio.
- Para evitar que personal no autorizado, tenga acceso a los archivos almacenados en la computadora, se implementaran tres niveles de protección de acceso a la computadora: primer nivel clave de acceso a nivel bios, segundo nivel clave de acceso a nivel sistema

operativos, tercer nivel clave de acceso a nivel software como el de protector de pantalla, para evitar que personal no autorizado encienda e ingrese a los diferentes archivos.

- Queda terminantemente prohibido la instalación de software en los equipos de cómputo de la dirección, sólo el personal de servicios del área de TI está autorizada a instalar.
- Está prohibido llevar al centro de trabajo computadoras personales para formulación de documentación clasificada, asimismo el personal que labora en la dirección no debe sacar de las instalaciones documentación clasificada.
- Se prohíbe al personal que labora en la dirección realizar conexiones se sus equipos celulares a los equipos de cómputo de la dirección.
- Está prohibido bajo responsabilidad que el personal que labora en la dirección transporte y saque en dispositivos de almacenamiento externo como DVD, CD, USB y otros conteniendo información clasificada.

7. Control de acceso a la red

Para el acceso a la red se consideran los siguientes lineamientos, los cuales serán aplicados a través del procedimiento de gestión de accesos:

a. El operador de servicios de TI es el responsable de asignar equipos de trabajo con acceso a la red interna de la dirección.
b. La asignación de cuentas de usuario al personal de la dirección es autorizado por el Jefe del área de TI.
c. Mantener configuraciones que obliguen a los usuarios a tener cuentas con contraseñas seguras, bloqueo por inactividad, cambio de contraseña, entre otros.
d. Los servicios tecnológicos que contengan información de la dirección, deberán estar sujetos a mecanismos de autenticación.
e. Las subdirecciones deben comunicar al servicio de TI sobre el cese o cambio de personal para el retiro de accesos o actualización del usuario.

f. El oficial de seguridad y el encargado de servicios de TI deberán realizar revisiones periódicas de los accesos asignados al personal de la dirección.

8. Seguridad informática

El Jefe del área TI de la Dirección es la responsable de distribuir y aplicar controles de seguridad y criptográficos, bajo solicitud formal de cada área responsable.

a. Los dispositivos que cuentan con información sensible deberán ser encriptados.
b. Antivirus y firewalls de detección de amenazas informáticas.
c. La eliminación de registros de bitácoras de auditoría, sobre los usuarios y administradores, debe ser con autorización del comando.
d. Análisis de vulnerabilidades sobre las plataformas informáticas de la dirección.

9. Equipos informáticos

El personal del área de servicios de TI es responsable de administrar los equipos informáticos de la dirección, mediante las siguientes actividades:

a. Instalar o gestionar los equipos informáticos adquiridos por la Dirección, adoptando las recomendaciones del fabricante y las mejores prácticas de seguridad.
b. Personal de TI debe ejecutar el mantenimiento preventivo de los equipos de la dirección, así como el correctivo de insidentes.
c. En caso de transferir o dar de baja los equipos se debe formatear y eliminar los componentes que contienen información clasificada.

10. Gestión de redes

El personal del área de servicios de TI es responsable de administrar la infraestructura y servicios de la Dirección, a través de las siguientes actividades:

a. Administrar el firewall, y otras herramientas de seguridad de información.
b. La red interna debe estar independizada en segmentos y además aislada de la red externa como es internet.
c. El servicio de correo electrónico debe estar bajo arquitectura y protocolos seguros.

11. Gestión de activos

La dirección define las siguientes políticas para la administración de los activos críticos:

a. El Oficial de seguridad de información debe mantener el inventario de los activos críticos de seguridad de información de la dirección.
b. Los activos críticos involucrados en seguridad de información fueron identificados en la matriz de evaluación de riesgos.
c. Toda información impresa debe ser sellada con la etiqueta de “confidencial”, “reservado” o “secreto” según corresponda, antes de su distribución autorizada.
d. Los equipos y repositorios de información que por motivos de mantenimiento, sean llevados fuera de las instalaciones de la dirección, deben contar con el permiso del comando.

12. Seguridad física

El oficial de seguridad de la dirección, es responsable de velar por el mantenimiento y operación adecuado de los controles físicos que la dirección ha implementado:

a. Verificar el cumplimiento de las funciones del servicio de vigilancia de la misma forma revisar los registros de los incidentes.
b. Implementar y verificar el servicio de CCTV - videograbación en las inmediaciones y dentro de la Dirección.
c. Verificar el funcionamiento adecuado de las cerraduras en los ambientes de trabajo de la Dirección.

d. Contar con mecanismos de detección y reacción ante amenazas de desastres naturales como como sismo, inundaciones, incendio, corto circuito, humedad u otros.
e. En la dirección, mantener los mecanismos de contingencia eléctrica en condiciones adecuadas.
f. Controlar el acceso al área donde se encuentra información clasificada, llevando el registro de acceso del personal autorizado.

13. Responsabilidades del Usuario

Todo el personal de la Dirección que maneja activos de información e infraestructura tecnológica tiene la denominación de usuario y tiene las siguientes responsabilidades:

a. Almacenamiento de información de la Dirección, custodiar la información confiada, usar el sistema de control de acceso lógico y ejecutar periódicamente copias de seguridad.
b. Aplicación, mantenimiento y revisión las medidas de seguridad de información definidas por los encargados de la información.
c. Aplicación de las políticas de seguridad de la información, normas, procedimientos y legislación aplicable. Deben comprender perfectamente estos requisitos y cumplir con ellos.
d. Actualización de la información de registro de inventario de activos.
e. Identificación del nivel de clasificación de los activos de información.
f. Aplicación de los controles apropiados para asegurar la confidencialidad, integridad y disponibilidad de la información.

Diagrama de procesos

Diagrama de procesos de identificación de activos críticos del departamento de Administración:

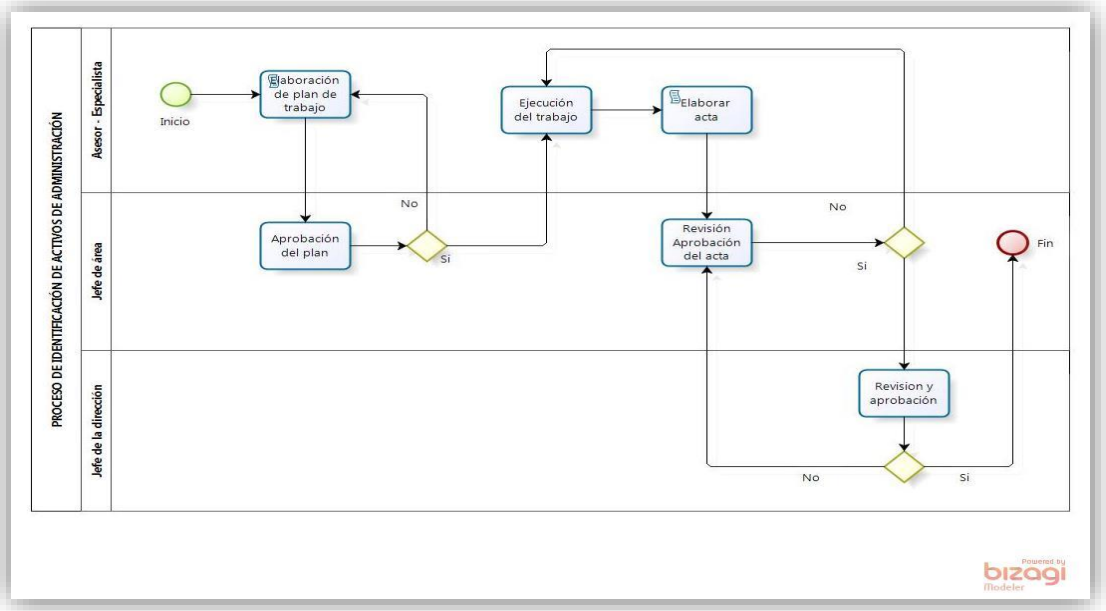


Figura 41: Procesos de identificación de activos
Fuente: Elaboración propia

Diagrama de procesos de identificación de activos críticos del departamento de mesa de partes

