# UNIVERSIDAD NACIONAL DEL CALLAO

FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS


**"PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS, 2023"**

TESIS PARA OPTAR EL TITULO PROFESIONAL DE

INGENIERO DE SISTEMAS

**AUTORES:**

LISADELA CAROL ESTALLA CASTRO
MÁXIMO JHONN MORALES MEDINA

ASESORA: DRA. SALLY KARINA TORRES ALVARADO

LINEA DE INVESTIGACION: INGENIERÍA Y TECNOLOGÍA

**Callao, 2024**

**PERÚ**

Ouriginal by Turnitin

## Document Information

| | |
|---|---|
| **Analyzed document** | TESIS - ESTALLA Y MORALES.docx (D181523361) |
| **Submitted** | 2023-12-11 19:16:00 UTC+01:00 |
| **Submitted by** | Unidad FIIS |
| **Submitter email** | fiis.investigacion@unac.edu.pe |
| **Similarity** | 21% |
| **Analysis address** | fiis.investigacion.unac@analysis.urkund.com |

## Sources included in the report

SA **TESIS ROGER PARRAGA -ROBERT CEDEÑO.docx**
Document TESIS ROGER PARRAGA -ROBERT CEDEÑO.docx (D141488546)

W URL: https://repositorio.continental.edu.pe/bitstream/20.500.12394/7202/3/IV_FIN_108_TI_Pachao_Pizarro_2019.pdf
Fetched: 2/21/2023 6:40:17 AM

SA **TESIS_GABRIELA FERNÁNDEZ_Versión Final_MGS.pdf**
Document TESIS_GABRIELA FERNÁNDEZ_Versión Final_MGS.pdf (D112176848)

W URL: https://www.globalsuitesolutions.com/what-is-the-iso-27001-standard-and-what-is-its-purpose/
Fetched: 10/23/2023 11:52:32 AM

SA **M1.823_20211_PEC2_15539534.txt**
Document M1.823_20211_PEC2_15539534.txt (D115319438)

SA **T005_45627256_M.docx**
Document T005_45627256_M.docx (D142440826)

W URL: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5865/BC-4223%20ROJAS%20VIERA-ZAVALETA%20VERONA.pdf?sequence=1&isAllowed=y
Fetched: 11/6/2021 5:59:04 AM

SA **M1.880_20212_PEC4_17360595.txt**
Document M1.880_20212_PEC4_17360595.txt (D134936721)

W URL: https://digitk.areandina.edu.co/bitstream/handle/areandina/2767/Seguridad%20de%20la%20informaci%C3%B3n%20en%20una%20empresa%20de%20seguridad%20privada%20de
sequence=1&isAllowed=y
Fetched: 5/30/2020 11:04:54 AM

SA **1521516145_615__PROYECTO%252BFINAL%252BNORMAS%252BISO%252B27001.pdf**
Document 1521516145_615__PROYECTO%252BFINAL%252BNORMAS%252BISO%252B27001.pdf (D36730975)

SA **Respuestas Caso Práctico 1.docx**
Document Respuestas Caso Práctico 1.docx (D131355479)

SA **TESIS FINAL.docx**
Document TESIS FINAL.docx (D126461636)

SA **b300c3e88208d254478df8e20d10f885da8642b9.html**
Document b300c3e88208d254478df8e20d10f885da8642b9.html (D129007976)

W URL: https://1library.co/article/control-acceso-sistema-gesti%C3%B3n-seguridad-informaci%C3%B3n-basado-norma.q05wwxxy
Fetched: 7/8/2022 4:10:18 AM

SA **Resolucion caso practico 1.pdf**
Document Resolucion caso practico 1.pdf (D136256221)

W URL: https://www.minsalud.gov.co/Ministerio/Institucional/Procesos%20y%20procedimientos/ASIS02.pdf
Fetched: 3/12/2023 3:55:22 PM

W URL: https://www.catastrobogota.gov.co/sites/default/files/archivos/2019IE21771_Inf_Auditoria%20SGSI%202019%20editable.pdf
Fetched: 3/9/2023 2:40:46 AM

W URL: https://vsip.info/anexo-a-iso-27001-pdf-free.html
Fetched: 7/22/2022 7:01:01 AM

SA **M1.880_20222_PEC4_19896696.txt**
Document M1.880_20222_PEC4_19896696.txt (D166780776)

SA **Caso Práctico ISO IEC 27001 - Fabian Santibañez.pdf**
Document Caso Práctico ISO IEC 27001 - Fabian Santibañez.pdf (D160577344)

## Entire Document

# INFORMACIÓN BÁSICA

**UNIDAD DE INVESTIGACIÓN**: **FACULTAD DE INGENIERÍA INDUSTRIAL Y DE SISTEMAS**

**TÍTULO: "PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS, 2023"**

**AUTORES:** LISADELA CAROL ESTALLA CASTRO/0009-0008-1227-1381/47174059

MAXIMO JHONN MORALES MEDINA/0009-0009-5310-5133/43335670

**ASESORA**: DRA. SALLY KARINA TORRES ALVARADO/0000-0001-6657-2931/15724611

**LUGAR DE EJECUCIÓN**: AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS – LIMA

**TIPO DE INVESTIGACIÓN:** BÁSICA PRE-EXPERIMENTAL APLICADA.

**TEMA OCDE**: INGENIERÍA Y TECNOLOGÍA

# ACTA DE SUSTENTACIÓN

## ACTA DE SUSTENTACION POR MODALIDAD DE CICLO TALLER DE TESIS PARA LA OBTENCIÓN DEL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

## ACTA N° 001-2024-I-CTT-IS

Siendo las 08:55 horas del día 06 de Enero del año 2024, encontrándose reunidos en el Auditorio de la FIIS, el **Dr. ENRIQUE GARCÍA TALLEDO,** en representación de la Rectora de la UNAC; el **JURADO DE SUSTENTACIÓN DE TESIS** (designado por resolución **002-2024-CF-FIIS**)de la Facultad Ingeniería Industrial y de Sistemas de la Universidad Nacional del Callao, para la evaluación de las Tesis que conllevan a la obtención del Título Profesional de **INGENIERO DE SISTEMAS**, el que se encuentra conformado por los siguientes docentes ordinarios:

| | |
|---|---|
| **PRESIDENTE** | **MG. MANUEL ABELARDO ALCÁNTARA RAMÍREZ** |
| **SECRETARIO** | **MG. ANGELINO ABAD RAMOS CHOQUEHUANCA** |
| **VOCAL** | **MG. JOSÉ JESÚS BRINGAS ZÚÑIGA** |
| **SUPLENTE** | **MG. YESMI KATIA ORTEGA ROJAS** |

Con el quórum reglamentario de ley y de conformidad con lo establecido por el Reglamento de Grados y Títulos vigente se dio inicio al Acto de Sustentación de la Tesis de las Bachilleres: **MORALES MEDINA MÁXIMO JHONN, ESTALLA CASTRO LISADELA CAROL**, quienes, habiendo cumplido con los requisitos para optar el Título Profesional de **INGENIERO DE SISTEMAS**, sustentan la tesis titulada **"PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS, 2023"**, cumpliendo con la sustentación en acto público, de manera presencial.

Luego de la exposición, y de la absolución de las preguntas formuladas por el Jurado de Sustentación y efectuadas las deliberaciones pertinentes, **SE ACORDÓ**: Dar por **APROBADO** con la escala de calificación cuantitativa **( 16 )** y calificación cualitativa **(Muy Bueno)** a la presente tesis, conforme a lo dispuesto en el Art. 24 del Reglamento de Grados y Títulos de la UNAC, aprobado por Resolución de Consejo Universitario N° 150-2023-CU del 15 de junio del 2023.

Se dio por concluida la Sesión a las 09.30 horas del día 06 de enero del 2024.

MG. MANUEL ABELARDO ALCÁNTARA RAMÍREZ
Presidente

MG. ANGELINO ABAD RAMOS CHOQUEHUANCA
Secretario

MG. JESÚS JOSÉ BRINGAS ZÚÑIGA
Vocal

MG. YESMI KATIA ORTEGA ROJAS
Suplente

# INFORME N° 001-2024 – JS ICTTS

**PARA** : **DR. PAUL GREGORIO PAUCAR LLANOS**
**DECANO FIIS**

**DE** : **JURADO DE SUSTENTACIÓN DEL I CICLO TALLER DE TESIS DE INGENIERÍA DE SISTEMAS**

**ASUNTO** : **INFORME FAVORABLE DEL JURADO DE SUSTENTACION**

**FECHA** : **Callao, 06 de enero del 2024**

Los miembros del Jurado de Sustentación designados por **Resolución N° 002-2024-CF-FIIS** y de acuerdo al Reglamento de Grados y Títulos, aprobado por Resolución 150-2023-CU del 15 de junio de 2023 Art. 71, visto el Acta de Sustentación **N° 001-2024 – JS ICTTS** de Tesis Titulada: **"PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS, 2023"**

**Presentado por:**
**MORALES MEDINA MÁXIMO JHONN**
**ESTALLA CASTRO LISADELA CAROL**

Para obtener Título de Profesional de **INGENIERO DE SISTEMAS**, por modalidad de Tesis con Ciclo Taller de Tesis, habiendo obtenido nota aprobatoria de (16) dieciséis, Muy Bueno.

En tal sentido, los miembros del Jurado de Sustentación informan que no existe observación alguna a dicha Tesis por lo que se da la **CONFORMIDAD**, lo cual se debe comunicar a los interesados.

Sin otro particular reiteramos los sentimientos y estima personal.

.....
MG. MANUEL ABELARDO ALCÁNTARA RAMÍREZ
Presidente

.....
MG. ANGELINO ABAD RAMOS CHOQUEHUANCA
Secretario

.....
MG. JESÚS JOSÉ BRINGAS ZÚÑIGA
Vocal

.....
MG. YESMI KATIA ORTEGA ROJAS
Suplente

## DEDICATORIA

A nuestros estimados profesores asesores, cuya experiencia y orientaci experta han sido fundamentales en ca etapa de esta investigación, también dedicado a nuestros seres queridos y todos aquellos que han desempeñado papel esencial en este desafiante enriquecedor viaje hacia la culminación nuestro proyecto de tesis.

Este logro es el resultado de esfuerzo, dedicación y compromiso, y lo compartimos con gratitud con todos aquellos que han sido parte de nuestro viaje.

## AGRADECIMIENTO

A nuestras familias, por su apoyo inquebrantable, paciencia y comprensión durante esta travesía académica. Su amor y aliento nos han impulsado en cada paso.

A nuestros respetados profesores y asesores, cuyo conocimiento experto y orientación fueron cruciales para dar forma a este proyecto y llevarlo a cabo de manera efectiva.

A la Agencia de Compras de las Fuerzas Armadas del Perú, por brindarnos la oportunidad de llevar a cabo esta propuesta. Su apertura y cooperación fueron fundamentales.

¡Gracias por su apoyo y contribución a nuestro éxito!

# ÍNDICE

# ÍNDICE DE TABLAS

# ÍNDICE DE FIGURAS

# RESUMEN

El presente proyecto de tesis tiene como objetivo principal proponer un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 para la Agencia de Compras de las Fuerzas Armadas (ACFFAA). Este proyecto se enmarca en una investigación pre-experimental, donde se implementarán procesos específicos siguiendo la normativa ISO 27001.

La norma ISO 27001 se presenta como una guía integral que facilita el establecimiento, implementación, mantenimiento y mejora continua de un SGSI. En este contexto, se utilizará el ciclo de Deming (Plan-Do-Check-Act) como un enfoque metodológico para la mejora continua de los procesos de seguridad de la información (Ver ilustración 1).

Comienza con un análisis exhaustivo de las normas ISO/IEC 27001, identificando los requisitos esenciales para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en la Agencia de Compras de las Fuerzas Armadas. Con base en este análisis, se desarrolla el diseño del modelo de SGSI junto con un procedimiento detallado para su implementación.

El objetivo a largo plazo es facilitar la implementación del SGSI en la Agencia de Compras de las Fuerzas Armadas, brindándole la capacidad de salvaguardar su información de manera efectiva y destacarse en el ámbito de la seguridad.

**Palabras clave:** Seguridad de la Información, Norma ISO/IEC 27001, Sistema de Gestión de Seguridad de la Información (SGSI), Implementación de SGSI, Gestión de Riesgos de la Información, Protección de Activos de Información
Auditoría de Seguridad Informática, ISO 27001, Mejora Continua en Seguridad de la Información.

# ABSTRACT

The main objective of this thesis project is to propose an Information Security Management System (ISMS) based on the ISO 27001 standard for the Armed Forces Procurement Agency (ACFFAA). This project is part of a descriptive research, where specific processes will be implemented following the ISO 27001 standard.

The ISO 27001 standard is presented as a comprehensive guide that facilitates the establishment, implementation, maintenance, and continuous improvement of an ISMS. In this context, the Deming cycle (Plan-Do-Check-Act) will be used as a methodological approach for the continuous improvement of information security processes.

It begins with an exhaustive analysis of the ISO/IEC 27001 standards, identifying the essential requirements for the implementation of the Information Security Management System (ISMS) in the Armed Forces Acquisition Agency. Based on this analysis, the design of the ISMS model is developed along with a detailed procedure for its implementation.

The long-term objective is to facilitate the implementation of the ISMS in the Armed Forces Procurement Agency, giving it the ability to store its information effectively and excel in the field of security.

**Keywords:** Information Security, ISO/IEC 27001 Standard, Information Security Management System (ISMS), ISMS Implementation, Information Risk Management, Information Asset Protection Computer Security Audit, ISO 27001, Continuous Improvement in Information Security.

# INTRODUCCIÓN

En la actualidad, con el progreso de la tecnología de la información, esta se ha convertido en uno de los recursos más esenciales dentro de cualquier entidad. Este papel destacado la expone a diversos riesgos, incluyendo amenazas y vulnerabilidades. Dada la inestimable importancia de la información en el contexto organizacional, resulta crucial implementar medidas de protección efectivas contra posibles amenazas y vulnerabilidades. La aplicación de técnicas diseñadas para salvaguardar los activos de información contribuirá de manera significativa al fortalecimiento de la seguridad de la información en una organización como la Agencia de Compras de las Fuerzas Armadas (ACFFAA).

En el contexto específico de la Agencia de Compras de las Fuerzas Armadas, la adopción de la norma ISO/IEC 27001 en sus herramientas tecnológicas se presenta como una estrategia clave. Esta norma posibilitará el establecimiento y desarrollo de un Sistema de Gestión de la Seguridad de la Información, proporcionando así un marco sólido para salvaguardar la integridad, confidencialidad y disponibilidad de la información manejada por la entidad.

Se maneja un tipo de investigación básica – pre-experimental – aplicada. La gestión de la seguridad de la información abarca a toda la empresa, no solo al departamento de tecnología. Es crucial sensibilizar a todo el personal acerca de las amenazas y las posibles repercusiones.

Se subraya la importancia de seguir un modelo de seguridad que conlleva un manejo adecuado de la información y la protección de los activos vitales mediante normativas o políticas que regulen las operaciones diarias. Estas directrices deben ser compartidas con todos los empleados mediante capacitaciones, fomentando su compromiso con el uso responsable de la información y los recursos, al mismo tiempo

que se promueven principios fundamentales como la integridad, autenticidad y confidencialidad de la información.

Este proyecto tiene como objetivo presentar a la sede principal de la Agencia de Compras de las Fuerzas Armadas del Perú una propuesta para implementar un Sistema de Gestión de Seguridad de la Información. Este sistema se enfoca en establecer pautas que garanticen la seguridad de la información y demás activos informáticos, utilizando la norma ISO 27001 como marco de referencia, aprovechando sus mejores prácticas para alcanzar los objetivos del proyecto.


Ilustración 1 Ciclo de Deming: Metodología de mejora continua | PDCA -PHVA. - Elaboración Propia

# I. PLANTEAMIENTO DEL PROBLEMA

## 1.1 Descripción de la realidad problemática

La globalización como proceso económico, tecnológico, político, social y cultural, producido principalmente por la sociedad, ha abierto sus puertas a la revolución informática; una revolución que ha cambiado todos los aspectos de la vida diaria al punto que hoy es difícil para las sociedades imaginar la vida cotidiana sin tecnología.

Así como existen muchos beneficios generados por el progreso y la expansión tecnológica; los países y sus organizaciones enfrentan diariamente el problema de amenazas y vulnerabilidades de los activos de información.

En ese sentido, la Agencia de Compras de las fuerzas Armadas (ACFFAA), con el fin de preservar la confidencialidad, integridad y disponibilidad de sus activos de seguridad de la información, requiere implementar, mantener y mejorar continuamente su Sistema de Gestión de Seguridad de la Información, basado en la ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos. (Standardization, 2014).

## 1.2 Formulación del problema.

En la actualidad la Agencia de Compras de las Fuerzas Armadas, aunque cuente con recursos tecnológicos, no cuenta con la implementación del Sistema de Gestión de Seguridad de la Información, que es fundamental para prevenir, mitigar, neutralizar o eliminar los riesgos provenientes de ataques informáticos, espías informáticos y/o personas.

### 1.2.1 Problema general

¿Se puede desarrollar un Sistema de Gestión de Seguridad de la Información para la Agencia de Compras de las Fuerzas Armadas, 2023?

### 1.2.2 Problemas específicos

- ¿Se puede identificar el estado situacional de los procesos existentes en la Agencia de Compras de las Fuerzas Armadas en el Área de TI (Tecnologías de Información)?
- ¿En los procesos existentes se puede planificar un análisis de brecha para identificar la confidencialidad del Sistema de Gestión de Seguridad de la Información en la ACFFAA?
- ¿Se puede identificar qué controles de acuerdo con la ISO 27001 se pueda implementar en el Sistema de Gestión de Seguridad de la Información para resguardar la confidencialidad, la disponibilidad e integridad en los procesos de la Agencia de Compras de las Fuerzas Armadas?

## 1.3 Objetivos

### 1.3.1 Objetivo General

Desarrollar un Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 para la Agencia de Compras de las Fuerzas Armadas, 2023.

### 1.3.2 Objetivos Específicos

1. Identificar el estado situacional actual de los procesos existentes en la Agencia de Compras de las Fuerzas Armadas en el Área de TI (Tecnologías de Información)
   - Planificar un análisis de brecha para identificar la confidencialidad del Sistema de Gestión de Seguridad de la Información en la ACFFAA.
   - Identificar qué controles de acuerdo con la ISO 27001 se puede implementar en el Sistema de Gestión de Seguridad de la

Información para resguardar la confidencialidad, la disponibilidad e integridad en los procesos de la Agencia de Compras de las Fuerzas Armadas.

## 1.4 Justificación

Justificación Teórica Guzmán (2016) argumenta en su investigación que el diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013 proporciona las condiciones necesarias para garantizar la gobernabilidad, oportunidad y viabilidad de la seguridad de la información. Esto respalda la gestión financiera, administrativa y operativa de una entidad, contribuyendo al cumplimiento de su misión.

Justificación Social Villegas y Gaviria (2013) destacan la importancia de definir un Sistema de Gestión de Seguridad de la Información (SGSI) en función de los objetivos de seguridad de la información y la metodología adecuada para el análisis de riesgos. Esto se relaciona con la seguridad de la información en el contexto empresarial y organizacional.

Justificación Metodológica Aguirre y Aristizábal (2013) enfatizan que un SGSI es esencial para competir en un entorno global exigente, donde las certificaciones de seguridad de la información brindan ventajas competitivas. Además, destaca la necesidad de realizar transacciones electrónicas de manera segura y eficiente.

Justificación Institucional Hoy en día, muchas empresas carecen de un proceso de seguridad eficiente en comparación con los estándares establecidos por la norma técnica peruana (NTP) ISO 27001. Esto hace que sea crucial para las instituciones adoptar adecuadamente estos estándares para mitigar los riesgos de seguridad de la información.

## 1.4 Delimitantes de la investigación

**1.5.1 Limitaciones de Tiempo**: La implementación de un SGSI de acuerdo con la norma ISO 27001 es un proceso que lleva tiempo y requiere una planificación cuidadosa. Las limitaciones de tiempo debido a proyectos

existentes y otras prioridades pueden ralentizar el proceso de implementación.

**1.5.2 Limitante espacial**: El personal no tiene conocimiento de que trata el Sistema de Gestión de la Seguridad de la Información, el cual requiere sea capacitado mediante charlas y concientizaciones en las diferentes áreas al respecto.

# II. MARCO TEÓRICO

## 2.1. Antecedentes

### 2.1.1 Antecedentes Internacionales:

Según la investigación, (LOPEZ, 2016). El levantamiento de los riesgos fue en base a considerar los principios fundamentales que comprometen a la seguridad de la información, que son: disponibilidad, confidencialidad y la integridad. El objetivo de este trabajo de tesis es elaborar una propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información para Institutos de Educación Superior Tecnológica Aeronáutica en el Ecuador. Primero, fue necesario conocer el estado actual de los Riesgos y de la Gestión de Seguridad de la Información en estos Institutos, en base a encuestas y entrevistas, cuyos resultados fueron analizados y procesados con una metodología cualitativa; se agruparon los datos según su naturaleza y se los evaluó posteriormente. Las muestras se realizaron en base a las encuestas que permitió identificar los riesgos, considerando su orden de importancia , así como las debilidades detectadas en la gestión de la seguridad de la información; por lo que con este análisis y fundamentados en el propósito de demostrar que es factible realizar una gestión competente, efectiva y continua de la seguridad en el marco de los riesgos detectados y de que se pueden adoptar las medidas adecuadas en proporción a la magnitud y tipo de organización, se identificaron los requerimientos de Seguridad de la Información. Posteriormente se analiza y estudia la serie de la norma ISO 27000, determinando usar combinadamente el Estándar ISO:27002 (mejores prácticas) que no es certificable, con el Estándar ISO:27001 certificable, para realizar la construcción del Modelo de Sistema de Gestión de Seguridad de la Información SGSI en estos Centros de Enseñanza Aeronáutica, ya que se adaptan a la naturaleza cambiante en estructura y procesos de ellos. El problema se basa en la necesidad

de profesionalizar los centros de instrucción en materia de aeronáutica civil del Ecuador ha incrementado la utilización de tecnologías de información sin contar con una normatividad o reglamentación orientada a proteger sus activos. Entonces al partir de la hipótesis de trabajo: “Es posible gestionar adecuadamente la seguridad de la información en los institutos de educación superior aeronáutica, mediante un Sistema de Gestión de Seguridad de la Información”. Como resultado el desarrollo de este proyecto se efectuaron los análisis para demostrar lo indicado.

(Hidalgo Narváez, 2022) Esta tesis tiene como objetivo determinar cómo influye el diseño e implementación de un modelo de Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar internacional ISO/IEC 27001:2013 en la eficacia de la administración de los recursos públicos. Para ello se ha tomado como referencia el modelo del SGSI implementado por el Registro de la Propiedad y Mercantil del Cantón Pedro Moncayo (RPMPM); que, por su operatividad en el manejo de datos públicos, logró obtener una marca internacional en Seguridad de la Información (SI) y se convirtió en un referente de buenas prácticas a nivel nacional. La metodología cualitativa describe el SGSI adoptado por el RPMPM, bajo los estándares de la Norma ISO/IEC 27001: 2013 y la integración con la Norma de Control Interno (NCI) expedido por la Contraloría General del Estado (CGE), que al ser aplicados son eficaces al estar completamente segura la información. Del mismo modo, a través de la matriz de riesgos y actas del Comité de SI, se analiza cuantitativamente la evolución del SGSI antes, durante y posterior para asegurar su correcta implementación. Para la comprobación de los beneficios de dichas aplicaciones, se formuló una encuesta a través de Google a 200 personas relacionadas directamente con el SGSI, para determinar el nivel de conocimientos respecto al estándar, y, proponiendo un prototipo de índice para evaluar la eficacia de los recursos públicos

asignados a la SI, administrados por las Registradurías en el Ecuador, determinando que existe un 93% (2020) y 100% (2021) de eficacia al tener la capacidad para lograr los objetivos estratégicos de SI y a contribuir al buen control gubernamental. Los datos que se analizan comprenden los períodos 2019, 2020 y 2021.

En esta investigación (Carvajal, y otros, 2021), tuvo como objetivo determinar la influencia del SGSI en la empresa Soltesi S.A.C. con el uso de la ISO 27001. La investigación fue de tipo aplicada, el diseño de investigación fue descriptiva. Como resultado se obtuvo que las incidencias que se efectuaban en la empresa y no se solucionaban al 99% implementando el SGSI con la norma ISO 27001 mejorara significativamente en resolver las incidencias al menor tiempo posible, teniendo como pruebas los resultados por cada indicador aplicando el pre test y post tes. El resultado del indicador de integridad, con el pre-test se obtuvo con un valor media de 32% de incidencias resueltas al mes y que al realizar el post-test se obtuvo un valor media de 75% de incidencias resultas en un mes, siguiendo con el resultado de la confidencialidad, con el pre-test se obtuvo con un valor media de 15% de incidencias resultas al mes y que al realizar el post-test se obtuvo un valor media de 80% de incidencias resultas en un mes, como fin el resultado de disponibilidad, con el pre-test se obtuvo con un valor media de 17% de incidencias resultas al mes y que al realizar el post-test se obtuvo un valor media de 81% de incidencias resultas en un mes.

Según la investigación, (LOPEZ, 2016). Hoy con la globalización, se genera gran cantidad de datos que deben almacenarse de manera segura. Las organizaciones en Costa Rica no escapan a esa situación. El objetivo es que estos informes que contengan datos básicos hasta confidenciales y primordiales para las empresas puedan ser gestionados con la seguridad de la información ya que existen normas

como la ISO 27000 que da pautas para mantener la referencia de manera que incluya los tres pilares básicos del saber: confidencialidad, integridad y disponibilidad. Con una metodología cuantitativa de tipo de investigación experimental. La muestra de los incidentes provocados por virus y programa maligno son de un 72,73 % y 54,55 %, respectivamente, estos son generados por la falta de cultura en la seguridad de la información, de igual forma, no hay que desinteresarse por los demás incidentes que puede afectar a una organización, de ahí la importancia que se implementen los controles de la gestión de percances, dentro de un plan se seguridad de la información. Se usó como instrumentos encuestas. El resultado fue la creación e implementación de un sistema de gestión de seguridad de la información, formado por más dominios con procesos bien definidos y claramente establecidos.

Según la investigación, (Alvarez Zurita, y otros), sustentó la tesis con el título “Implementación de un Sistema de Gestión de Seguridad de la Información basado en La Norma Iso 27001, para la Intranet de la Corporación Metropolitana De Salud”. En la Escuela Politécnica Nacional, Ecuador. Tuvo como objetivo aumentar el valor de un servicio "seguro “a través de un SGSI para potenciar un servicio que ya incorpora funciones de seguridad. Con una metodología cuantitativa Se aplicó una encuesta a 18 personas determinándose que la incorporación de la norma es compleja debido a los estándares, lo cual propone el desarrollo de una guía detallada para prevenir riesgos, se usó como herramientas como: MAGERIT que persigue una aproximación metódica que no deje lugar a la improvisación. Los resultados obtenidos En el área de Informática, e logrará realizar revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

Según el estudio (Jacome Sanchez, 2022), la empresa de transporte La Ecuatoriana valora su Sistema de Información (SI) como un activo fundamental para sus operaciones diarias. La tesis se centra en proponer la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001. Esta propuesta tiene como objetivo gestionar los riesgos del SI de manera documentada y eficiente. Se establecerán políticas y procedimientos alineados con los objetivos del estudio para salvaguardar el SI contra cualquier amenaza. El enfoque metodológico utilizado es el PHVA (Planificar, Hacer, Comprobar y Mejorar), basado en estándares de la norma ISO 27001 y adaptado a las necesidades de La Ecuatoriana. La falta de planificación y protocolos de seguridad ha llevado a problemas de seguridad en la empresa. La implementación del SGSI según la normativa ISO 27001 se considera esencial para preservar la confidencialidad, integridad y disponibilidad de la información. Esta medida no solo mejora la seguridad, sino que también fortalece la imagen corporativa y la confiabilidad de La Ecuatoriana ante clientes, proveedores y asociados de negocios.

La presente investigación (Nizo Mesa, 2023) tiene como objetivo desarrollar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los estándares de la norma ISO 27001:2022. Este sistema está destinado a reducir los riesgos y vulnerabilidades que enfrenta la empresa ARIA PSW. Actualmente, la empresa carece de procedimientos, monitoreo y controles sobre el uso de equipos, instalaciones e información. La investigación se enfoca en preservar la confidencialidad, integridad y disponibilidad de la información de la empresa, reduciendo así los riesgos asociados, como la pérdida y manipulación de información confidencial. La metodología de la investigación es cualitativa y descriptiva. En la primera fase, se identificarán los posibles riesgos y vulnerabilidades en los Sistemas de Información de la empresa. Luego, se describirán estrategias para

minimizar estos riesgos. Se utilizará la metodología GAP para comparar la situación actual de la empresa con la situación deseada. Los resultados del análisis GAP indican que la empresa ARIA PSW actualmente cuenta solo con el 1% de los controles optimizados y el 78% de los controles son inexistentes según los estándares de la norma ISO 27001:2022. En conclusión, el diseño e implementación del SGSI contribuirá significativamente a minimizar los riesgos para las partes interesadas de ARIA PSW, protegiendo la integridad, confidencialidad y disponibilidad de la información de la empresa. La necesidad de implementar un SGSI se fundamenta en la alta probabilidad de ocurrencia de pérdida, manipulación y falta de disponibilidad de información, lo que podría tener un impacto catastrófico en la empresa, tanto en términos de tiempo como de recursos financieros.

El trabajo denominado (Arango, 2016), tiene como objetivo establecer las bases para un proceso de mejora continua y proponer acciones para minimizar los riesgos potenciales. Se utilizará el modelo de madurez de la capacidad (CMM) para evaluar el grado de madurez en la implementación del SGSI, basado en la norma ISO 27002:2013, que comprende 114 controles en 14 dominios con 35 objetivos de control. Las fases del proyecto incluyen la documentación de mejores prácticas en seguridad de la información, definición clara de la situación actual y objetivos del SGSI, análisis de riesgos con identificación y valoración de activos, evaluación del cumplimiento de la ISO/IEC 27002:2013, propuestas de proyectos para una gestión adecuada de la seguridad, y diseño del esquema documental del sistema de gestión de seguridad de la información. La implementación del SGSI optimizará recursos, reducirá costos y ayudará a Textilera S.A. a alcanzar sus objetivos. Mejorar el sistema de gestión de seguridad permitirá cumplir los estándares de la organización y acercarse a la certificación ISO 27001:2013. Además, garantizará la integridad, confidencialidad y

disponibilidad de la información, siendo crucial para el crecimiento de Textilera S.A. La gestión de riesgos identificó activos críticos y desarrolló medidas de protección. Se identificaron procesos faltantes y se evaluó el cumplimiento de los controles de la norma ISO 27001:2013. La dirección y la sensibilización permanente de los usuarios son clave para el éxito del SGSI.

Según la investigación denominada (Cazco, 2016), tenía como objetivo analizar el estado actual de la Universidad del Salvador (UES) en cuanto a la gestión de la seguridad de la información. Este análisis sirvió como base para la propuesta de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) fundamentado en la norma ISO 27001:2005. Durante el estudio realizado en la UES, se evaluaron los riesgos de sufrir incidentes de seguridad, tanto voluntarios como involuntarios, que podrían originarse tanto dentro de la organización como debido a catástrofes naturales y fallas técnicas. A pesar de que la UES es reconocida como una universidad destacada a nivel nacional e internacional, carece de un departamento específico dedicado a la gestión de la seguridad de la información. Cada área de tecnología de la información (infraestructura, telecomunicaciones, desarrollo, etc.) tiene sus propios métodos y procedimientos de seguridad, pero no están centralizados ni se aplican de manera consistente. La falta de un SGSI documentado y políticas de seguridad definidas crea la necesidad urgente de implementar un SGSI para fortalecer los controles que garanticen la disponibilidad, confidencialidad e integridad de la información de la UES. Este sistema también sería crucial para administrar los riesgos de seguridad de la información y promover el uso adecuado de las tecnologías de información y comunicación en toda la universidad, incluyendo áreas administrativas y estudiantes. Para que los proyectos propuestos se implementen eficazmente, es esencial asignar personal dedicado a cada tarea y concientizar a todos los involucrados sobre su importancia.

### 2.1.2 Antecedentes Nacionales:

(Burga Segovia, 2022) En su propuesta de tesis tiene como objetivo Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) asociado al proceso de Créditos de la Edpyme CREDIVSIÓN, para el diseño se utiliza los procedimientos y lineamientos indicados en la norma internacional ISO/IEC 27001 en su versión 2013 y los controles de seguridad asociados en el Anexo A de la misma. Se detallan actividades para una correcta implementación del antes mencionado Sistema para la referida empresa. Se destaca la priorización de la sensibilización de su recurso humano el en la importancia de salvaguardar la información que manejan en sus diferentes actividades laborales. El diseño del referido Sistemas identifica 226 activos de información, y 106 activos críticos que interactúan en el proceso de créditos; también, se identifican por cada activo sus amenazas y vulnerabilidades y los agentes que lo provocan. En base la matriz de riesgos se identifican 23 riesgos críticos para lo que se propone plan de tratamiento de riesgos tomando como base la declaración de aplicabilidad (SOA) del anexo A, para tal caso se identifican 93 controles que aplican y reducen la probabilidad y el impacto del riesgo alineados a los objetivos de negocio, para la mejora de la disponibilidad, confidencialidad e integridad del proceso de créditos. Para contrastar la hipótesis se utiliza la prueba T Wilcoxon cuyos resultados son: 4.5355, valor mayor que la toma decisión:1.645, concluyendo así que el diseño de un sistema de gestión de la seguridad de la información basado en la Norma ISO 27001:2013 aplicado a Edpyme CREDIVSIÓN permite mejorar la confidencialidad, integridad y disponibilidad en el proceso de créditos.

Este estudio (Chuna Chinga, 2018), se enfocó en proponer un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los controles especificados por la Norma Técnica Peruana en uso para la

Dirección Regional de Trabajo y Promoción de Empleo – Filial Piura. Para ello, se realizó un análisis de los activos físicos, lógicos y de información de la entidad a través de encuestas y registros, identificando 30 vulnerabilidades y 20 riesgos. Estos riesgos fueron evaluados mediante la metodología Magerit, revelando que el 50% son de alto riesgo, el 40% son riesgos altos, el 5% son de nivel medio y el 5% son de bajo riesgo. Posteriormente, se seleccionaron 75 controles apropiados para abordar estos riesgos, siguiendo la NTP ISO/IEC 27001:2014, a través de una declaración de aplicabilidad. Se establecieron políticas y controles de seguridad conforme a estos controles seleccionados. El SGSI tiene como objetivo permitir a la entidad utilizar sus activos de manera aceptable, implementar mecanismos para manejar eventos no deseados a través de un plan de tratamiento de riesgos, asignar roles y responsabilidades para una respuesta rápida a incidentes de seguridad, y establecer procedimientos y reglas de seguridad para proteger sus activos. La documentación del SGSI se adaptó al formato establecido por el ONGEI (Oficina Nacional de Gobierno Electrónico e Informática).