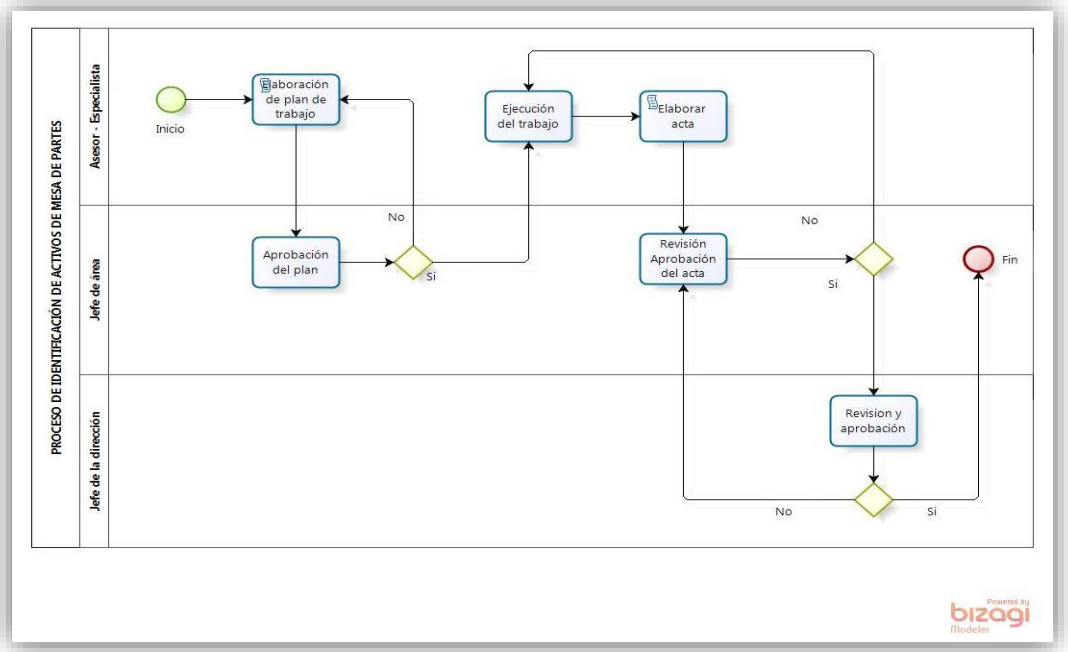


Diagrama de procesos de identificación de activos críticos del departamento de criptología

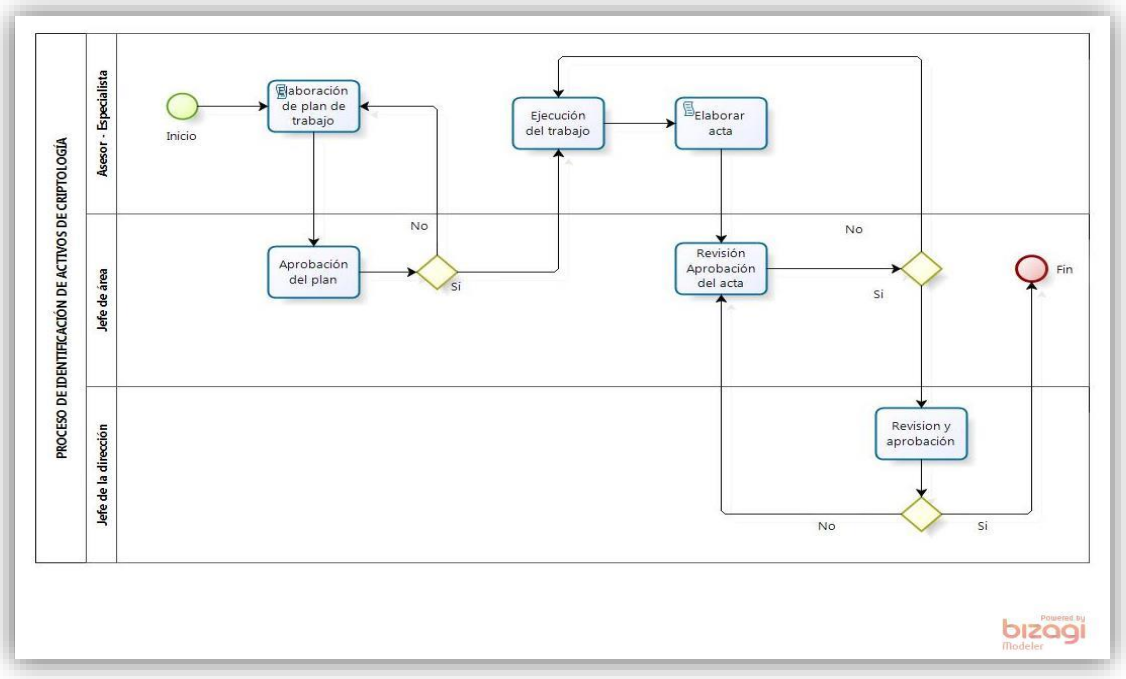


Diagrama de procesos de identificación de activos críticos del departamento de informaciones:

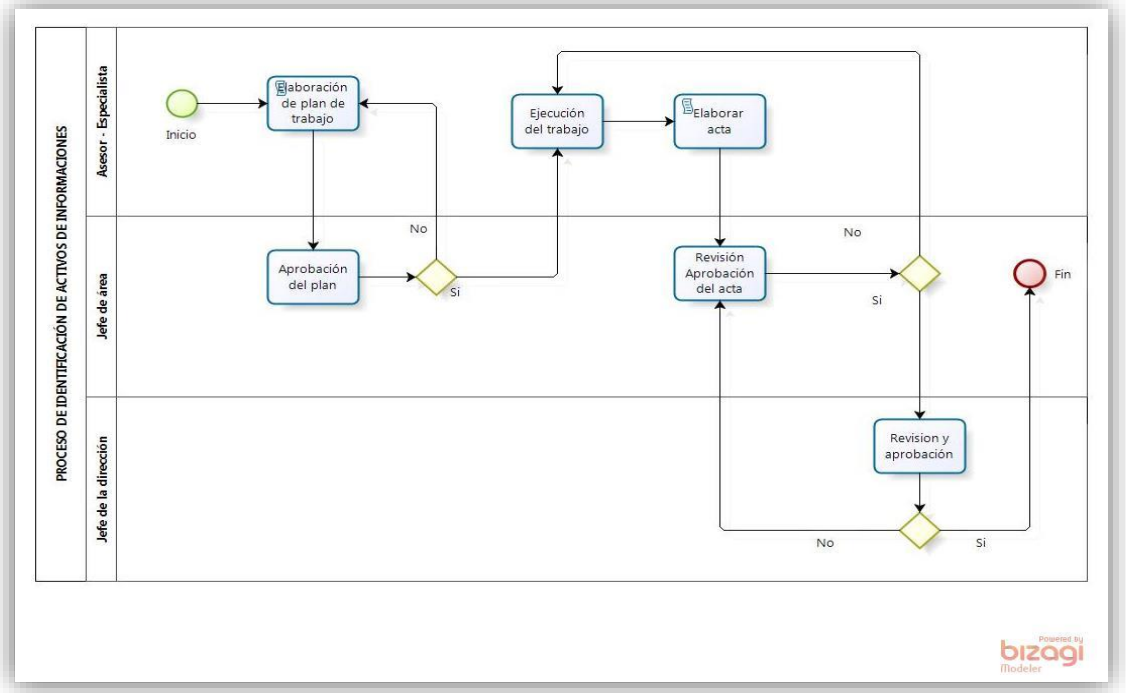


Diagrama de procesos de identificación de activos críticos del departamento de Planeamiento:

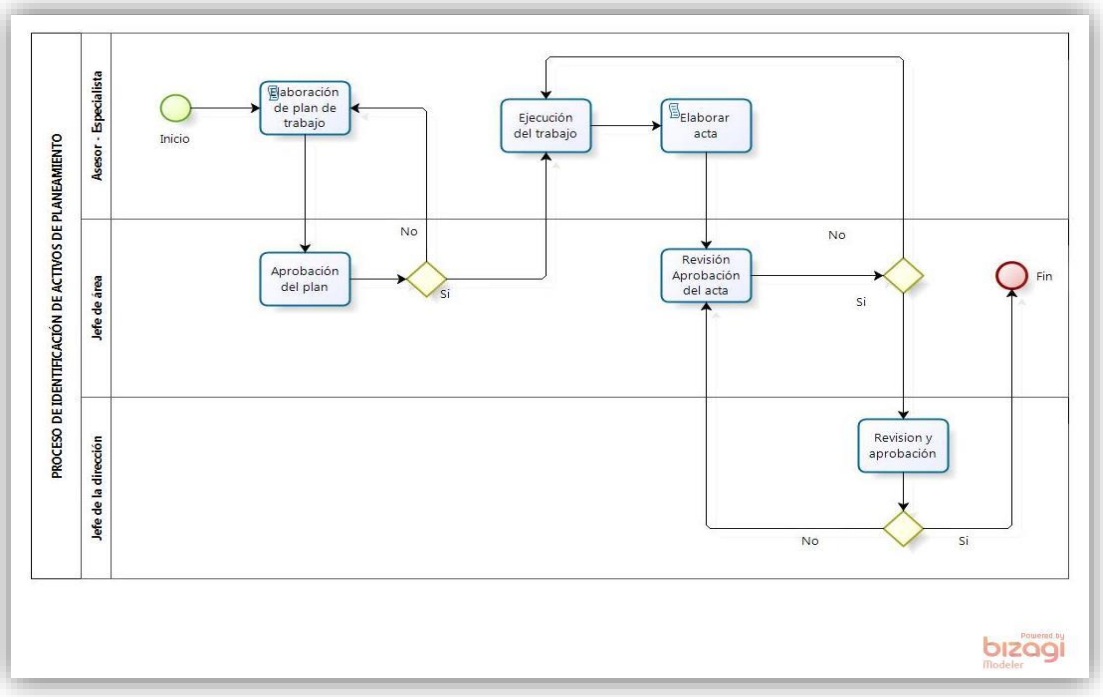


Diagrama de procesos de identificación de activos críticos del departamento de presupuesto:

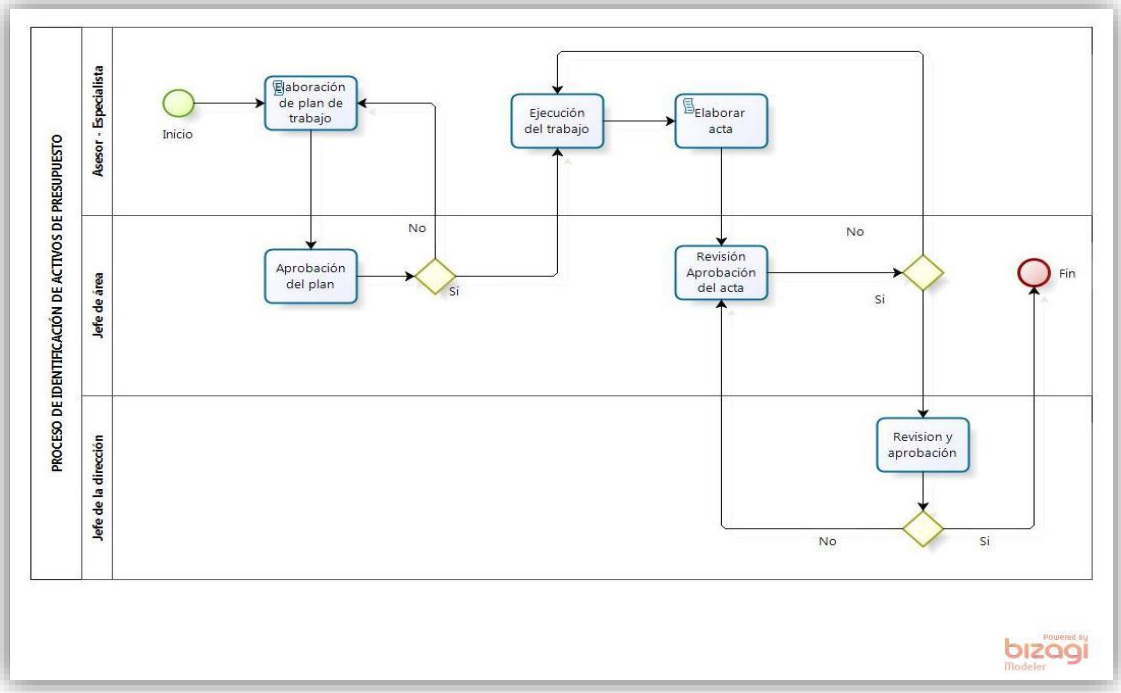


Diagrama de procesos de identificación de activos críticos del departamento de organización:

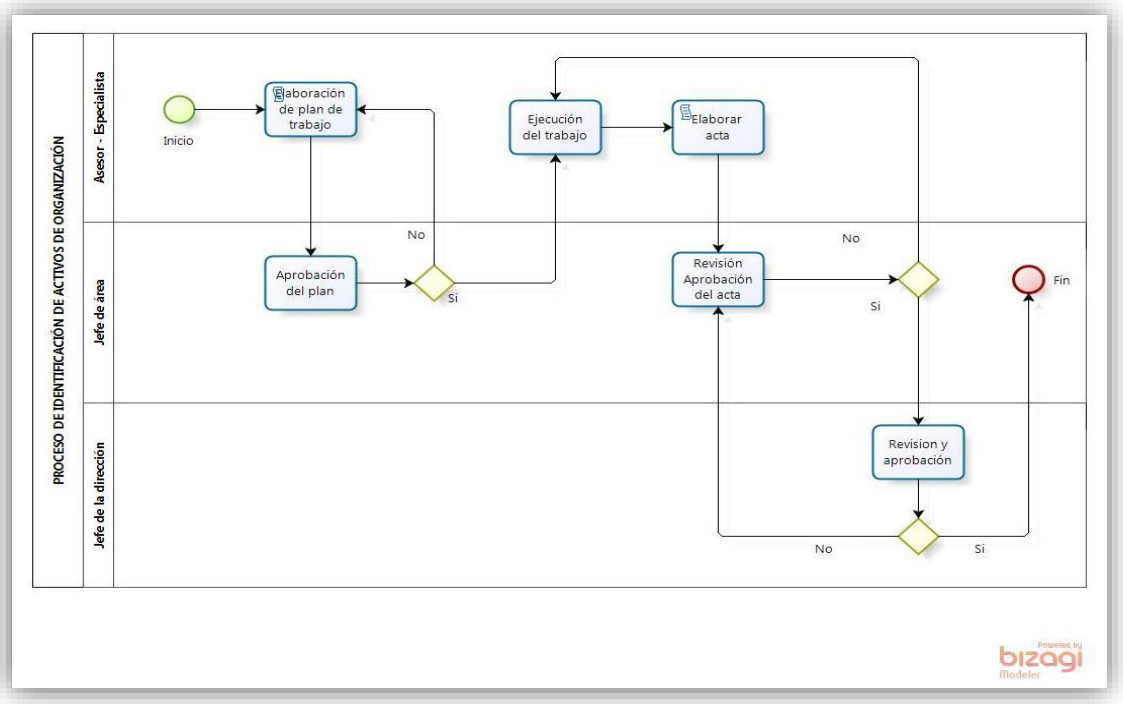


Diagrama de procesos de identificación de activos críticos del departamento de inteligencia:

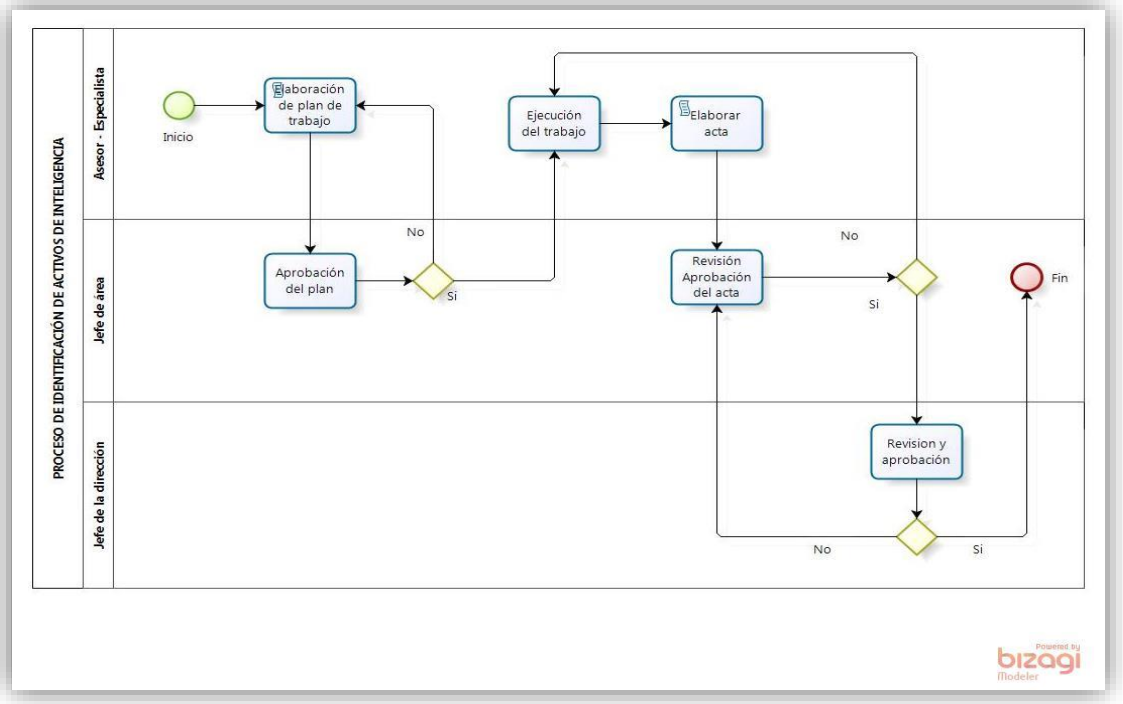


Diagrama de procesos de identificación de activos críticos del departamento de jurídico:

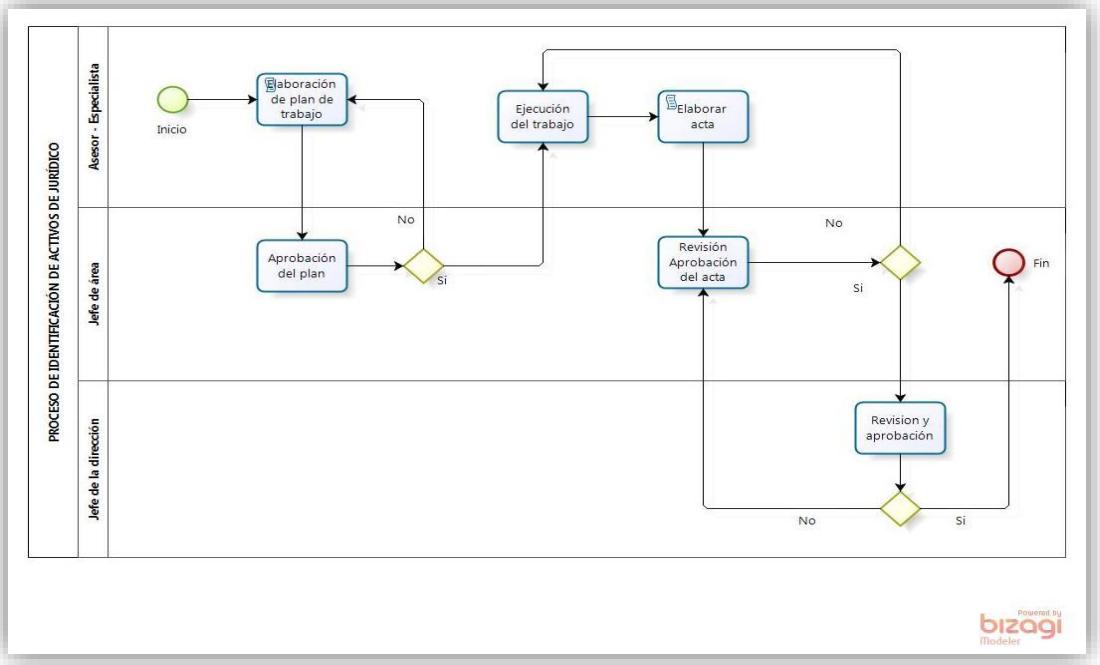


Diagrama de procesos de identificación de activos críticos del departamento de economía:

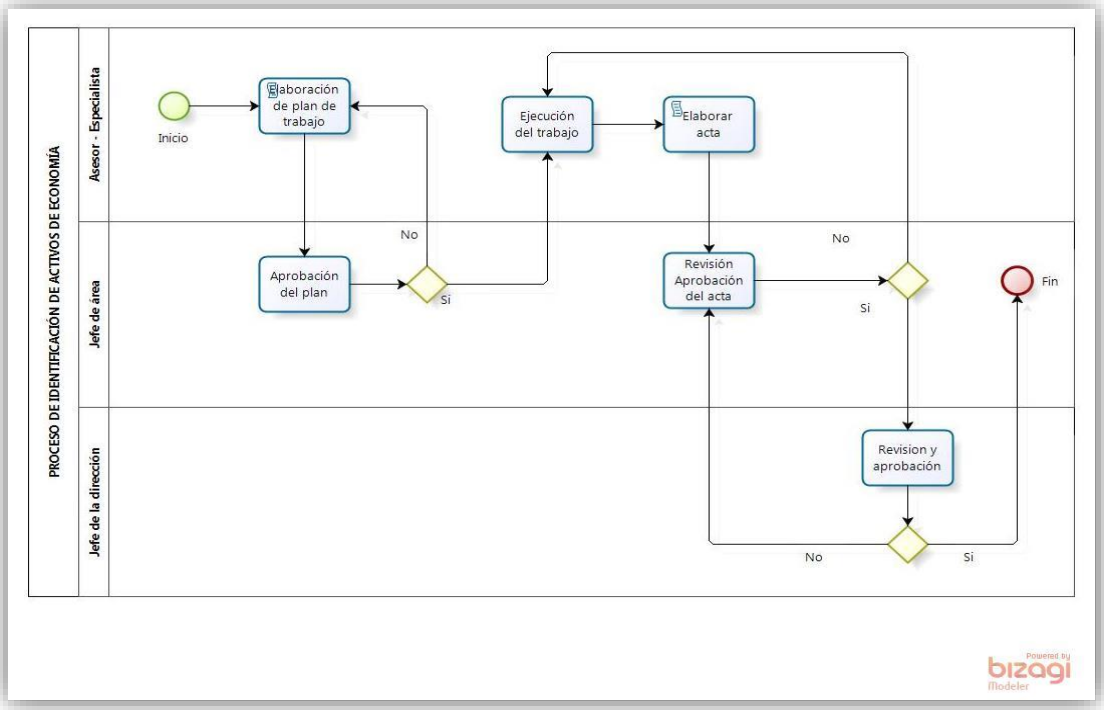


Diagrama de procesos de identificación de activos críticos del departamento de control interno:

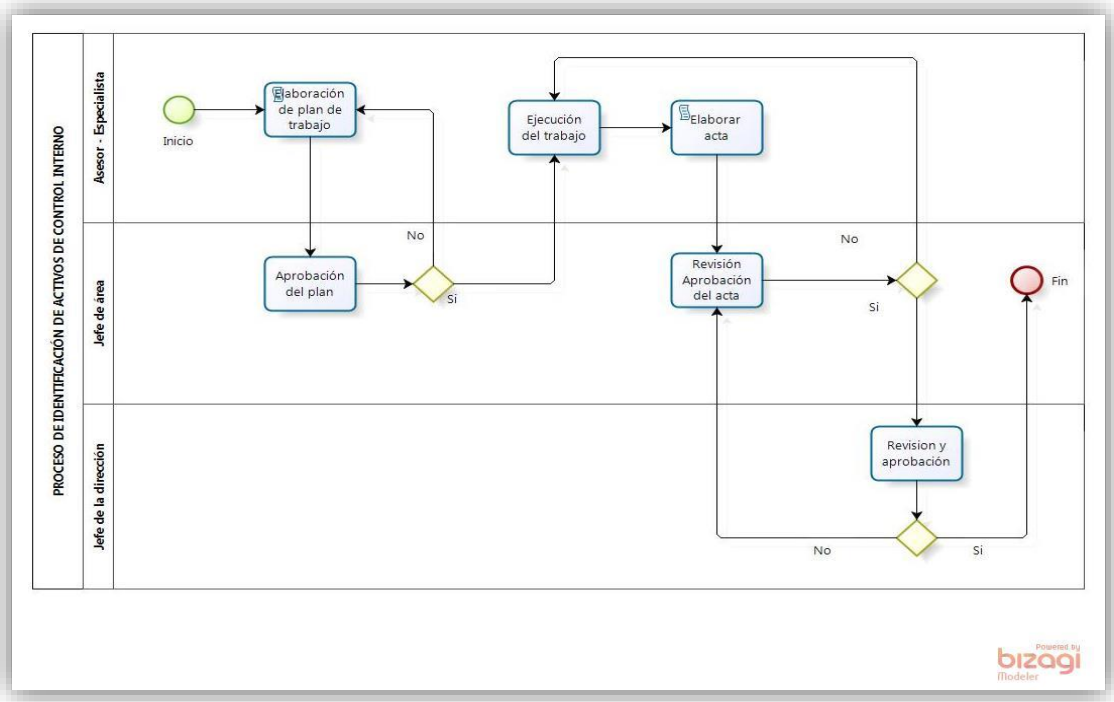


Diagrama de procesos de identificación de activos críticos del departamento de seguridad:

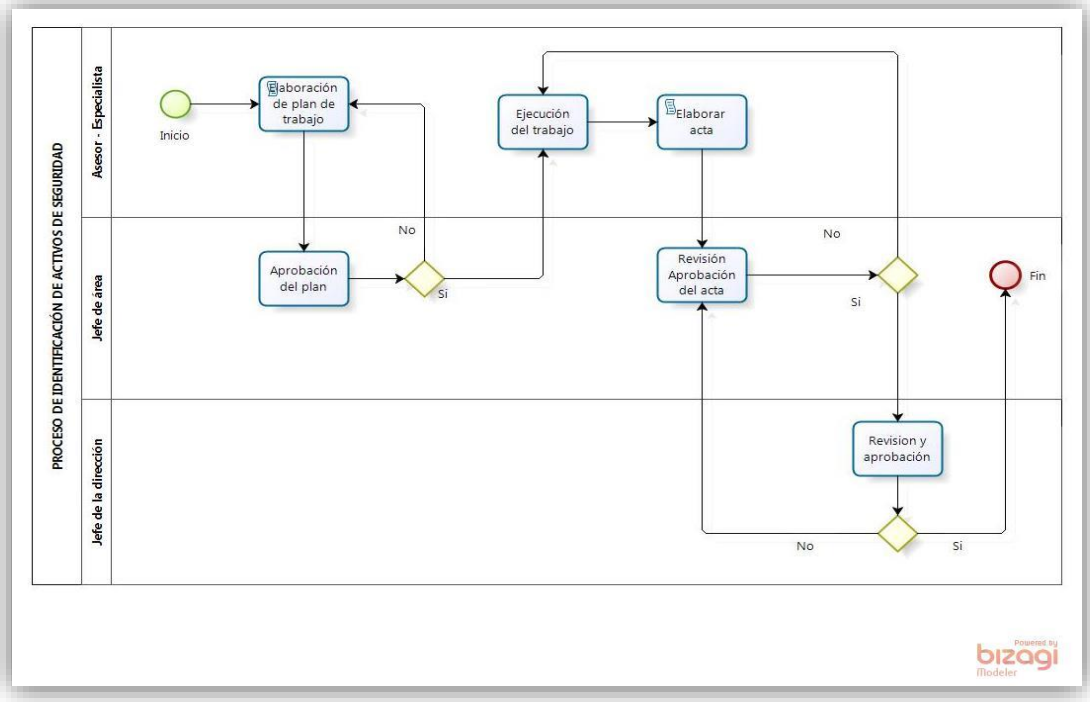


Diagrama de procesos de identificación de activos críticos del departamento de área de TI:

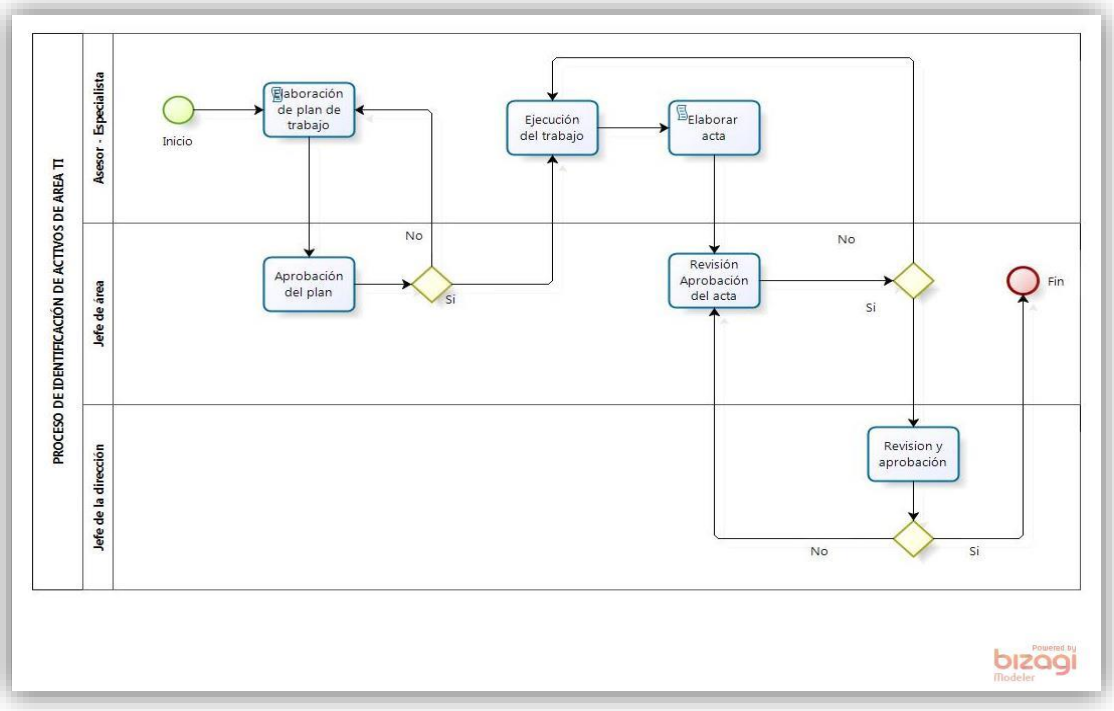


Diagrama de procesos de identificación de activos críticos del departamento de personal.