(Brocca Castillo, 2019) En su presente tesis tuvo como objetivo general: Determinar cómo influye la implementación del Sistema de Gestión de Seguridad de la Información basado en los requisitos de la Norma Técnica Peruana ISO/IEC 27001:2014 reduce los niveles de riesgo de los establecimientos de salud. En este informe es un estudio de tipo aplicado, de nivel descriptivo y de diseño pre-experimental. La población estuvo conformada por los trabajadores del Centro de Salud Alicia Lastre de la Torre del Distrito de Barranco de la ciudad de Lima, el tipo de muestreo fue el no probabilístico y la muestra estuvo dirigida a los 33 trabajadores que hacen uso de la información de las historias clínicas. La conclusión principal de este estudio fue que la implementación del Sistema de Gestión de Seguridad de la Información basado en los requisitos de la Norma Técnica Peruana ISO/IEC

27001:2014 se ha reducido los niveles de riesgo, dado que durante el procesamiento del instrumento de trabajo se obtuvo una mejora sustancial en relación con la seguridad de los datos de los pacientes que manejan los establecimientos de salud de la Dirección de Redes Integradas de Salud Lima Sur.

(Garcia Cruz, 2020) Este estudio fue desarrollada bajo la línea de investigación: Sistemas de Gestión de la Calidad y Seguridad de la Información, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; tuvo como objetivo Realizar una propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, para minimizar la pérdida de información, la investigación fue desarrollada cuantitativamente bajo el diseño descriptivo de transcripción no experimental. La población de la muestra de la tesis fue constituida por los 23 trabajadores; de los cuales se obtuvo como resultado: el 91% de los trabajadores encuestados expresaron NO están satisfacción con la situación actual; mientras el 9% indicó que, SI se encuentran satisfacción con la situación actual, el 100.00% de los trabajadores encuestados expresaron SI necesitan la seguridad de información con norma ISO 27001. El alcance abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para preservar la confidencialidad, integridad y disponibilidad de la información en la oficina de tecnologías de información del Gobierno Regional Piura. En conclusión, se determinó que la propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura mejoro sus procesos de seguridad de la información y comunicación.

(Cornejo Miranda, 2022)La presente investigación tiene como objetivo general Garantizar la Seguridad de la Información en la Subgerencia

de TI del GRLL con la Implementación de un sistema de gestión de seguridad basado en NTP-ISO/IEC 27001, se utilizó el diseño de investigación experimental y del tipo preexperimental, la población en estudio fueron los 11 trabajadores del área de tecnologías de información y se utilizó la prueba de normalidad de Shapiro Wilk; además se utilizó la norma técnica peruana ISO 27001 para la realización de la investigación, finalmente se concluye que el nivel de integridad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.80 puntos, mientras con la implementación del sistema propuesto es de 4.33 puntos, obteniendo un incremento del 50.60% sobre el nivel de integridad de la información sobre el personal del área tecnologías de información; en el segundo indicador se concluye que el nivel de confidencialidad de la información con respecto a la seguridad de la información con el sistema actual se obtuvo una puntuación de 1.82 puntos, mientras con la implementación del sistema propuesto es de 4.49 puntos, obteniendo un incremento del 53.40% sobre el nivel de confidencialidad de la información sobre el personal del área tecnologías de información; y por último se cuenta una escala del 1 al 5 para medir el nivel de uso de nuevas políticas de seguridad, se obtuvo con el sistema actual de 1.80 puntos y con la implementación propuesta sobre el nivel de uso de nuevas políticas de seguridad es de 4.76 puntos, alcanzando un incremento de 2.96 puntos equivalente al porcentaje de 59.20%.

Según esta tesis (Vilca Mosquera, 2016), tuvo como objetivo la implementación de un sistema de gestión de la seguridad de la información con el fin de mejorar la seguridad en cuanto al uso de los activos y tecnologías de la información en la empresa Geosurvey de la ciudad de Lima en el año 2016. La metodología que se empleó fue bajo el enfoque cuantitativo, y de tipo aplicativo; se utilizó la tecnología para la solución de un problema, se empleó el diseño preexperimental, se

llevó a cabo un experimento en condiciones controladas. Tanto la población como la muestra estuvo conformada por 33 trabajadores siendo no probabilística, se tomaron en cuenta todos los trabajadores de las diferentes áreas de la empresa. Para la recolección de datos como técnica se utilizó un cuestionario, para luego los datos ser procesados en el software estadístico SPSS. Como resultado se obtuvo el diagnóstico de la gestión de riesgos de la empresa, la elaboración de la política se seguridad y asimismo el sistema de gestión de incidentes para poder controlar y mejorar la seguridad de la información de la empresa.

¿De qué forma la implementación del Sistema de Gestión de la Seguridad de la información mejorará la seguridad del área de recursos humanos de la empresa GEOSURVEY SA?

(Coaguila Mamani, 2020) La presente investigación se orienta hacia la elaboración de un Plan de Gestión de Seguridad de la Información alienado la norma ISO/IEC 27001, para fortalecer la seguridad de los sistemas informáticos de la Universidad Nacional de Moquegua. El tipo es aplicada, el diseño es no experimental – transversal, la información fue obtenida a través de la técnica de la encuesta, para esto se utilizó un cuestionario en base a la norma ISO-IEC 27001:2013, la muestra de estudio estuvo conformada por 8 docentes, 81 alumnos y 7 directores de escuela, incluyendo al jefe de DASA, siendo en total 96 encuestados. La propuesta consta de 3 capítulos: Capítulo I el contexto organizacional, el Capítulo II la gestión de riesgos y el Capítulo III el tratamiento de riesgos. Finalmente, la validación de la propuesta se realizó con la participación de 3 expertos, obteniendo un alto nivel de validez, con estos resultados queda demostrada la hipótesis general.

En su estudio titulado: “desarrollo de un sistema hotelero para gestionar la información de los clientes, basado en el apartado de operación de la norma ISO 27001:2014, para el Puerto Hotel-La Libertad tiene por finalidad Determinar de qué manera influye el desarrollo de un sistema

hotelero para gestionar la información de los clientes, basado en el apartado de operación de la Norma ISO 27001:2014, para la empresa El puerto Hotel La Libertad. Este estudio empleo una metodología de tipo aplicada de diseño pre experimental de enfoque cuantitativo, la población está compuesta por 70 trabajadores del Hotel y la muestra está compuesta por 50 trabajadores. Se realizó el análisis de datos mediante software SPSS V 26. Los resultados es que de implementarse mejorará la gestión de la información mantendrá la información segura, secreta y confiable. Se concluye el desarrollo de un sistema hotelero mejorara la gestión de la información, porque el desarrollo del sistema está amparado en la norma ISO 27001

(Giap, 2021)La presente investigación fue ejecutada durante el año 2021, tuvo como objetivo principal determinar la influencia de un sistema de gestión para la seguridad de la información basado en la norma 270001:2013 en la Empresa Constructora Pérez & Pérez SAC, ya que presenta vulnerabilidades en todo los procesos de toda las áreas y peligra los activos de información de la organización, la metodología fue cuantitativa aplicada, se trabajó con el diseño de investigación experimental del tipo preexperimental. Además, se conformó la muestra de 20 registros en cada indicador con la finalidad de obtener un resultado favorable en las dimensiones de seguridad de la información, la confidencialidad de la información de un 68,85% de vulnerabilidad disminuyó a un 15,40% para la integridad de la información tuvo una disminución de vulnerabilidad de un 52,60% a 11,40% y por último la disponibilidad de la información se logró disminuir la vulnerabilidad de un 47,15% a 11,95% en los tres dimensiones se logró aumentar la seguridad de la información a un 80% a 90% de efectividad. Finalmente se acierta que el sistema de gestión para la seguridad de la información basado en la norma iso27001 influye favorablemente en la constructora Pérez & Pérez SAC

(Cabrera Cubas, 2018) Este estudio de investigación tiene como objetivo implantar el diseño de un modelo de políticas basado en la norma ISO 27001 para la gestión de la seguridad de la información en la Municipalidad Distrital de Florida, Bongará – Amazonas, 2018, donde han incrementado mejoras en la seguridad de la información. Por tal motivo el estudio tiene un diseño “Pre-experimental” y una población conformada por el personal administrativo; como el alcalde, Gerente, Tesorero, etc. que en su conjunto suman 13 trabajadores. Los resultados que se obtuvieron en el post test fueron satisfactorios ya que los trabajadores que laboran en dicha entidad están comprometidos y capacitados con temas relacionados con la seguridad de la información, eso quiere decir que la información que posee dicha entidad se encuentra protegida y segura. La investigación se dio por medio de cuatro dimensiones como: Políticas, Servicio, Riesgo y Consistencia; de estas dimensiones se muestra que la significancia bilateral (valor de P) es 0,717, 0,732, 0,394, 0,886 la cual es mayor a 0.05.

Este proyecto (Sandoval Alania, 2020), se originó a partir de la preocupación en la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco acerca de la seguridad de su información. La organización carecía de políticas y medidas para salvaguardar sus activos contra amenazas y riesgos. Para abordar esta problemática, se emplearon la Norma Técnica Peruana NTP – ISO/IEC 27001:2014 y la metodología MAGERIT versión 3 (v3) para analizar y gestionar los riesgos de los activos. El proceso comenzó con una evaluación del estado inicial de la organización en términos de seguridad de la información, seguido de la planificación y diseño del Sistema de Gestión de Seguridad de la Información. Se definieron el alcance, las políticas y el comité de seguridad, y luego se procedió al análisis y gestión de riesgos para identificar las amenazas y vulnerabilidades a las que estaban expuestos los activos de información. Los resultados

del análisis se utilizaron para desarrollar un tratamiento de riesgos, establecer controles de seguridad y diseñar una declaración de aplicabilidad conforme a la Norma Técnica Peruana NTP – ISO/IEC 27001:2014. Además de identificar los controles necesarios, el proyecto familiarizó a la organización con la seguridad de la información y proporcionó la documentación esencial para futuras implementaciones del Sistema de Gestión de Seguridad de la Información en los procesos de la entidad.

La investigación denominada (Silva Guerrero, 2018), para el proceso de ventas de la empresa 'Energía Perú S.A.C.', 2018" se enfoca en gestionar los activos de información durante el proceso de venta. La empresa enfrenta desafíos a medida que crece, incluyendo la dificultad para mantener la información organizada y confiable. La responsabilidad del uso adecuado de la información recae en todos los empleados, pero no todos le otorgan la misma importancia ni la protección necesaria. Esta falta de cuidado puede exponer a la empresa a riesgos como daños económicos, daños a su reputación, robo o alteración de datos, entre otros. El estudio se plantea la pregunta de cómo la Norma Internacional ISO/IEC 27001:2013 puede mejorar la Gestión de la Información en Energía Perú S.A.C. Se concluye que cumplir con los requisitos de la norma no es suficiente; la participación de la alta dirección en el proceso de Diseño e Implementación del Sistema de Gestión de Seguridad de la Información (SGSI) es fundamental. Además, este sistema debe estar alineado constantemente con los objetivos de la organización. Después de implementar la ISO/IEC 27001:2013, la empresa puede obtener mayores beneficios al integrar otras normas ISO, lo que mejora el rendimiento de los procesos y permite ofrecer un servicio o producto de mejor calidad con una inversión mínima.

(Ibarra Caqui, 2023)El estudio presenta por objetivo general determinar

la influencia de la implementación ISO 27001:2013 en la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, referente a la metodología que se adoptó en el estudio se considera de tipo aplicada, el diseño fue experimental, con subcategoría preexperimental, el alcance temporal que presento fue longitudinal. La población se confirmó por 42 trabajadores, la muestra se conformó por la misma cantidad y el muestreo aplicado fue el no probabilístico, dentro de ello, se aplicó como técnica a la encuesta y el instrumento fue el cuestionario, para la aplicación se realizó el proceso de validación y confiabilidad, alcanzando un valor de 0.859. Logrando concluir: Se ha mejorado significativamente (sig. = 0.000 < 0.05) la gestión del manejo de información en la UGEL Bolognesi Ancash 2023, a través de la implementación ISO 27001:2013, en el nivel deficiente se redujo en 52.4% en el post-test, luego para el nivel regular se mejoró en 19.0% y el nivel eficiente se incrementó en 71.4%.

(Luna Castillo, 2019) La presente investigación tuvo como objetivo general proponer una Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014 para la seguridad de la información en la Municipalidad Provincial de Recuay. La investigación fue del tipo no experimental descriptivo porque se describieron los aportes de las normas estudiadas a la seguridad de la información de la municipalidad. La población de estudio estuvo conformada por 48 servidores públicos que utilizan el sistema de información y a la vez procesan información en Municipalidad Provincial de Recuay, y la muestra por 20 servidores públicos, para el desarrollo del presente informe se utilizó la Norma ISO/IEC 27001:2013 Y NTP ISO/IEC 27001:2014 La investigación concluyó que el estado en que se encontró la seguridad de la información además de los riesgos, vulnerabilidades y formas de prevención en la Municipalidad Provincial de Recuay fue porcentualmente bueno y que las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración de la información

fue mayormente buena.

(Cosios Avila, 2021)presente investigación ha sido desarrollada bajo la línea de investigación desarrollo de modelos y aplicación de las tecnologías de información y comunicaciones para la mejora continua de calidad de las organizaciones del Perú de la escuela profesional de Ingeniería de Sistemas, la cual estuvo basada en realizar una Implementación de Auditoría Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; 2020.El tipo de investigación fue no experimental, descriptiva y de corte transversal, teniendo como objetivo general Implementar una Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; para mejorar el sistema de información. Con una muestra de 40 miembros. Los resultados obtenidos en el primer nivel de conocimiento de la información de Implementación de auditoria informática con la ISO 27001, el 50% de los trabajadores encuestados indicaron que NO tienen conocimiento de seguridad informática y seguridad de un sistema de información. En la segunda dimensión seguridad de la información, el 55% de los trabajadores encuestados indicaron que NO hay seguridad de la información en dicha municipalidad, se puede concluir que en la municipalidad los trabajadores desconocen acerca lo que es seguridad de información y por lo cual no se realiza una buena seguridad de la información en el sistema.

(Rodriguez Baca, Liset Sulay, Cruzado Puente de la Vega, Carlos Francisco, Mejía Corredor, Carolina, Alarcón Diaz, Mitchell Alberto, 2020) El avance de la tecnología en el mundo provoca, entre otros aspectos, el manejo de importante información la misma que puede considerarse como fundamental para los intereses estratégicos de las empresas. La investigación tuvo como objetivo el analizar la influencia de la aplicación del ISO 27001 en la seguridad de la información de una empresa privada de Lima (Perú). A partir de la aplicación de una

metodología cuantitativa, se empleó un estudio preexperimental en el que se determinó la influencia de la aplicación del ISO 27001.Para ello se consideró a una muestra de 30 colaboradores de la empresa. La conclusión cuantitativa muestra que si existe una influencia de la aplicación del ISO en la seguridad de la información y en las dimensiones confidencialidad, integridad y disponibilidad.

Según la investigación, (García Martínez 2006), sustentó la tesis con el título “Proyecto CAMERSEC - Implantación de Sistemas de Gestión de Seguridad de la Información en PYMES”. En la Universidad Pedro Ruiz Gallo, Perú. Tuvo como objetivo Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad Del Área De Operaciones Y Tecnología De Global BPO Center Allus Chiclayo. Con una metodología cuantitativa, pre experimental, ya que se ha empleado para recopilar datos numéricos y medibles con el fin de realizar análisis estadísticos, con una muestra de 1 área con 10 usuarios como parte interesada, se usó como instrumentos: PDCA, COBIT. Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación. Se logró incrementar los procedimientos utilizados en favor de la empresa permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla.

Según la investigación (Martinez, 2006), sustentó la tesis con el título “Proyecto CAMERSEC - Implantación de Sistemas de Gestión de Seguridad de la Información en PYMES”. En la Universidad Pedro Ruiz Gallo, Perú. Tuvo como objetivo Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad Del Área De Operaciones Y Tecnología De Global BPO Center Allus Chiclayo. Con una metodología cuantitativa, pre experimental, ya que se ha empleado para recopilar datos

numéricos y medibles con el fin de realizar análisis estadísticos, con una muestra de 1 área con 10 usuarios como parte interesada, se usó como instrumentos: PDCA, COBIT. Los resultados obtenidos permitieron determinar de forma real que, al incorporar la norma ISO/IEC 27001 basada en una Guía de Implementación. Se logró incrementar los procedimientos utilizados en favor de la empresa permitiéndole la detección de anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla.

## 2.2 Bases teóricas:

### 2.2.1. EL SGSI (Sistema de Gestión de la Seguridad de la Información).

SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), y su origen (de la propia organización o de fuentes externas) (Chang, 2011).

Este proceso es el que constituye un SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información. La Seguridad de la Información consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

“Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015” (G, 2007)

Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth 52

De una manera más estricta una metodología para, un Sistema de Gestión de

Seguridad de la Información es aquella parte del Sistema General de gestión de una organización que deberá incorporar:

- La Política.
- La Estructura Organizativa.
- Los Procedimientos.
- Los Controles necesarios para implantar la gestión de la Seguridad de la Información. (Ampuero, 2011)

### 2.2.2. ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de la información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de la organización para asegurar el máximo beneficio de nuevas oportunidades de mejora de la organización, son algunos de los aspectos fundamentales para la creación de una metodología para la implementación de un SGSI, es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una metodología “Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015”

Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth 53 sistemática definida, documentada y conocida por todos, que se

revisa y mejora constantemente. (Ampuero, 2011)

### 2.2.3. Fundamentos de un SGSI

Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

"Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de la Agencia de Compras de las Fuerzas Armadas - 2023" (G, 2007)

### 2.2.4. Norma ISO 27001

ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

"Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de la Agencia de Compras de las Fuerzas

Armadas - 2023”

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento.

Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth 57. (Center, 2014)

### 2.2.5. ¿Cómo funciona la ISO 27001?

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo).

Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica (por ejemplo, software y equipos).

Sin embargo, en la mayoría de los casos, las empresas ya tienen todo el hardware y software, pero utilizan de una forma no segura; por lo tanto, la mayor parte de la implementación de ISO 27001 estará

relacionada con determinar las reglas. (Center, 2014)

### 2.2.6 Definición Técnica de Seguridad

La etimología de "seguridad" se origina en el latín "securitas," derivado de "securus" (carecer de preocupaciones), que denota la ausencia de peligro o daño. Desde una perspectiva psicosocial, se considera un estado mental que genera en los individuos (personas y animales) un sentimiento de estar libres de peligro en cualquier circunstancia. La seguridad representa la garantía de estar exento de daño, amenazas, peligros o riesgos. Es la necesidad de sentirse protegido contra cualquier factor que pueda perturbar o amenazar la integridad física, moral, social e incluso económica.

La seguridad se desglosa en dos dimensiones: individual y social. La primera se refiere al autocuidado de cada individuo para evitar poner en riesgo su salud y vida. La seguridad social abarca leyes, organismos, servicios e instalaciones que cubren y protegen las necesidades de la población, como la atención médica, pensiones y subsidios. Es esencial comprender que la seguridad implica realizar las actividades de manera correcta, por lo que se requiere un esfuerzo significativo en la eliminación de riesgos y la prevención de accidentes. (Venemedia, 2014)

### 2.2.7 Definición Técnica de Seguridad en Tecnología de la Información (TI)

La seguridad de la información abarca un conjunto de medidas preventivas y reactivas implementadas por organizaciones y sistemas tecnológicos. Su objetivo principal es preservar y salvaguardar la información, con énfasis en la confidencialidad, disponibilidad e integridad de los datos.

Es importante distinguir el concepto de seguridad de la información de la seguridad informática. La primera se centra en la protección de la

información, independientemente de su forma o medio, mientras que la seguridad informática se enfoca exclusivamente en la seguridad de los sistemas informáticos.

La seguridad de la información tiene un impacto significativo en la privacidad de las personas y puede variar en función de las diferencias culturales.

Este campo de estudio experimentó un notable crecimiento y evolución desde la Segunda Guerra Mundial y ha adquirido reconocimiento a nivel global. Ofrece diversas áreas de especialización, incluyendo auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otras.

### 2.2.8 ¿Qué es un riesgo?

La palabra Riesgo viene del italiano Risicare, que Significa desafiar, retar, enfrentar; también se define como poner en peligro a una persona, en algunos escritos se refiere a la proximidad de un daño. El riesgo también es conocido como la probabilidad de pérdida la cual permite cuantificar el riesgo a diferencia de la posibilidad de riesgo donde este no se puede cuantificar. El riesgo es Incertidumbre relacionado con la duda ante la posible ocurrencia de algo que puede generar pérdidas. (Mejía, 2014)

### 2.2.9 Concepto Técnico de Riesgo

La palabra "Riesgo" tiene su origen en el italiano "Risicare," que se traduce como desafiar, retar o confrontar. En términos técnicos, se define como la exposición a la posibilidad de un daño o pérdida. El riesgo también se asocia con la probabilidad cuantificable de sufrir una pérdida, a diferencia de la mera posibilidad de riesgo, que no

puede medirse de manera precisa. En un contexto técnico, el riesgo se interpreta como la incertidumbre vinculada a la duda sobre la eventualidad de un evento que podría resultar en pérdidas.

### 2.2.10 Riesgos Del Entorno

Comprende elementos como el país donde está ubicada la empresa, su naturaleza, la región y ciudad, además del sector, la industria y condiciones económicas, políticas, sociales y culturales. En este orden de ideas se pueden presentar riesgos como:

- Riesgo asociado a la naturaleza: Relacionados con riesgos meteorológicos y climáticos como huracanes, lluvias, maremotos, sequías, que afectan el logro de Objetivos.
- Riesgos asociados al País: De acuerdo con el País se pueden encontrar riesgos como el riesgo país que hace referencia al grado de peligro que represente este para las inversiones extranjeras

### 2.2.11 Riesgos generados en la empresa:

A nivel de la empresa se pueden presentar un sinfín de riesgos que pueden afectar los procesos, recursos humanos, físicos, tecnológicos, financieros y organizacionales, a los clientes y hasta la imagen de la empresa. En este orden de ideas se pueden presentar riesgos como:

- **Riesgo de reputación:** es el desprestigio de la empresa que trae como consecuencia la pérdida de credibilidad y confianza del público por fraude, insolvencia, conducta irregular de los empleados, rumores, errores cometidos en la ejecución de alguna operación por falta de capacitación del personal clave o deficiencia en el diseño de los procedimientos, este riesgo puede traer efectos como disminución de la demanda, o la perdida de negocios atribuibles al desprestigio generado.
- “Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de la Agencia de Compras de las

Fuerzas Armadas - 2023”.

- **Riesgo puro:** este riesgo al materializarse origina perdida, como un incendio, un accidente, una inundación.
- **Riesgo especulativo:** al materializarse genera la posibilidad de generar instantáneamente beneficio o pérdida, como una aventura comercial, la inversión en divisas ante expectativas de devaluación o revaluación, la compra de acciones, el lanzamiento de nuevos productos, etc.
- **Riesgo estratégico:** son las pérdidas ocasionas por las definiciones estratégicas Inadecuadas y errores en el diseño de planes, programas, estructura, integración del modelo de operación con el direccionamiento estratégico, asignación de recursos, estilo de dirección, además de ineficiencia en la adaptación a los cambios constantes del entorno empresarial, entre otros.
- **Riesgo operativo:** es la posibilidad de pérdidas ocasionadas en la ejecución de los procesos y funciones de la empresa por fallas en procesos, sistemas, procedimientos, modelos o personas que participan en dichos procesos.
- **Riesgo de mercado:** puede generar ganancias o pérdidas a la empresa al invertir en bolsa, debido a la diferencia en los precios que se registran en el mercado.
- **Riesgo precio de insumos y productos:** se refiere a la incertidumbre sobre la magnitud de los flujos de caja debido a posibles cambios en los precios que una empresa puede pagar por la mano de obra, materiales y otros insumos de su proceso de producción, y por los precios que puede demandar por sus bienes o servicios.
- **Riesgo de crédito:** consiste en que los clientes y las partes a las cuales se les ha prestado dinero fallen en el pago. La mayoría de las empresas se enfrentan al “Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de la

Agencia de Compras de las Fuerzas Armadas - 2023”

- Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth 47 este riesgo por cuentas por cobrar, pero esta exposición es más alta en las instituciones financieras.
- **Riesgo legal:** se refiere a la pérdida en caso de incumplimiento de la contraparte en un negocio y la imposibilidad de exigirle jurídicamente el cumplimiento de los compromisos adquiridos. También se puede presentar al cometer algún error de interpretación jurídica u omisión en la documentación, y en el incumplimiento de normas legales y disposiciones reglamentarias que pueden conducir a demandas o sanciones.
- **Riesgo tecnológico**: el uso de la tecnología genera riesgos como los virus, el vandalismo puro y de ocio en las redes informáticas, fraudes, intrusiones por hackers, el colapso de las telecomunicaciones que pueden generar el daño de la información o la interrupción del servicio. También está el riesgo del constante cambio de tecnología lo que puede ocasionar que las empresas no estén preparadas para adoptarlas y esto incremente sus costos, menor eficiencia, incumplimiento en las condiciones de satisfacción de los servicios prestados a la comunidad.
- **Riesgos laborales:** pueden ser accidentes de trabajo y enfermedades profesionales, pueden ocasionar daños tanto a la persona como a la misma empresa.
- **Riesgos físicos:** afectan a los materiales como, por ejemplo; corto circuito, explosión física, daño en la maquinaria, daño en equipos por su operación, por su diseño, fabricación, montaje o mantenimientos; deterioros de productos y daños en vehículos.
- **“Sistema de Gestión de Seguridad de Información (SGSI**) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de la Agencia de Compras de las Fuerzas Armadas - 2023”

### 2.2.12 ¿Qué es un Activo?

Es el conjunto de bienes económicos, derechos a cobrar que posee un comerciante o una empresa y aquellas erogaciones que serán aprovechadas en ejercicios futuros. El Marco Conceptual para la Información Financiera del IASB (International Accounting Standards Board (Junta de Normas Internacionales de Contabilidad)), emitido el 1 de enero de 2012, establece la siguiente definición:

«Un activo es un recurso controlado por la entidad como resultado de sucesos pasados, del que la entidad espera obtener, en el futuro, beneficios económicos».

En las registraciones o registros contables cuando se produce una variación de un elemento de activo, ésta puede ser de dos tipos: aumento del activo, se carga o debita anotándose en él debe o disminución del activo se abona o acredita, esto es, se realiza una anotación en el haber.

### 2.2.13. Tipos de Activos

Dentro de los activos de la empresa se pueden diferenciar dos tipos:

#### 2.2.13.1 Activo fijo:

Hace referencia a aquellos bienes y derechos duraderos, que han sido obtenidos con el fin de ser explotados por la empresa. Se trata de aquellos bienes inmuebles, materiales, equipamiento, herramientas y utensilios con los que no se va a comercializar, es decir, que no se van a convertir en líquido, al menos durante el primer año.

En cualquier tipo de empresa se pueden diferenciar dos tipos de activos fijos:

“Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015”

Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth 49 (Empresarial, 2016)

- **Activos fijos tangibles.**

  Dentro de esta categoría se incluyen todos aquellos bienes y materiales tangibles, es decir, se pueden tocar. En función de las características de tu negocio los activos fijos podrán variar de manera notoria. Algunos de los bienes tangibles de los que pueden disfrutar las empresas, acorde a la clasificación establecida por el Plan General Contable, son:

- Terrenos y bienes naturales. Aquellos terrenos y solares que posea la empresa, ya sea urbanos o no.
- Construcciones. Hace referencia a todo tipo de inmuebles, en general, que son propiedad de la organización, como edificios, naves, pisos o locales.
- Instalaciones técnicas. Este concepto hace alusión a todos aquellos elementos que, en conjunto, constituyen una unidad de uso especializada necesaria para la actividad de la empresa. Se trata de montajes en cadena y otro tipo de construcciones similares.
- Maquinaria. Dentro de este apartado se incluyen todas aquellas máquinas,
- vehículos industriales y herramientas necesarias para la actividad cotidiana.
- Mobiliario. Todas las estanterías, mesas, sillas, mostradores y demás muebles que la empresa posee.
- Equipos para procesos informáticos. Compuesto por ordenadores, impresoras, escáner y demás aparatos electrónicos.
- Elementos de transporte. Dentro de esta categoría se encuentran todos los medios de transporte que formen

parte de los bienes de la compañía, como coches, “Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015”

Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth 50 camiones, motos, barcos, etc., utilizados para el transporte de personas, mercancías, materiales o animales.

- Otros. Aquellos bienes que no se puedan incluir dentro de ninguna de las categorías nombradas.

- **Activos fijo-intangibles.**

  Por su parte, los activos intangibles hacen referencia a aquellos bienes y derechos que no son físicos o palpables como tal. Se trata de bienes como marcas, permisos, patentes, derechos de traspaso, fondos de comercio o gastos de investigación.

  Marcas registradas. Una marca registrada es un derecho que pude ser adquirido, vendido o arrendarse.

- Patentes. Es un derecho que te otorga un permiso especial y exclusivo, para vender o fabricar un producto o servicio.
- Derechos de autor. Con este derecho se garantiza al autor su derecho a explotar sus productos.
- Franquicias. Por medio de este derecho, la empresa adquiere permiso para poder hacer uso de la marca y productos de otra empresa durante un tiempo determinado.
- Licencias y permisos. Se trata de autorizaciones a través de las que se concede el uso de bienes diferentes, como el caso de recursos software para la empresa.

"Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo - 2015"

Rojas Viera Cinthia Katherine – Zavaleta Verona Tefhany Lisseth

#### 2.2.13.2. Activo circulante:

Este tipo de activo, también denominado corriente o líquido, hace referencia al dinero del que dispone la empresa o del que puede disponer en un plazo inferior a doce meses. Es decir, aquellos bienes, derechos o créditos, que pueda utilizarse o convertirse en líquido cuando se necesite.

## 2.3. Marco conceptual

Los sistemas de Gestión de seguridad de la información representan una realidad en constante innovación, potencializada por las técnicas de información y comunicación (TIC) y por las exigencias actuales de la sociedad en la seguridad de la información. Garantizar un nivel de protección total es probablemente imposible, incluso en el caso de disponer de un presupuesto ilimitado. Es importante, sin embargo, tomar las medidas para mejorar continuamente para alcanzar a competir a nivel global. Es evidente que es necesario implementar acciones para que las empresas sean certificadas bajo la norma ISO/IEC 27001 en un mediano plazo, como una obligación para poder competir en el mercado (Flores Barrios, y otros, 2011). En los últimos años con el uso intensivo de las tecnologías de información, la seguridad de la información se ha convertido en un tema crucial y estratégico para la gestión organizacional. Diversos estándares y guías para la seguridad de la información como ISO/IEC 27001, ISO/IEC 27002, COBIT se han desarrollado, sin embargo, las organizaciones enfrentan aun

dificultades en su implementación. La información es uno de los activos más importantes que cuentan las organizaciones. El crecimiento de las TI y el uso intensivo de internet traen consigo amenazas, riesgos y vulnerabilidades. La información de las instituciones públicas puede estar en riesgo si es que no se implementan el Sistema de Gestión de la Seguridad de la Información. En el Perú se ha establecido la NTP ISO/IEC 27001 como norma de cumplimiento obligatorio. Las instituciones aun presentan dificultades en la implementación de la norma. Aspectos como personal calificado, concientización, falta de formación han sido identificados como dificultades. Al respecto, diversos autores y estudios demuestran que existe un conjunto de factores críticos que deben ser considerados cuando se implementan las buenas prácticas internacionales. En la gestión pública, toda información que maneja el Estado es de dominio público, sin embargo, debe tener presente la información sensible establecida por la Ley de protección de datos personales. Finalmente, es necesario sensibilizar al más alto nivel sobre la importancia de la seguridad de la información y sus efectos en caso de no adoptar acciones preventivas (Sussy, y otros, 2015). Se debe promover un eficiente sistema de aterramiento para las líneas de energía en toda la infraestructura de la empresa y fomentar el uso de equipos que permiten proteger ante fluctuaciones de voltaje, seguidos de permanentes programas de mantenimiento de equipos informáticos, considerando el control de registros de acuerdo con el tipo de mantenimiento, además de propiciar la inversión para compensar la obsolescencia de las tecnologías, como también afianzar los mecanismos de seguridad correspondientes al cambio periódico de password para el personal de la organización. Sin dejar de destacar, llevar a la práctica cada una de las fases del modelo de Sistema de Gestión de Seguridad la Información en redes locales para empresas de desarrollo de software, que permitan alcanzar la implementación de este. Del mismo modo, estimular la creación de estrategias o políticas de seguridad desarrolladas por el personal de los departamentos de desarrollo y soporte con el objetivo de contrarrestar nuevas amenazas (Salamanca, 2016). La cantidad de normas con que cuenta actualmente la familia ISO/IEC 27000

para llevar a cabo la implementación de un sistema de gestión de seguridad de la información, pone de manifiesto una complejidad adicional al proceso de desarrollo de este (Francisco Javier Valencia-Duque 1, 2017). Un Sistema de Gestión de Seguridad de la Información (SGSI) permite recepcionar, administrar y organizar la documentación generada en el proceso de implantación del SGSI. Para soportar dicho software, se diseña e implementa un modelo que define acciones de gestión necesarias para la aprobación, revisión, actualización, estados y legibilidad en documentos durante el ciclo de vida del SGSI. Sobre el modelo y la herramienta que lo soporta se podría obtener: 1) identificar el estado de los documentos; 2) Prevenir la utilización de documentos obsoletos; 3) Garantizar la disponibilidad, accesibilidad y seguimiento a documentos asignados; 4) Permitir trabajar bajo procedimientos estrictamente del estándar ISO 27001; y 6) Modelo de trabajo cíclico (Raúl J. Martelo, 2015).

## 2.4 Definición de términos básicos

### 2.4.1. ¿Qué es un Análisis de brecha?

En la investigación: (ROCHA CAHUEÑAS, 2019) , se utilizó el workbook oficial de la norma ISO 27001 como herramienta para evaluar la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO/IEC 27001. En el contexto organizacional, se notó la ausencia de una política de seguridad de la información adaptada al proceso estratégico analizado. Una de las figuras reveló un nivel de cumplimiento de implementación inferior al 50% en algunos casos, indicando una falta de controles básicos. Esto sugiere una vulnerabilidad significativa ante ataques externos, confirmada por pruebas de intrusión con OWASP ZAP. El Análisis de brecha fue usado para determinar el nivel de vulnerabilidad de la plataforma ante ataques que pudieran comprometer la disponibilidad, integridad y confidencialidad de la información. (ROCHA CAHUEÑAS, 2019)

### 2.4.2. Sistema de Gestión de la Seguridad de la Información

La información se estructura de datos que provienen de diferentes fuentes y que circulan a través de las bases y las redes cibernéticas, transformando las organizaciones modernas y destacando la importancia de gestionar adecuadamente la seguridad de esta información. (LOPEZ, 2016)

### 2.4.3 ISO 27001

La ISO 27001 promueve un enfoque basado en procesos adoptando el modelo de Deaming, en el que se plantea un ciclo de mejora continua, a través de la repetición de la fase de "Planificar-Hacer-Verificar-Actuar conocido como (PHVA) o (PDCA) por sus siglas en inglés "Plan-Do-Check-Act). (Jacome Sanchez, 2022)

# III. HIPOTESIS y VIARIABLES

## 3.1 Hipótesis

La ISO 27001 permitirá desarrollar un Sistema de Gestión de Seguridad de la Información para la Agencia de Compras de las Fuerzas Armadas, 2023.

### Hipótesis Específicas

1.- La ISO 27001 permitirá definir el estado situacional permitirá conocer como están definidos los procesos actualmente existentes en la Agencia de Compras de las Fuerzas Armadas, 2023.

2.- La ISO 27001 permitirá establecer la brecha o comparación que nos ayudará a ver exactamente cómo estamos protegiendo nuestros datos ahora y cómo deberíamos hacerlo con el nuevo sistema de seguridad planteado basado en la ISO 27001.

3.- La ISO 27001 permitirá establecer controles y responsabilidades para desarrollar el Sistema de Gestión de Seguridad de la Información para la Agencia de Compras de las Fuerzas Armadas, 2023.