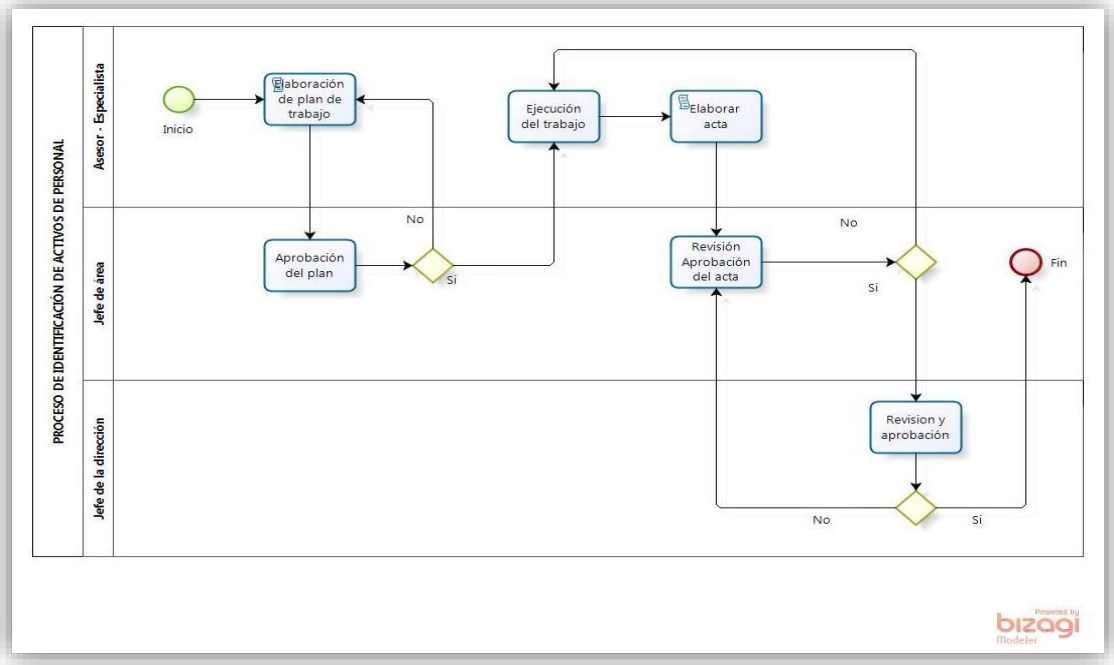
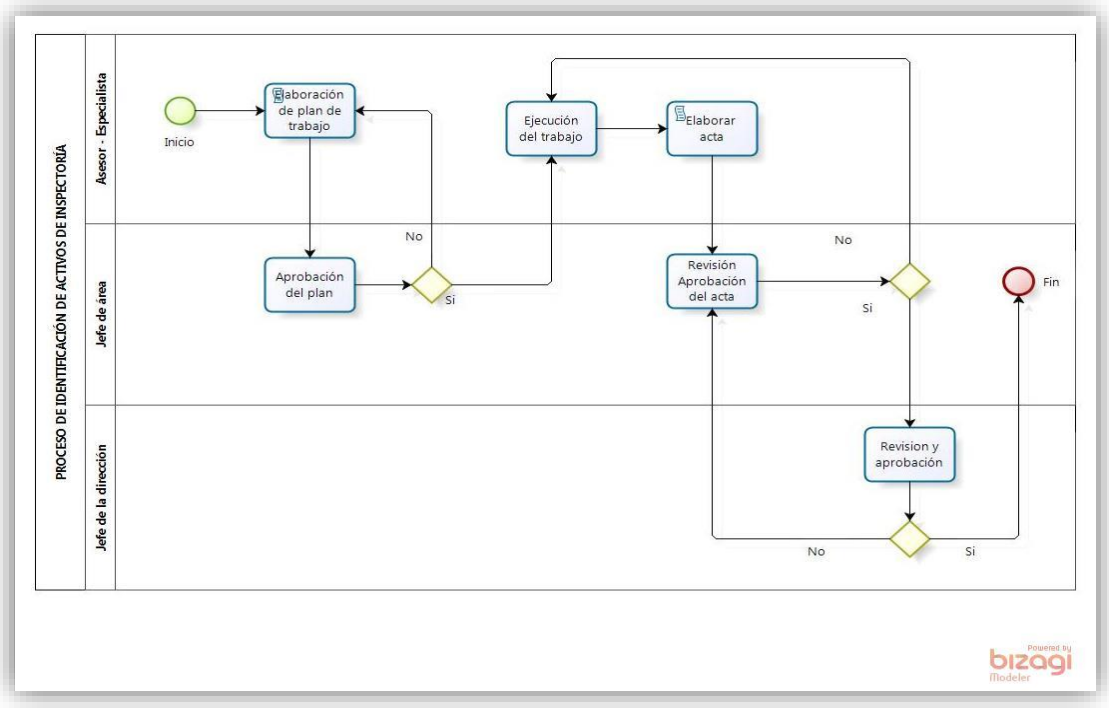
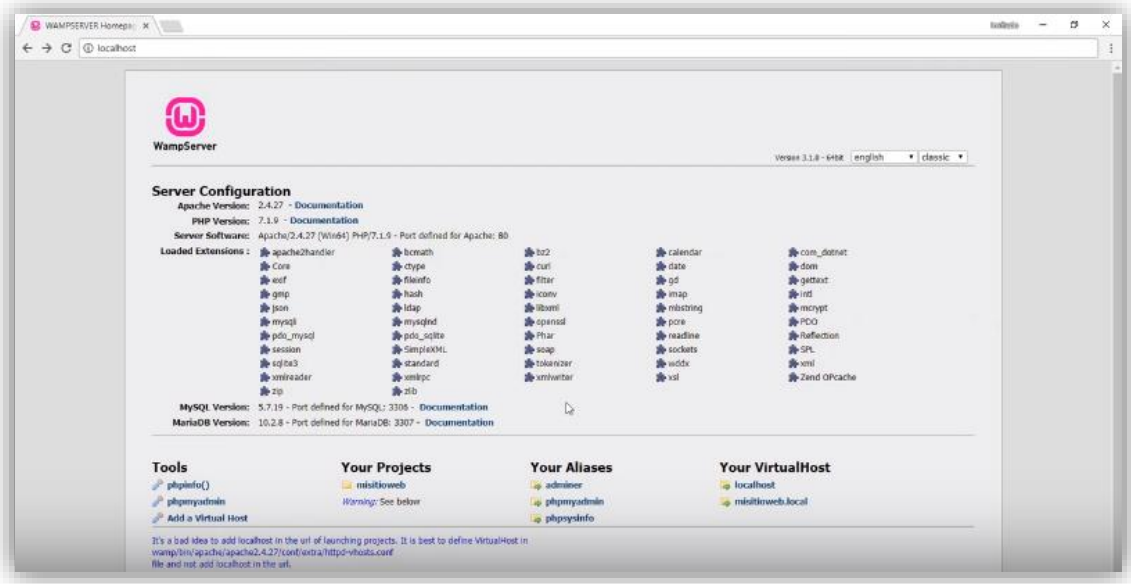
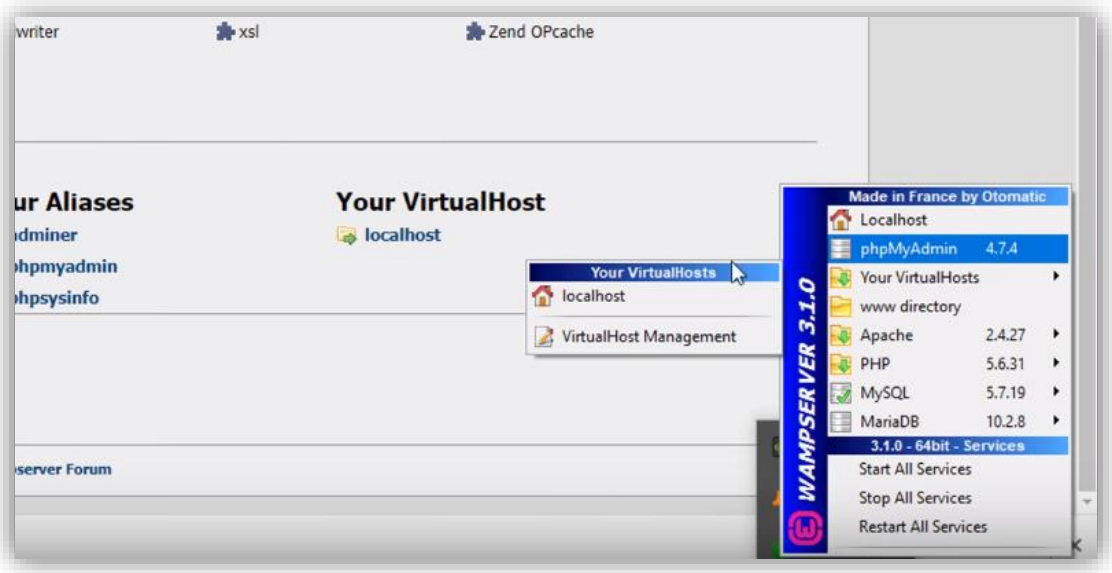