### 3.1.1. Operacionalización de variables

**Matriz de Operacionalización**

En el presente trabajo se han planteado como variable independiente El Sistema de Gestión de Seguridad de la Información y, como variable dependiente ISO 27001. En el anexo 3 se desarrolla la operacionalización, en la cual se definen los conceptos, operaciones, indicadores y escalas de medición. (Ver Tabla 1).

| Variables | Definición Conceptual | Definición Operacional | Dimensiones | Indicadores | Concepto del Indicador |
|---|---|---|---|---|---|
| **Sistema de Gestión de Seguridad de la Información** | Es posible gestionar adecuadamente la seguridad de la información en los institutos de educación superior aeronáutica, mediante un Sistema de Gestión de Seguridad de la Información. (LOPEZ, 2016) | La Gestión de la ISO 27001 se mide, en cláusulas PDCA de propuestas según sus dimensiones e indicadores. | Número de Procesos /Dominios/Controles Implementados | Duración Operativa<br><br>Nivel de Implementación | **Duración Operativa= Tiempo en Minutos/Días/Semanas**<br><br>**Nivel de Implementación = (Número de Procesos Implementados/ Total de Procesos)x100** |
| **ISO 27001** | La implementación del SGSI según la normativa ISO 27001 se considera esencial para preservar la confidencialidad, integridad y disponibilidad de la información. Esta medida no solo mejora la seguridad, sino que también fortalece la imagen corporativa y la confiabilidad. (Jacome Sanchez, 2022) | | Tiempo de duración de la Implementación del proceso | Procesos en Desarrollo<br><br>Índice de Riesgo<br><br>% de Cumplimiento de Requisitos de Seguridad | **Procesos en Desarrollo = Número de Procesos Implementados a Medias**<br><br>**Índice de Riesgo = Probabilidad x Impacto**<br><br>**% de cumplimiento = (Número de requisitos cumplidos / Número total de requisitos) * 100** |

Tabla 1 Matriz de Operacionalización.

Elaboración Propia.

# IV. METODOLOGÍA DEL PROYECTO

## 4.1. Diseño metodológico

En este estudio, adoptamos una perspectiva de exploración profunda, influenciada por las orientaciones de Sampieri. En este estudio, adoptamos una perspectiva de exploración profunda, influenciada por las orientaciones de Sampieri. En lugar de un diseño descriptivo clásico, nos sumergimos en el análisis detallado de fenómenos, evitando la manipulación de variables en condiciones controladas. Este enfoque se destaca por su idoneidad en investigaciones pioneras y exploratorias, donde buscamos comprender la complejidad sin imponer condiciones artificiales.

En vez de centrarnos en relaciones causales en un contexto limitado, nuestra atención se dirige hacia la comprensión holística de los fenómenos estudiados. A través de la exploración profunda, buscamos revelar patrones, conexiones y matices que podrían escapar a un enfoque meramente descriptivo. Este cambio nos permite capturar la riqueza y la diversidad de los datos de manera más auténtica, contribuyendo a una comprensión más completa de los temas explorados.

La implementación de la NTP ISO/27001:2014 implica una serie de controles y medidas para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) en una organización. A continuación, se analiza cómo influyen estos controles en la implementación de un SGSI y cómo se puede medir el avance y desarrollo de cada uno de ellos:

Antes de la implementación:

- Riesgos de seguridad de la información: Antes de la implementación, una organización puede estar expuesta a diversos riesgos de seguridad de la información, como la pérdida de datos, la brecha de la confidencialidad y la integridad de la información, así como la interrupción de los servicios.

- Falta de un SGSI formal: La organización puede carecer de un marco estructurado para gestionar la seguridad de la información. Los procedimientos y políticas de seguridad pueden ser ad hoc o inexistentes.
- Escaso control de accesos: Puede haber poca claridad sobre quién tiene acceso a qué información. La gestión de contraseñas y las políticas de acceso pueden ser débiles o inconsistentes.

## 4.2. Método de investigación

La investigación sigue un método básico-aplicado-descriptivo, tal como indican (Neill, 2017). Conlleva la adición de un análisis GAP que permitirá probar la implementación en diferentes etapas, desde un 0% inicial hasta un 100% futuro.

## 4.3. Población y muestra.

La población abarca la totalidad del entorno organizacional y sus activos de información, siendo el Sistema de Gestión de Seguridad de la Información (SGSI) responsable de salvaguardar todas las áreas y activos propensos a riesgos de seguridad.

En el proceso de implementación del SGSI, la muestra se materializa mediante el desarrollo de políticas y controles específicos. Estos están diseñados para abordar de manera focalizada las áreas críticas identificadas durante el análisis de riesgos. Así, la muestra, en este contexto, representa las medidas específicas y personalizadas que se aplican para mitigar y gestionar los riesgos de seguridad identificados.

## 4.4. Lugar de estudio y periodo desarrollado.

El lugar de estudio es la Agencia de Compras de las Fuerzas Armadas del Perú ubicado en la Av. Arequipa cuadra 3 s/n Cercado de Lima. Se desarrollo la propuesta durante 3 meses.

## 4.5. Técnicas e instrumentos para la recolección de la información.

En el proceso de implementación de un Sistema de Gestión de Seguridad

de la Información (SGSI) basado en la norma ISO 27001, se empleará una combinación de técnicas y herramientas específicas para asegurar la integridad y eficacia del sistema:

**Técnica de Recolección de Datos Teóricos Científicos:**

Se utilizará la técnica de exploración conceptual, enfocada en la revisión detallada de materiales bibliográficos específicos relacionados con la norma ISO 27001 y sus requisitos de seguridad informática.

**Instrumentos para la Demostración de la Hipótesis:**

Para obtener datos descriptivos relevantes, se implementarán políticas específicas definidas por la norma ISO 27001, utilizando herramientas de auditoría y análisis de riesgos.

Los resultados de estas auditorías y análisis de riesgos serán los instrumentos clave para respaldar la eficacia del SGSI.

Este enfoque integral garantiza que la propuesta de implementación del SGSI se alinee de manera directa con las mejores prácticas y requisitos establecidos por la norma ISO 27001, asegurando un abordaje sólido y efectivo en la seguridad de la información.

## 4.6. Análisis y procesamiento de datos.

Las variables involucradas en la investigación no presentan naturaleza estocástica, por lo que no necesitan análisis estadístico. En su lugar, se emplean métodos descriptivos en la evaluación de un SGSI.

## 4.7. Aspectos Éticos en Investigación

**Consideración de la Privacidad de los Datos:**

Es crucial garantizar la confidencialidad de la información recopilada durante la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

**Consentimiento Informado:**

Obtener el consentimiento informado de todas las partes involucradas en la investigación, asegurándose de que comprendan los objetivos y

riesgos del SGSI.

**Transparencia y Honestidad:**

Ser transparente en la recopilación y uso de datos, comunicando claramente los propósitos y beneficios del SGSI a todas las partes interesadas.

**Evitar Conflictos de Interés:**

Identificar y gestionar cualquier conflicto de interés que pueda surgir durante la implementación del SGSI, garantizando la imparcialidad y objetividad en la investigación.

**Protección de Participantes:**

Implementar medidas para proteger a los participantes del SGSI, asegurando que no se vean afectados negativamente por su participación.

**Revisión Ética:**

Someter la propuesta de implementación del SGSI a una revisión ética por parte de un comité ético, si es necesario, para garantizar la conformidad con los estándares éticos y normas establecidas.

# V RESULTADOS

## 5.1 Diseño

### 5.1.1 Diseño de las políticas de los dominios en base a la ISO 27001

El objetivo es crear políticas que no solo cumplan con estándares globales, sino que también se integren sin problemas en la cultura y operaciones diarias de la empresa.

### 5.1.2 CLÁUSULAS DE LA NORMA ISO/IEC 27001:2014 CONTEXTO DE LA ORGANIZACIÓN

La ACFFAA debe analizar el contexto interno y externo, identificar

las necesidades y partes interesadas, así como determinar el alcance del SGSI con la finalidad de implementar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información, de conformidad con los requisitos de la ISO/IEC 27001:2013. La ilustración 2 detalla el contexto de la organización por cada ente respectivo (Ver Ilustración 2).

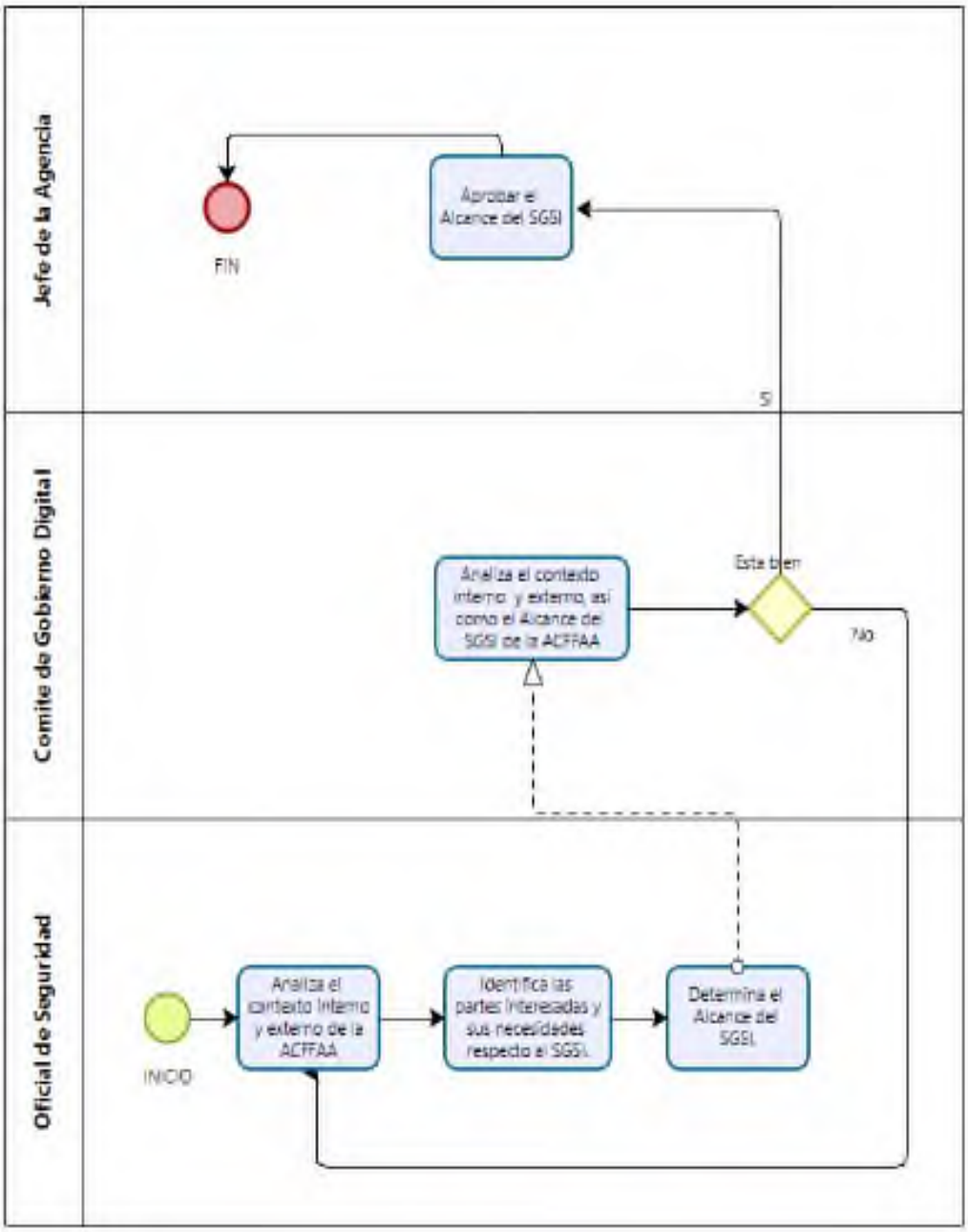


Ilustración 2 Diagrama de Contexto de la Organización.

Elaboración Propia.

## 5.2 LIDERAZGO

La ACFFAA define roles y funciones, así como las responsabilidades del SGSI aprobadas por el Jefe de la ACFFAA para el cumplimiento de las políticas. La ilustración 3 detalla las actividades de liderazgo por cada ente respectivo.

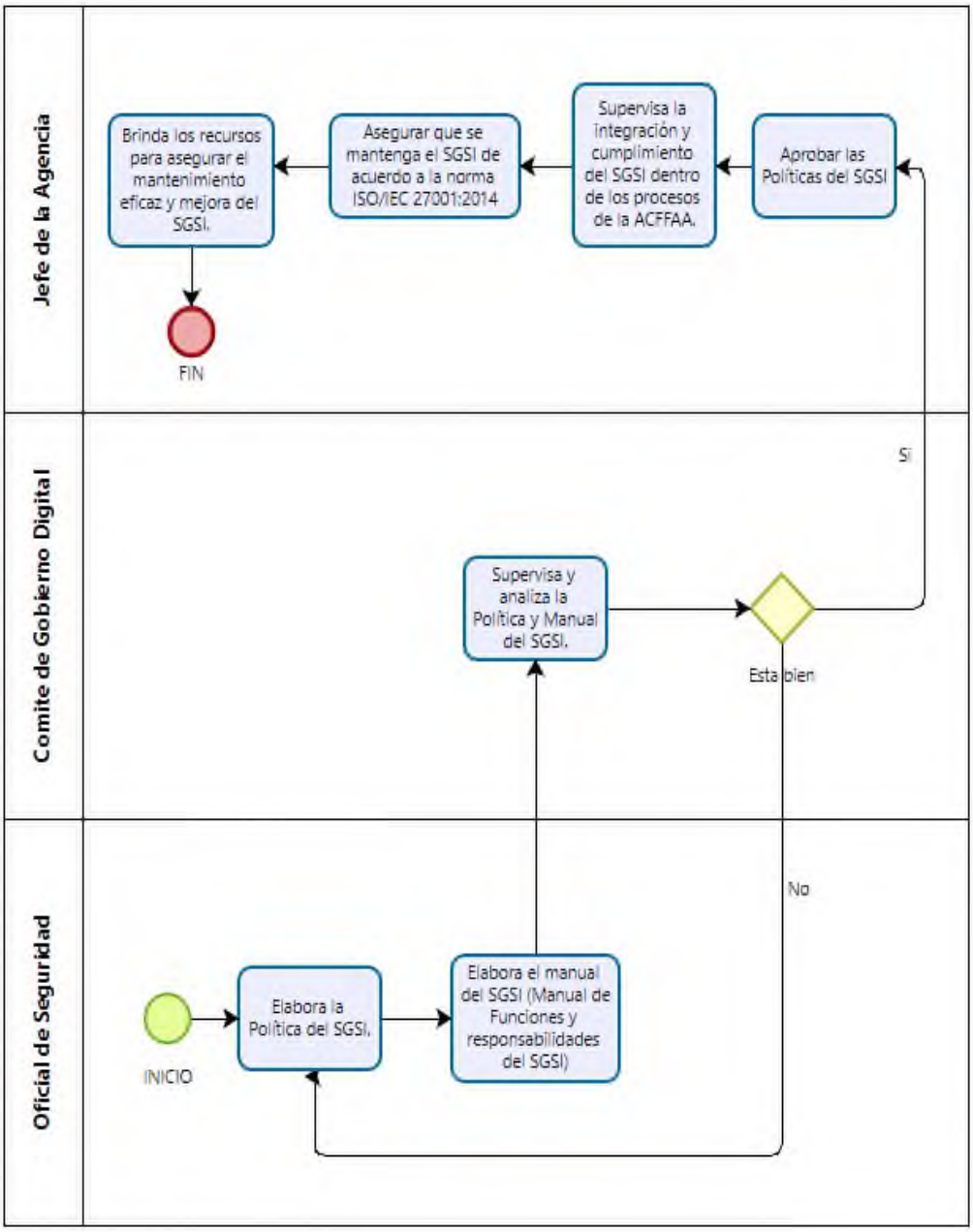


Ilustración 3 Liderazgo.

Fuente Elaboración Propia.

## 5.3 PLANIFICACIÓN

La ACFFAA describe principalmente el establecimiento de los requisitos para medir el riesgo y como alinearlos a los objetivos de la ACFFAA. En la ilustración 4 se detalla las actividades de panificación por cada ente respectivo.

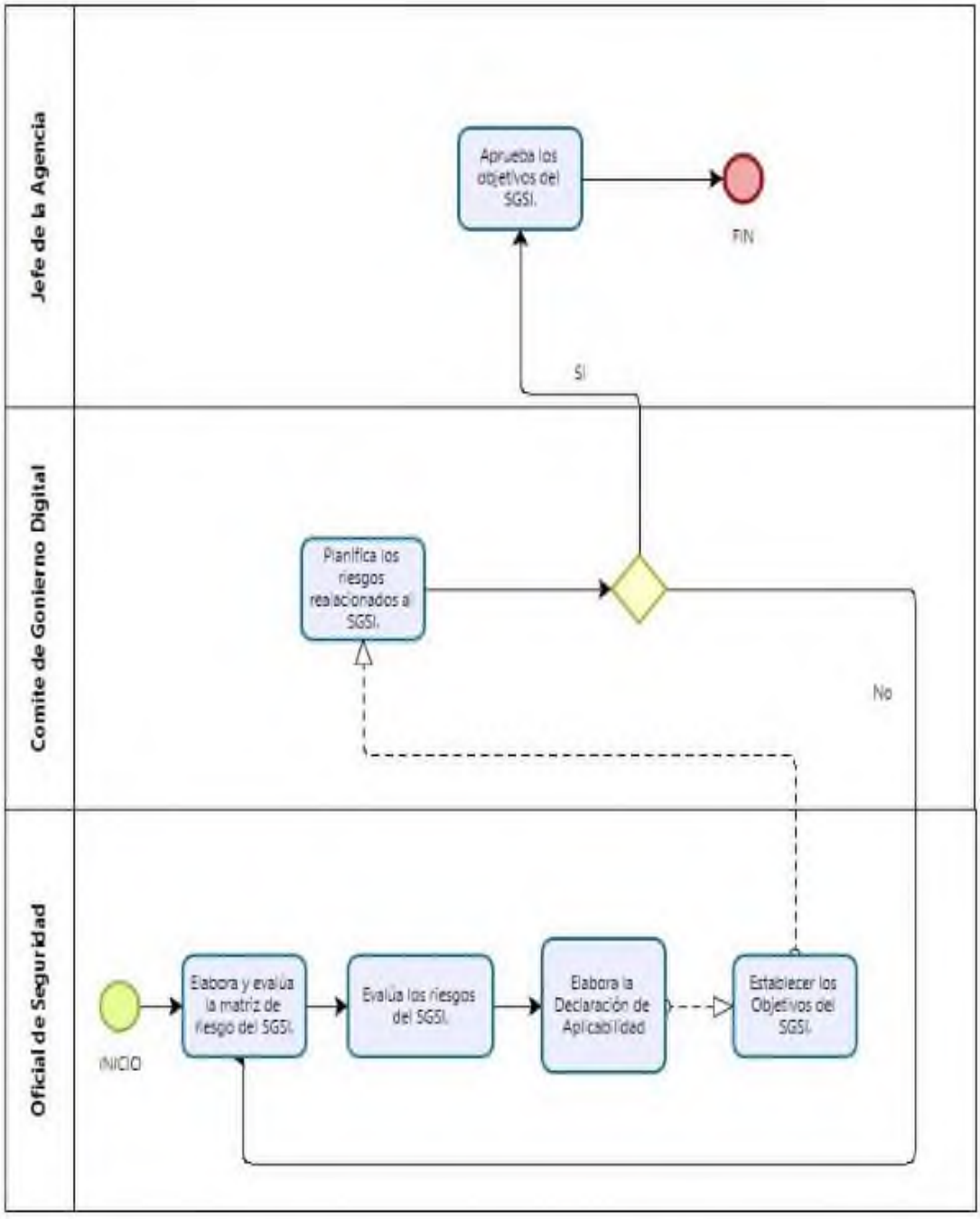


Ilustración 4 Planificación.

Elaboración Propia.

## 5.4 SOPORTE

La ACFFAA propone impartir la comunicación, documentación, los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI. En la ilustración 5 se detallan las actividades correspondientes a Soporte por cada ente respectivo.

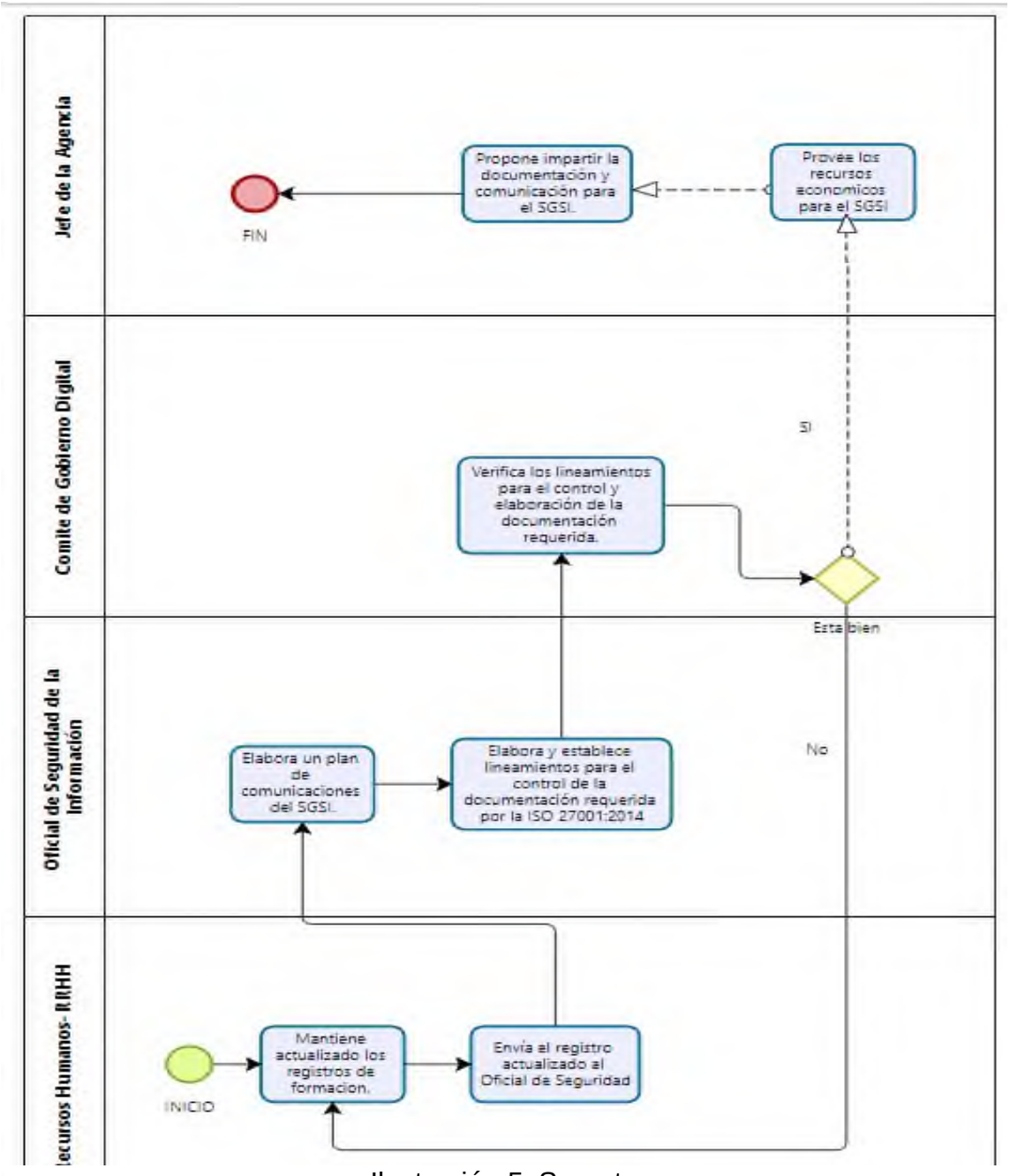


Ilustración 5 Soporte.

Elaboración Propia.

## 5.5 OPERACIÓN

La ACFFAA planificar implementar y controlar los procesos necesarios para cumplir con los requisitos del SGSI. En la ilustración 6 se detalla la planificación y control de parte del ente respectivo.

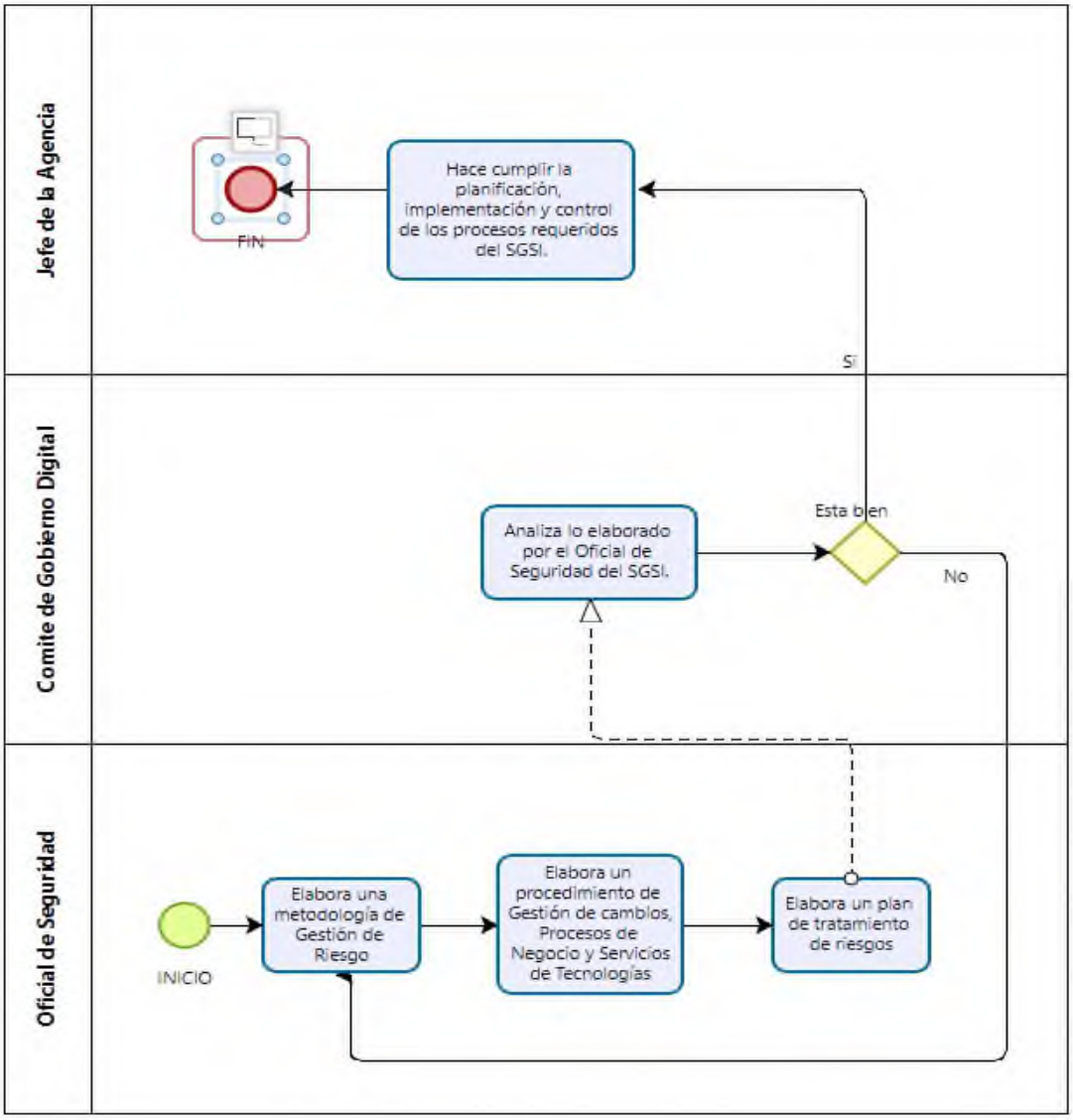


Ilustración 6 Operación.

Elaboración Propia.

## 5.6 EVALUACIÓN DEL DESEMPEÑO

La ACFFAA debe monitorear los procesos que se implementaron y está en funcionamiento continuo, debe ser evaluado constantemente ante posibles incidentes u oportunidades de mejora.

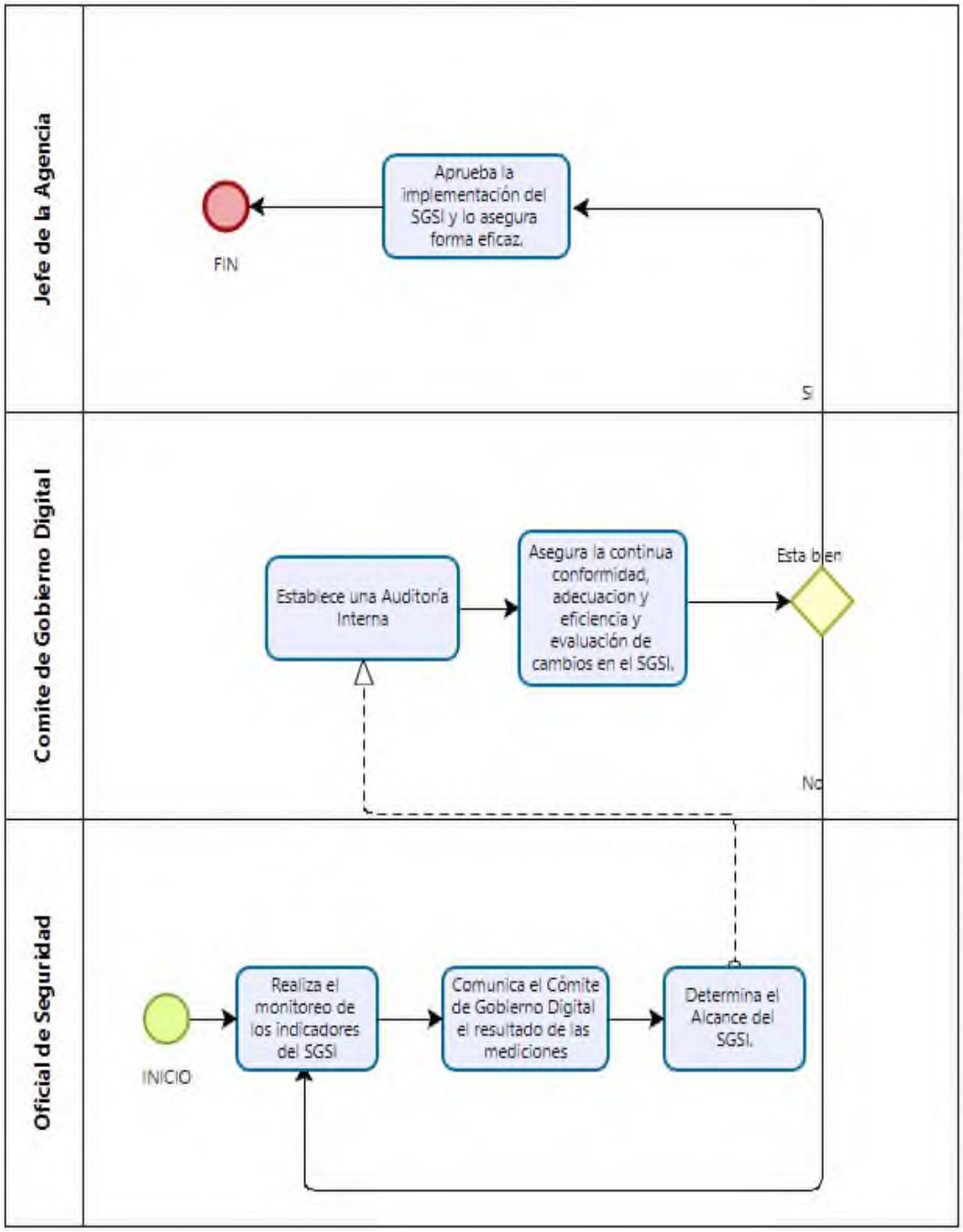


Ilustración 7 Evaluación del Desempeño.

Elaboración Propia.

## 5.7 MEJORA

La ACFFAA debe mejorar continuamente todo lo relacionado a los procesos ya implementado, para corregir y mejorar el SGSI. En la figura 8 se detalla el proceso que debe realizar cada ejecutar con respecto a la mejora continua.

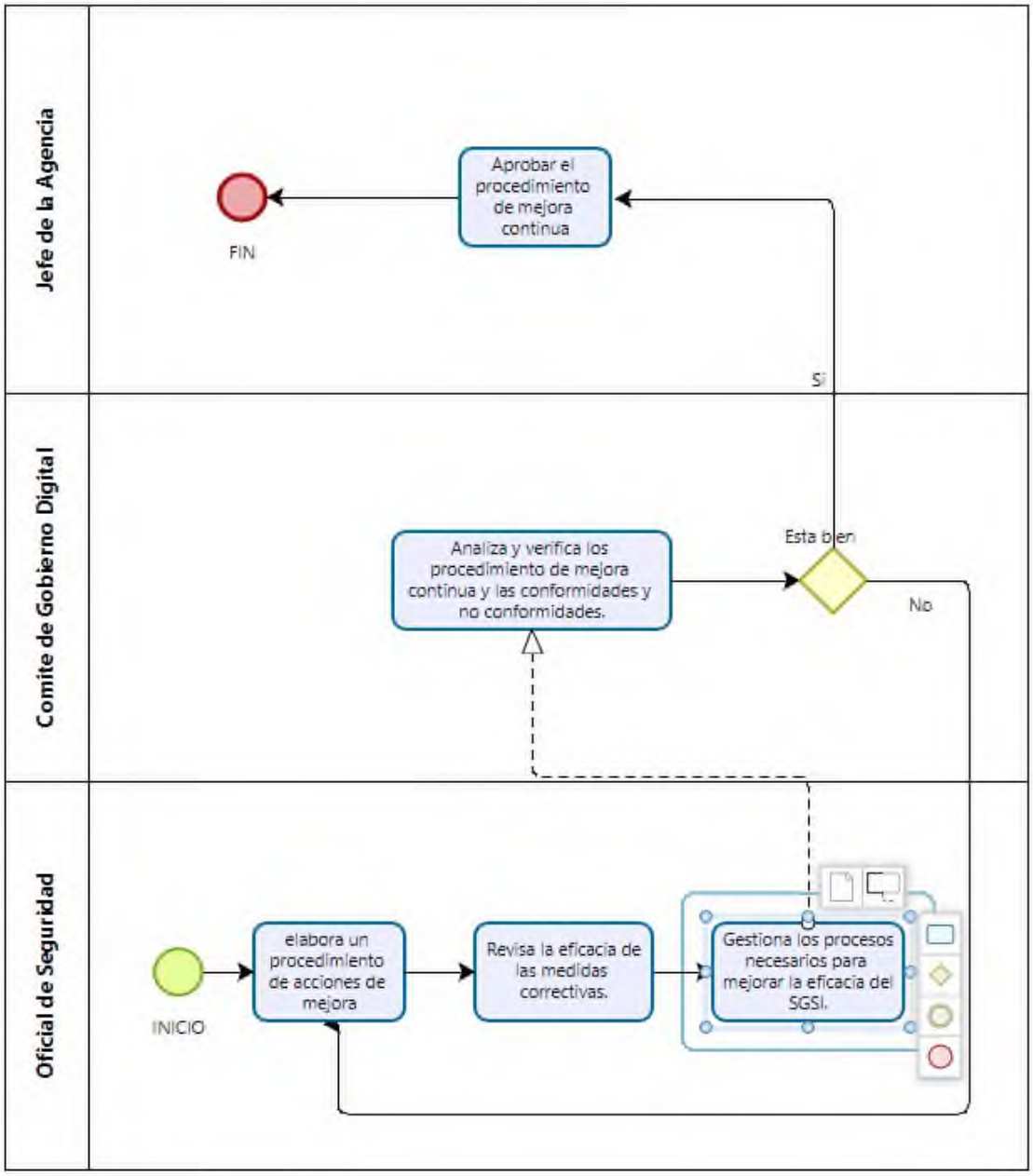


Ilustración 8 Mejora.