Diagrama de procesos de identificación de activos críticos del departamento de inspectoría:

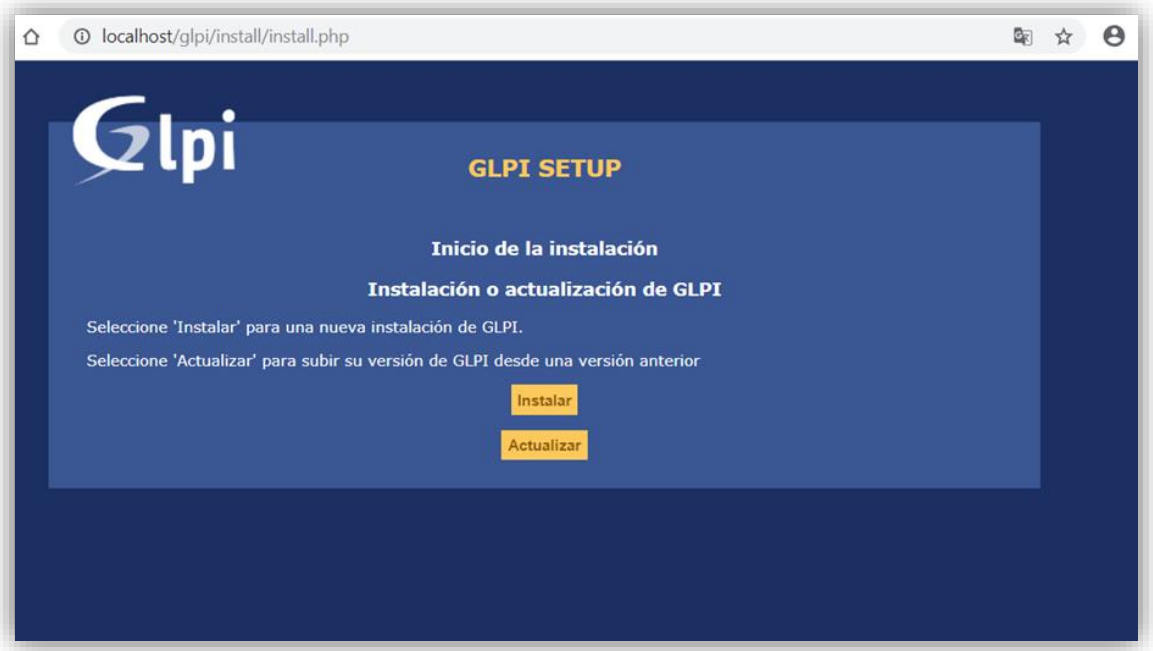


Instalación de Wampserver32 3.1.0 la que permitirá levantar un servidor local para fines de demostración del trabajo de investigación en la dirección:

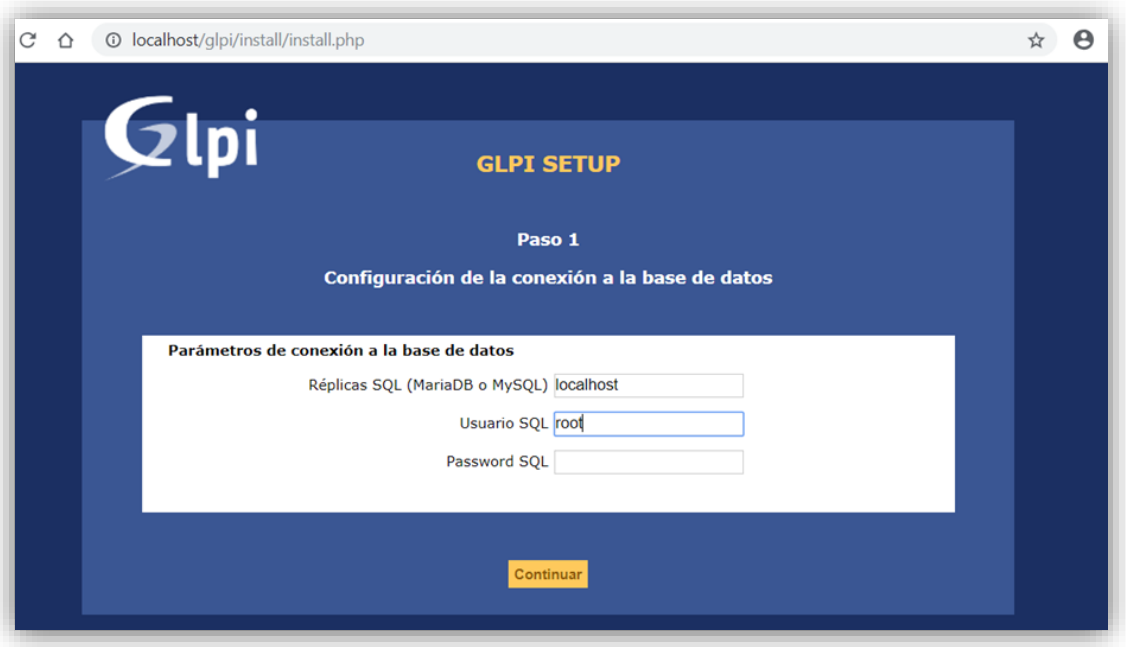




Instalación de Gestión Libre de Parque informático (GLPI) software libre que permite la administración de activos críticos, asignar usuarios, reportar incidentes, solicitar servicios y principalmente el análisis de los incidentes a través de los dashboard para su mejor comprensión y toma de decisión del comando de la dirección.