Elaboración Propia.

Después de la implementación se realizará:

## VI. Operación para la realización de la Matriz de Riesgos

Establecimiento de un SGSI: La implementación de la norma NTP ISO/27001:2014 implica la creación de un SGSI documentado y estructurado que define roles, responsabilidades y procesos relacionados con la seguridad de la información (Ver Ilustración 14).

**6.1** Identificación y evaluación de riesgos: Se realizan evaluaciones de riesgos para identificar amenazas y vulnerabilidades en la organización. Los controles de seguridad se establecen para mitigar estos riesgos.

**6.2** Políticas y procedimientos de seguridad: Se desarrollan políticas y procedimientos de seguridad de la información que abarcan aspectos como el cifrado, la autenticación, la gestión de contraseñas, la clasificación de datos y la gestión de incidentes de seguridad.

**6.3** Control de acceso y autenticación: Se implementan controles de acceso más estrictos, como autenticación de múltiples factores, contraseñas robustas y auditorías de acceso para garantizar que solo las personas autorizadas tengan acceso a la información crítica.

**6.4** Capacitación y concienciación: Se brinda formación y concienciación en seguridad de la información a los empleados para que sean conscientes de las políticas y procedimientos de seguridad y sepan cómo actuar en caso de incidentes.

Resultado después de la implementación:

- Mejorará de la seguridad de la información: La organización estará mejor preparada para identificar y mitigar los riesgos de seguridad de la información, lo que reduce la probabilidad de incidentes de seguridad.

- Gestión eficiente de incidentes: La organización puede responder de manera efectiva a incidentes de seguridad, minimizando el impacto en caso de un incidente.
- Cumplimiento de regulaciones: La organización cumple con regulaciones y requisitos de seguridad de la información, lo que puede ser fundamental para operar en ciertos sectores o al tratar con socios comerciales.
- Mayor confianza del cliente: La implementación de la NTP ISO/27001:2014 y sus controles demuestran un compromiso con la seguridad de la información, lo que puede aumentar la confianza de los clientes y socios comerciales.

La implementación de la NTP ISO/27001:2014 conlleva una transformación significativa en la forma en que una organización gestiona y protege la seguridad de la información. Los controles establecidos ayudan a reducir los riesgos, mejorar la eficiencia operativa y demostrar el compromiso de la organización con la seguridad de la información.

## 6.5 Identificación de controles según la ISO/IEC 27002:2014

A continuación, se realiza una descripción de las cláusulas de los controles de la ISO 27002:2014 que se van a implementar en la ACFFAA, el desarrollo de las políticas de seguridad tiene la finalidad de proteger la integridad, confidencialidad **y disponibilidad de la información de la ACFFAA.** La tabla 2 muestra los 14 dominios de Seguridad y sus descripciones.

### 6.5.1 DOMINIOS DE SEGURIDAD

| CLAUSULA DE LOS CONTROLES ISO 27002:2014 | DESCRIPCION |
|---|---|
| **A.5 POLITICAS DE SEGURIDAD DE LA INFORMACIÓN** | Se desarrollará diversas políticas de seguridad, con la finalidad de proteger la integridad, confidencialidad y disponibilidad de la información de la ACFFAA, dichas políticas son elaboradas, evaluadas e implementadas por el Comité de Gobierno Digital. |
| **A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION** | La Política Específica PO-SGSO-001 de la Organización de la Seguridad de la Información, permitirá establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la Seguridad de la Información dentro de la ACFFAA.<br><br>Asimismo, dicha política establece los lineamientos para:<br>1.Definir, asignar los roles y segregar las funciones y responsabilidades de la Seguridad de la Información (Ver Tabla 34).<br>2.Mantener contacto con autoridades y grupos de interés para el intercambio de conocimientos relacionados a la Seguridad de la Información.<br>3.El tratamiento de Seguridad de la Información en la Gestión de Proyectos.<br><br>Por otro lado, la política específica PO-SGSO-002 Política Específica de Equipos Móviles, para establecer los controles de seguridad de los dispositivos móviles utilizados en la organización (Ver ilustración 15). |
| **A.7 SEGURIDAD DE LOS RECURSOS HUMANOS** | El desarrollo de esta política específicas PO-SGSI-003 Política Específica de |

| | |
|---|---|
| | Seguridad de los Recursos Humanos asegura que se realice la verificación de antecedentes, establezcan las responsabilidades, capacitación y defina un proceso disciplinario para la seguridad de la información de la ACFFAA. |
| **A.8 GESTIÓN DE ACTIVOS** | El desarrollo de esta política específica PO-SGSI-004 Política Específica de Activos de Información, establece que se identifiquen los activos de información que se encuentran dentro del alcance del SGSI, para lo cual se cuenta con un inventario de los activos de información, en donde se establezcan sus propietarios, ubicaciones, clasificación, entre otra información relevante para el SGSI. Así mismo se haga un buen uso de estos activos y se establezca las medidas de protección. |
| **A.9 CONTROL DE ACCESOS** | La finalidad de la política específica PO-SGSI-005 Política Específica de Gestión de Accesos asegura el acceso autorizado a los sistemas de información y activos de información de la ACFFAA. |
| **A.10 CRIPTOGRAFÍA** | Este dominio tiene como finalidad crear una política específica PO-SGSI-006 Política Específica de Criptografía que permite garantizar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información. |
| **A.11. SEGURIDAD FÍSICA Y AMBIENTAL** | Con respecto a la seguridad física y ambiental, las siguientes políticas específicas:<br>1. **PO-SGSI-007** Política Específica de Seguridad Física y Ambiental<br>2. **PO-SGSI-008** Política Específica de Pantallas y Escritorios Limpios |

| | |
|---|---|
| | buscaran impedir el acceso físico no, autorizado, daño e interferencia a la información, a las instalaciones de procesamiento de la información de la ACFFAA, el daño y/o pérdida de los activos de información y la interrupción de las operaciones de la organización. |
| **A.12.SEGURIDAD DE LAS OPERACIONES** | El objetivo de este dominio es el asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras, mediante la proyección de código malicioso, respaldo de información, registro y monitoreo de eventos, control de software operacional, prevención de vulnerabilidades técnicas y minimizar el impacto de las actividades de auditoria en los sistemas operacionales, por lo que la ACFFAA cuenta con la política específica PO-SGSI-015 Política Específica de Seguridad de las Operaciones y PO-SGSI-016 Política Específica de Respaldo de Información. |
| **A.13. SEGURIDAD DE LAS COMUNICACIONES** | La finalidad de este dominio es dar a conocer los controles que se deben tener en cuenta para asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información, así como en la transmisión de información dentro de la organización y a cualquier entidad externa, por lo que la ACFFAA cuenta con la política específica PO-SGSI-014 Política Específica de Seguridad de las Comunicaciones. |
| **A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** | La finalidad de este dominio es garantizar que la seguridad de la información sea una parte integral de los sistemas de información, mediante el análisis de especificaciones de |

| | |
|---|---|
| | requisitos de seguridad de la información, desarrollo seguro, control de cambios, revisiones, principios de ingeniería, entre otros. Por lo que la ACFFAA cuenta con las políticas específicas PO-SGSI-013 Política Específica de Desarrollo de Software y PO-SGSI-014 Política Específica de Ingeniería de Software. |
| **A.15. RELACIONES CON LOS PROVEEDORES** | La finalidad de este dominio es asegurar la protección a los activos de la organización que son accesibles por los proveedores de la ACFFAA, mediante la definición de requisitos de seguridad de la información que permitan mitigar los riesgos asociados con el acceso por parte del proveedor, monitoreo y revisión de la entrega de servicios y un correcto control sobre su acceso a las instalaciones de la ACFFAA y/o a sus sistemas de información, por lo que la ACFFAA cuenta en la política específica PO-SGSI-009 Política Específica de Relación con Proveedores. |
| **A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | La finalidad de este dominio es el establecer un enfoque consistente y efectivo a la gestión de incidentes de la seguridad de la información, definiendo responsabilidades y procedimientos para una respuesta rápida, efectiva y ordenada, por lo que la ACFFAA cuenta con la política específica PO-SGSI-010 Política Específica de Gestión de Incidentes de Seguridad de la Información. |
| **A.17. SEGURIDAD DE LA INFORMACIÓN EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO** | Este dominio tiene como finalidad garantizar la continuidad operativa de la ACFFAA y preservar la confidencialidad e integridad de los activos de información. Para ello se deben aplicar los controles necesarios para evitar o |

| | |
|---|---|
| | minimizar las posibles interrupciones o fallas de las actividades institucionales que puedan tener impacto, por lo que la ACFFAA cuenta con la política específica PO-SGSI-017 Política Específica de Continuidad. |
| **A.18. CUMPLIMIENTO** | La finalidad de este dominio es evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad de la información, por lo que la ACFFAA debe contar con una política específica PO-SGSI-01 Política Específica de Cumplimiento. |

Tabla 2 Dominios de Seguridad ISO 27001 –

Elaboración Propia

### 6.5.2 POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Las siguientes tablas que se verán en esta sección muestran el desarrollo de las Políticas de Seguridad para, con un código por cada desarrollo.

| | | |
|---|---|---|
| | **POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN** | |
| | **CODIGO:** **PO-SGSI-001** | **Versión:** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | Definir la postura institucional de la Agencia de Compras de las Fuerzas Armadas (ACFFAA), respecto a la seguridad de la información que genera, procesa o almacena, de tal manera que todos los interesados internos y externos | |

| | |
|---|---|
| | conozcan y cumplan las disposiciones de esta.<br><br>Preservar la confidencialidad, integridad y disponibilidad de la información mediante la aplicación de un proceso de gestión del riesgo y garantiza, a las partes interesas, que los riesgos sean administrados adecuadamente. La seguridad de la información se define como la salvaguarda de la información. |
| **ALCANCE:** | El alcance de esta política se aplica al sistema de gestión de seguridad de la información de la ACFFAA, así como a toda persona vinculada laboral o contractualmente con la Agencia de Compras de las Fuerzas Armadas, incluyendo al personal de las Fuerzas Armadas que tienen relación con ella, y en general, a toda persona que usa, administra o accede a los activos de información de los procesos definidos en el alcance del SGSI. |
| **CONTROLES:** | **1.** Políticas de Seguridad de la Información<br>**2.** Revisión de las Políticas de la Seguridad de la Información. |
| **CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:** | |
| 1. La Alta Dirección realizara la aprobación de la Política de Seguridad de la Información, propuesta por el Comité de Gobierno Digital, el cual constituye la declaración escrita de su compromiso con el cumplimiento de los requisitos de seguridad de la información, legales y con la mejora continua del Sistema de Gestión de Seguridad de la Información. Así mismo, éste permite orientar al personal hacia el cumplimiento de los objetivos del SGSI.<br>2. Las políticas deben ser evaluadas e implementadas por el Comité de Gobierno Digital. | |

Tabla 3 Política de la Seguridad de la Información – ISO 27001 – Fuente. Elaboración Propia.

| | | |
|---|---|---|
| | **POLÍTICA DE ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | |
| | **CODIGO:** **PO-SGSI-002** | **Versión:** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | Establecer un marco de gestión para iniciar y controlar la implementación y operación de seguridad de la información dentro de la Agencia de Compras de las Fuerzas Armadas (ACFFAA). | |
| **ALCANCE:** | El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA. | |
| **CONTROLES:** | 3. Roles y responsabilidades para la seguridad de la información<br>4. Segregación de funciones<br>5. Contacto con autoridades<br>6. Contacto con grupos especiales de interés<br>**7.** Seguridad de la información en la gestión de proyectos. | |

**CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:**

8. Se establecerán roles y funciones de seguridad de la información en la ACFFAA.
9. Se segregarán funciones y áreas de responsabilidad para reducir las oportunidades de mal uso de los activos de la ACFFAA.
10. Para intercambiar conocimientos y obtener asesoramiento para la optimización de las prácticas y controles de seguridad de la información, se mantendrán contactos apropiados con autoridades y grupos de interés.
11. La ACFFAA debe integrar la seguridad de la información en el método de gestión de proyectos, para garantizar que los riesgos de seguridad de la información son identificados y tratados independientemente al tipo

| |
|---|
| de proyecto, los proyectos se registraran por el Oficial de Seguridad en una lista de proyectos.<br>12. LA ACFFAA establecerá una Política Específica de Dispositivos Móviles, en donde se establecen las medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.<br>13. LA ACFFAA establecerá una Política Específica de Teletrabajo, en donde se establecen medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de los equipos informáticos (Ver ilustración 16). |

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 4 Política de la Organización de la Seguridad de la Información - ISO 27001.

Elaboración Propia.

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE SEGURIDAD DE LOS RECURSOS HUMANOS** | |
| | **CODIGO:**<br>**PO-SGSI-002** | **Versión:**<br>**001** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | 1. Asegurar que el personal de la Agencia de Compras de las Fuerzas Armadas (ACFFAA) conozcan sus responsabilidades que conllevan al cumplimiento del Sistema de Gestión de Seguridad de la Información Implementado.<br>2. Proteger la confidencialidad, integridad y disponibilidad de los activos de información de la ACFFAA, en el proceso de desvinculación del personal de la ACFFAA. | |

| | |
|---|---|
| **ALCANCE:** | 1. El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores de la ACFFAA. |
| **CONTROLES:** | 2. Selección<br>3. Términos y condiciones del empleo<br>4. Responsabilidades de la Dirección<br>5. Concientización, educación y formación en seguridad de la información<br>6. Proceso disciplinario<br>7. Finalización o cambio de responsabilidades laborales |

**CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:**

8. El proceso de contratación de la ACFFAA, se realiza de acuerdo con la Directiva de Contratación de Personal aprobadas y procedimientos asociados, incluyendo el personal que se encuentra bajo la modalidad de formación de servicios.
9. Las directivas y/o procedimientos utilizados por la ACFFAA para la contratación de personal deberá incluir la verificación de la veracidad de los documentos presentados por los servidores y la validación de antecedentes policiales, judiciales y/o penales.
10. Los reglamentos internos que establezcan y regulen la normatividad a la que deben sujetarse los servidores de la ACFFAA, se deberá indicar las responsabilidades del personal de la ACFFAA, respecto a la seguridad de la información.
11. Los servidores de la ACFFAA, deberán suscribir un formato el Acuerdo de Confidencialidad para servidores, al inicio de su vínculo laboral, el cual deberá ser almacenado en su legajo personal.
12. El Jefe de la ACFFAA debe asegurar que los servidores de la ACFFAA, cumplan con las políticas y los procedimientos establecidos por la ACFFAA.
13. Los servidores de la ACFFAA deben ser capacitados en temas relacionados a la Seguridad de la Información.
14. El Oficial de Seguridad de la Información utilizará un formato de control para el Plan de capacitación del SGSI, para programar las capacitaciones de los servidores de la ACFFAA, el cual deberá ser aprobado por el Comité de Gobierno Digital.
15. Se cuenta con un proceso disciplinario formal y comunicado en el RIS (Reglamento Interno de los Servidores Civiles) para adoptar medidas aplicables al personal que ha cometido una falta a la seguridad, este proceso disciplinario debe también usarse como disuasivo para prevenir que el personal falte a las políticas y procedimientos de seguridad de la información de la ACFFAA.
16. La desvinculación del personal de la ACFFAA se realiza de acuerdo con las disposiciones establecidas en la Directiva de Desvinculación de Personal en la Agencia de Compras de las

| | |
|---|---|
| | Fuerzas Armadas. |
| 17. | Los derechos de accesos o permisos a los Sistemas y/o servicios Informáticos de la ACFFAA, deben ser removidos o modificados al producirse el término de la relación laboral o contrato. |
| 18. | El área de Recursos Humanos, mediante el Sistema de Mesa de Ayuda, genera un ticket solicitando la actualización o eliminación de las cuentas de usuarios, a fin de mantener actualizado los accesos a los sistemas de información y servicios informáticos (Ver Ilustración 9). |

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 5 Política Específica de Seguridad de los Recursos Humanos

Elaboración Propia

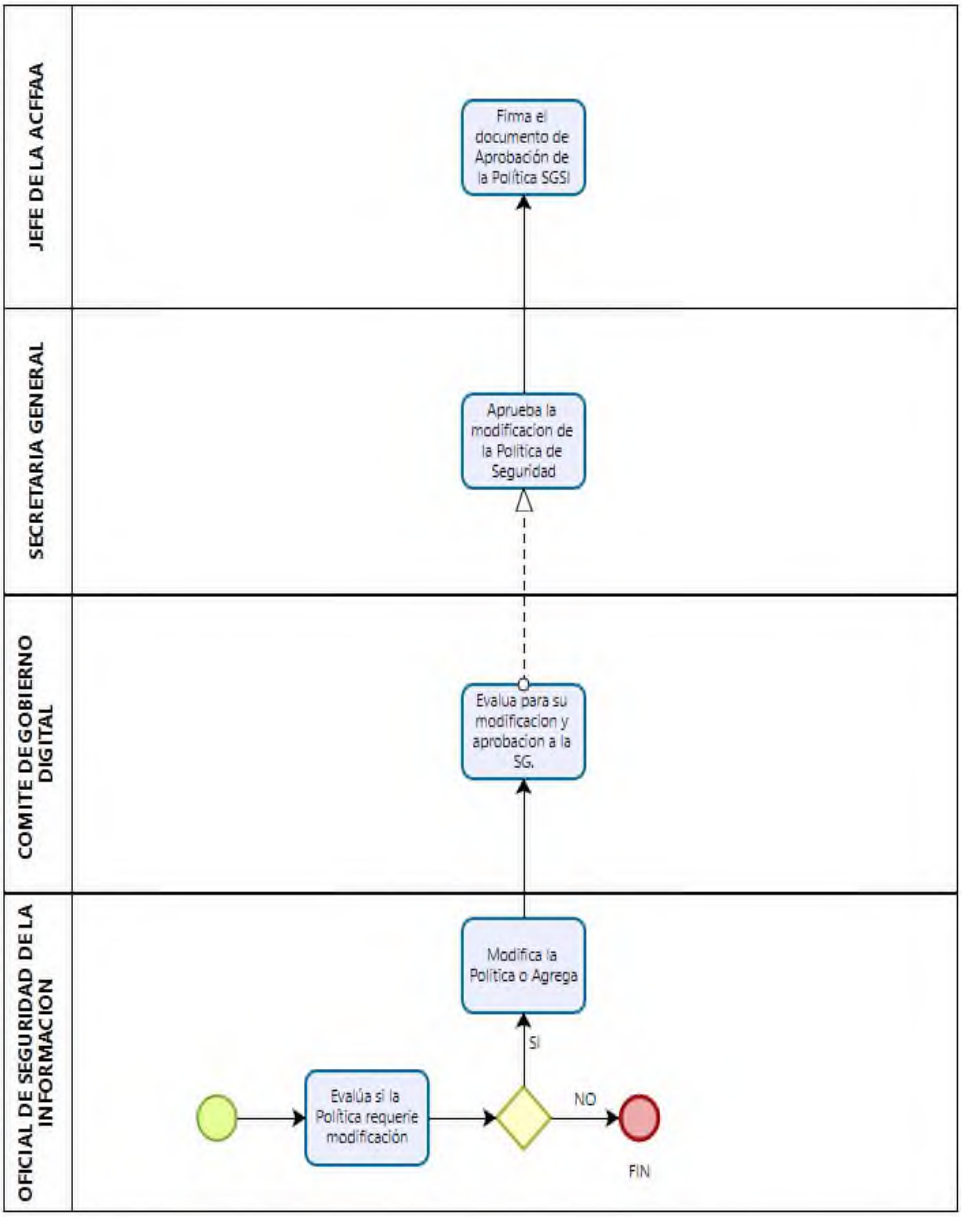


Ilustración 9 Diagrama de Flujo de Política Específica de los Recursos Humanos.