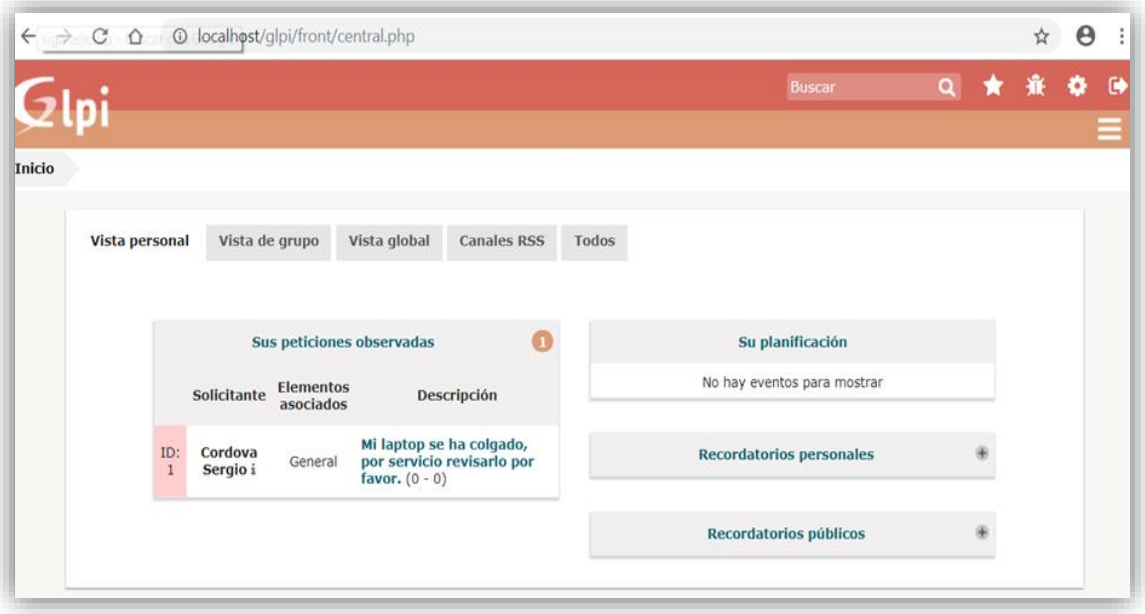
Configuración de GLPI para uso de base de datos de wampserver.



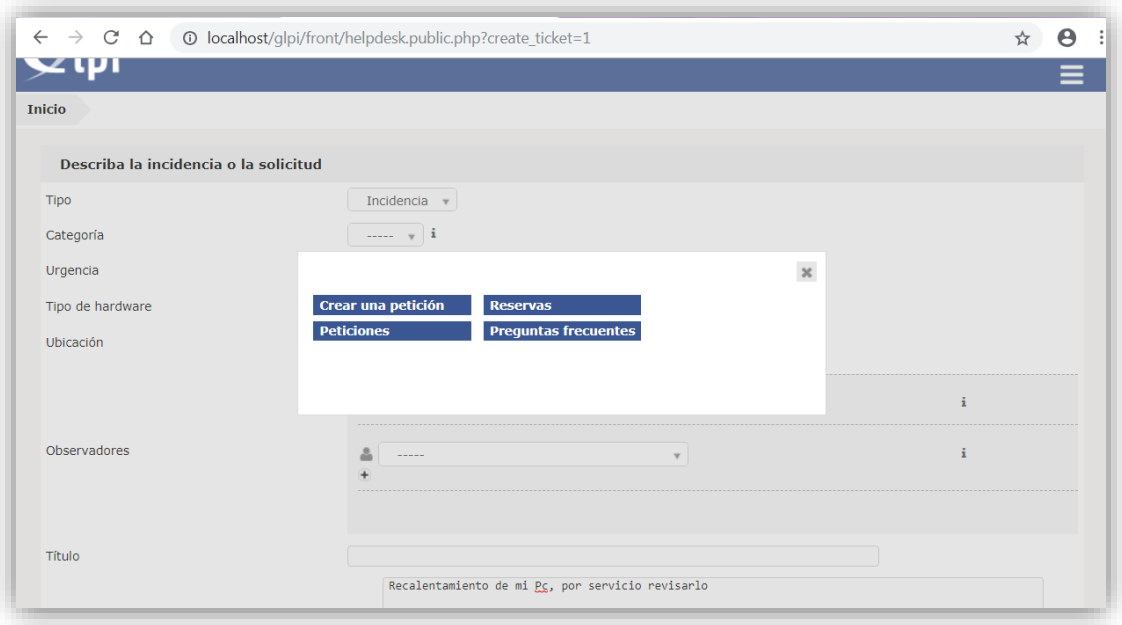
Creación de base de datos de los activos de la dirección.

Configurando los usuarios en Gestión Libre de Parque Informático – GLPI.

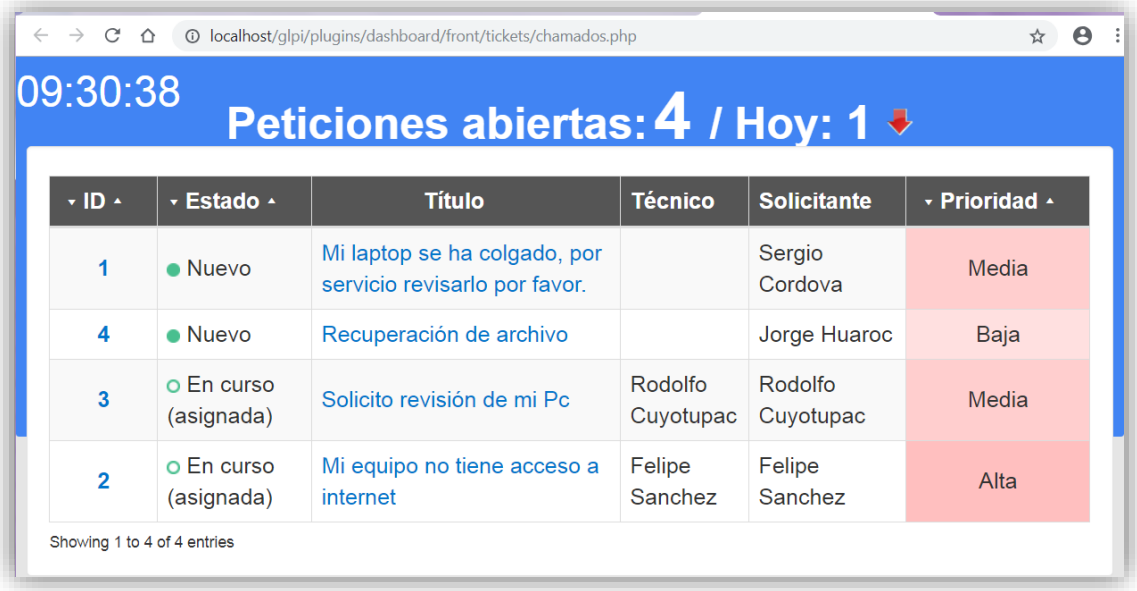
Atención a los usuarios que han presentado incidentes, solicitudes, peticiones con relación a seguridad de información o activos de información que involucra el proceso normal de la gestión de la información de la dirección.



Usuario reportando incidente de su activo



En el siguiente gráfico se muestra las peticiones, su estado, el asunto o título, el solicitante y la prioridad de solución que requiere el asunto o incidentes



En el siguiente gráfico se puede observar las estadísticas de los incidentes que nos muestra por día, mes, el total de peticiones, el tiempo de retraso que lleva cada petición, el número de usuarios, tablero de informes, gráficos, métricas, activos y otras características que permiten el análisis integral de los incidentes aportando a la gestión de riesgos que a su vez permiten identificar las amenazas y vulnerabilidades que podrían involucrar la seguridad de información de la dirección.