Elaboración Propia.

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE ACTIVOS DE INFORMACIÓN** | |
| | | |
| | **CODIGO:** **PO-SGSI-003** | **Versión:** 001 |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | 1. Identificar en forma correcta los activos de información y mantener un inventario de estos.<br>2. Proveer un nivel de protección adecuado a los activos de información. | |
| **ALCANCE:** | 3. El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA. | |
| **CONTROLES:** | 4. Inventarios de activos<br>5. Propiedad de los activos.<br>6. Uso aceptable de los activos<br>7. Retorno de activos | |

**CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:**

8. Se debe tener identificados los activos de información en un formato de Inventario de Activos de Información asociados a los procesos, sus propietarios y ubicación.
9. Se deberá realizar la actualización de los activos de información cada año o ante la necesidad de la entidad.
10. El uso de los activos de información debe ser para propósitos de las actividades de la organización de acuerdo con las políticas y procedimientos que se definan y considerando criterios de buen uso.
11. No se debe divulgar información que haya sido clasificada como “Confidencial” o de “Uso Interno”, a menos que la normatividad vigente lo permita.

12. Los envíos de información con clasificación Confidencial vía correo electrónico y/o medios extraíbles (USB, cd, etc.) se encuentran prohibidos.
13. De corresponder, el propietario de la Información, será el que autorice a terceros (consultorías, prestaciones de servicios, entre otros) el acceso a los activos de información clasificados como “Confidencial” o de “Uso Interno”, previa suscripción del acuerdo de confidencialidad correspondiente.
14. Se deben cumplir con los requisitos legales, contractuales y normativos relativos al uso de activos de información, incluyendo las políticas de seguridad que deben mantenerse alineadas con las leyes vigentes.
15. Se deben gestionar adecuadamente los elementos de control de acceso, como contraseñas (control lógico) así como llaves de cerradura (control físico).
16. El personal que ponga en riesgo los activos de información, se le aplicará medidas disciplinarias de acuerdo con el Reglamento Interno de los Servidores Civiles. Esta sanción estará sujeta a la gravedad del incidente ocasionado y conforme a las normas establecidas.
17. Der corresponder, el personal debe devolver los activos en su poder al término de su vínculo laboral.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 6 Política Específica de Seguridad de la Información.

Elaboración Propia.

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE GESTIÓN DE ACCESOS** | |
| | **CODIGO:** **PO-SGSI-004** | **Versión:** 001 |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | 18. Controlar los accesos a la información de la ACFFAA.<br>19. Prevenir accesos no autorizados a los sistemas de información. | |
| **ALCANCE:** | 20. El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA. | |
| **CONTROLES:** | 21. Requerimientos para el Control de Accesos<br>22. Acceso a redes y servicio de red<br>23. Registro y baja de usuarios<br>24. Aprovisionamiento de acceso a usuario<br>25. Gestión de derechos de acceso a privilegios<br>26. Gestión de información de autenticación secreta de usuarios<br>27. Revisión de derechos de acceso a usuarios<br>28. Remoción o ajuste de derechos de acceso<br>29. Uso de información de autenticación secreta<br>30. Restricción de acceso a la información<br>31. Procedimientos de ingreso seguro<br>32. Sistema de gestión de contraseñas<br>33. Uso de programas utilitarios privilegiados<br>34. Control de acceso al código fuente de los programas. | |
| **CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:** | | |
| **Requerimientos para el Control de Accesos**<br>35. Todos los accesos a los activos de información tanto lógicos como físicos deben basarse en la necesidad y rol del usuario. Se | | |

deberá tomar en cuenta los siguientes aspectos:

36. Los requerimientos de seguridad de cada una de las aplicaciones.
37. Identificación de toda la información relacionada a las aplicaciones y los riesgos a la que está expuesta.
38. Coherencia entre las políticas de control de accesos y las políticas de gestión de activos de información.
39. Uso de perfiles de usuarios estandarizados definidos según roles.
40. Revisión periódica de los controles de acceso.
41. Revocación de los derechos de acceso.
42. El personal de la organización solo debe tener acceso a redes y servicios a los que fueron específicamente autorizados a utilizar.
43. Todo el personal que requiera acceder a la red y servicios de red debe contar con las autorizaciones respectivas de los propietarios de los activos.
44. El acceso a los recursos de red debe ser controlado, de manera que el personal no comprometa la seguridad de los activos de información.

**Lineamiento de Contraseñas seguras**

Todas las contraseñas a los recursos de red deben de considerar lo siguiente:

45. Debe renovarse en un periodo de menor de 03 meses.
46. No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos
47. Tener una longitud mínima de seis caracteres
48. Incluir caracteres de tres de las siguientes categorías
49. Mayúsculas (de la A-Z)
50. Minúsculas (de la A-Z)
51. Dígitos de base 10 (del 0 al 9)
52. Caracteres no alfanuméricos (por ejemplo: *, $, #, %)

Ejemplo:

| Cómo podría ser | Cómo no debería ser |
|---|---|
| Agencia*123 | agencia123 |

1. En caso de ingresar erróneamente la contraseña en un total de 03 ocasiones, la cuenta será bloqueada por un periodo no menor de 15 minutos.

**Gestión de Acceso del Personal**

**Registro y baja de usuarios**

2. El área de Recursos Humanos (RR. HH) de la Oficina General de Administración es la encargada de solicitar el alta y/o baja de usuarios del personal de la ACFFAA, a través de un ticket de atención en el Sistema de Mesa de Ayuda a la Oficina de Informática, para el caso de creación de usuarios de terceros, el área de logística deberá solicitarlo mediante correo institucional al área de Recursos Humanos. Para lo cual la Oficina de Informática cuenta con el procedimiento PRO-SGSI-002 Gestión de Accesos.

**Gestión de acceso a los usuarios**

1. Se cuenta con el formato FOR-SGSI-13 Bitácora de Usuarios, en donde se mantiene un registro de todos los derechos de acceso otorgados a un determinado usuario sobre los sistemas o servicios de red.
2. El área de Recursos Humanos deberá informar a la Oficina de Informática, mediante el un ticket de atención del Sistema de Mesa de Ayuda, todo movimiento del personal de la ACFFAA tales como rotación, modificación/asignación de funciones, etc. Con la finalidad de actualizar y/o desactivar los accesos asignados, según corresponda.

**Gestión de derechos de acceso privilegiados**

3. Debe restringirse y controlarse la asignación y uso de los derechos de acceso privilegiados.
4. Para otorgar permisos de lectura y escritura de medios extraíbles y otros accesos no contemplados en la Bitácora de Usuarios, el Jefe inmediato deberá solicitar la autorización al Secretario General mediante correo institucional, posterior a ello se deberá generar un ticket de atención en el Sistema de mesa de ayuda, adjuntando la autorización y los datos del usuario.

5. Se identifica los derechos de acceso privilegiado asociados a cada sistema o proceso, así como los usuarios a los que se les está otorgando el acceso. Esta información se encuentra en el formato FOR-SGSI-13 Bitácora de Usuarios – Sección Usuarios Privilegiados.
6. Deben asignarse privilegios de acceso alineados a la política de control de acceso basados como requisito mínimo para sus roles y funciones.
7. Debe definirse la temporalidad de los accesos privilegiados otorgados.

**Gestión de la información de autenticación secreta de los usuarios**

8. Debe controlarse toda asignación de autenticación secreta con un proceso formal.
9. Debe verificarse la identidad del usuario antes de proporcionarle la información de autenticación temporal.
10. La entrega de la autenticación temporal debe hacerse en forma segura y única para cada individuo, para lo cual el usuario deberá registrar su conformidad a la recepción de la clave temporal, mediante el Sistema de Mesa de Ayuda.

**Revisión de los derechos de acceso de usuario**

1. La revisión de los accesos de los usuarios debe ser trimestral, la cual estará a cargo de la Oficina de Informática en coordinación con el área de Recursos Humanos.

**Eliminación o ajuste de los derechos de acceso**

1. Para la baja y cambios de los accesos, se cuenta con el procedimiento PRO-SGSI-007 Gestión de Usuarios.
2. Los derechos de acceso de todo el personal a información e instalaciones de procesamiento de información deben ser eliminadas como del fin del vínculo laboral, contrato o acuerdo o ser ajustado ante cambios.

**Responsabilidades del Personal**

3. Todo el personal es responsable de la confidencialidad de la contraseña asignada, y de las consecuencias por las acciones que terceras personas puedan hacer con el uso de esta.
4. Está prohibido compartir las contraseñas asignadas.
5. El personal debe de bloquear su estación de trabajo si por algún motivo se retira de su puesto de trabajo.

**Control de Acceso al Sistema y a las Aplicaciones**

6. El acceso a la información y a las funciones del sistema debe tener controles de seguridad (por ejemplo, usuario y contraseña), a fin de evitar accesos no autorizados a recursos o información, así mismo los derechos de acceso ya sea de lectura, escritura, borrar y ejecutar deben ser controlados, también los datos y aplicaciones que son accedidos por el usuario.
7. Dentro de los aspectos que deben ser tomados en consideración para definir los controles, se incluyen:
8. Procedimiento de inicio de sesión seguros.
9. Identificación y autenticación de usuarios.
10. Restricción del uso de herramientas utilitarias del sistema operativo con capacidades de eludir y/o sobrescribir los controles de seguridad.

**Uso de programas utilitarios privilegiados**

11. El uso de programas utilitarios está restringido y se limita el uso solo para usuarios autorizados y debe ser también controlado.
12. Todo programa utilitario debe pasar por un proceso de identificación, autenticación y autorización de uso, así como su registro, definición y documentación.
13. Todo programa innecesario debe ser desactivado, eliminado.

**Control de acceso al código fuente del programa**

14. El acceso al código fuente de los programas sólo es accesible por los desarrolladores y Jefe de la Oficina de Informática.
15. El código fuente de programas y sus componentes deben ser gestionados por procedimientos establecidos.
16. Los códigos fuentes de programas deben ser almacenado en un repositorio único, ubicado en un servidor distinto a los que fueron desplegados.
17. os códigos fuentes de los programas deben encontrarse sujetos a un procedimiento control de cambios.

**Usuarios de la ACFFAA**

18. Se debe de establecer los lineamientos de control de accesos a la información y a las aplicaciones, restringiendo el acceso únicamente para el personal debidamente autorizado.

| |
|---|
| 19. Se deben identificar los sistemas con información sensible asignándoles un entorno de procesamiento, creado a partir de métodos físicos o lógicos (por ejemplo, el uso combinado de cuentas de usuarios, de contraseñas y/o token).<br>20. Todas las cuentas de usuarios son gestionadas por la Oficina de Informática. |

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 7 Política Específica de Gestión de Accesos –

Elaboración Propia

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE CRIPTOGRAFIA** | |
| | **CODIGO:**<br>**PO-SGSI-005** | **Versión:**<br>**001** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | 1. Proteger la información que es procesada en las aplicaciones y trasmitida en las redes. | |
| **ALCANCE:** | El alcance de esta política abarca a las aplicaciones web de la institución publicadas en el internet. | |
| **CONTROLES:** | 2. Política sobre el uso de controles criptográficos.<br>3. Gestión de claves. | |
| **CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:** | | |
| **Criptografía**<br>**Controles Criptográficos**<br>4. El dominio acffaa.gob.pe en la actualidad trabaja con certificados digitales, los cuales son utilizados para el acceso a sus diferentes aplicaciones web publicadas en el internet. El certificado digital es un mecanismo que permite autenticar un sitio web en internet | | |

de manera que se conserve protegida la información de la organización y sus clientes.

5. Con la finalidad de establecer un control sobre los certificados digitales vigentes se detalla la verificación de dichos certificados digitales:
6. Se solicita la información sobre los certificados actuales y los que se van a implementar, verificamos uno a uno.

**Si es un certificado nuevo:**

1. Se verifica los requerimientos técnicos del certificado digital, como tipo de cifrados (1024, 2048 bits), vigencia, etc.
2. Se realiza el Pedido y la compra del nuevo certificado a la empresa elegida según las cotizaciones.
3. Se implementa el certificado en el aplicativo y dirección URL respectiva.
4. Se valida el funcionamiento del certificado, realizando las pruebas en la página respectiva, por lo que se emite un informe hacia el Jefe de la Oficina de Informática, sobre el funcionamiento de los certificados instalados como nuevos y la situación de los que ya se encuentran instalados.

**Si no es un certificado nuevo:**

1. Se verifica la vigencia del certificado de acuerdo con la información solicitada.
2. Si la vigencia es menor de 2 meses se solicita la renovación del certificado.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 8 Política Específica de Criptografía - ISO 27001-

Elaboración Propia

<table>
<tr><td></td><td colspan="2">POLÍTICA ESPECÍFICA DE SEGURIDAD FISICA Y AMBIENTAL</td></tr>
<tr><td rowspan="2"></td><td>CODIGO:<br>PO-SGSI-006</td><td>Versión:<br>001</td></tr>
<tr><td></td><td>Fecha de Aprobación:</td></tr>
<tr><td>OBJETIVO:</td><td colspan="2">1. Evitar accesos no autorizados, daños e interferencias contra las instalaciones y la información de la ACFFAA.<br>2. Evitar pérdidas y/o daños a los activos de información, así como la interrupción de las actividades en la ACFFAA.</td></tr>
<tr><td>ALCANCE:</td><td colspan="2">El alcance de la presente política abarca a las instalaciones y equipos que se encuentran dentro del alcance del SGSI. Esta política debe de ser conocida y cumplida por todo el personal que laboren o tengan relación con la ACFFAA.</td></tr>
<tr><td>CONTROLES:</td><td colspan="2">3. Perímetro de seguridad física<br>4. Controles de acceso físico<br>5. Seguridad en oficinas, despachos e instalaciones<br>6. Protección contra amenazas externas y del ambiente<br>7. Trabajo en las áreas seguras<br>8. Ubicación y protección del equipamiento<br>9. Servicios/Instalaciones de apoyo<br>10. Seguridad en el cableado<br>11. Mantenimiento de equipos<br>12. Retiro de activos de información de propiedad de la ACFFAA y Seguridad de equipos fuera del local<br>13. Disposición o reutilización segura de equipos<br>14. Equipo desatendido por el usuario y Pantalla y escritorios limpios</td></tr>
</table>

**CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:**

**Perímetro de seguridad física**

Los criterios para determinar un área segura son los detallados a continuación:

1. Dónde se procesa información relacionado al estudio de mercado y proceso de contratación.
2. Dónde se almacena información relacionada al proceso de contratación
3. Dónde se cuenta con información confidencial

La relación de las áreas seguras se encuentra en el formato FOR-SGSI-017 Lista de Áreas Seguras.

1. El perímetro de seguridad física debe estar claramente definido.
2. Se debe proteger las áreas donde funcionan las instalaciones de procesamiento de información que pudiesen afectar el funcionamiento de los sistemas de información.

**Controles de acceso físico**

1. En los accesos a la ACFFAA se deberá contar con controles que aseguren el acceso físico sólo al personal debidamente autorizado. Para lo cual se debe contar con la Directiva de Normas para el control de Ingreso y desplazamiento de servidores, visitas y proveedores en la Agencia De Compras de las Fuerzas Armadas.

**Seguridad en oficinas, despachos e instalaciones**

2. Deben existir controles de seguridad física, los cuales se deben mencionar en un formato de Lista de Áreas Seguras.
3. Los servidores de la ACFFAA no deben facilitar el acceso a las instalaciones a personas desconocidas.
4. Las áreas dedicadas al procesamiento de información identificados en un formato de Lista de Áreas Seguras, deben ser ubicadas en un lugar que no presente riesgos desde el punto de vista de acceso al público.

**Protección contra amenazas externas y del ambiente**

1. Los equipos de procesamiento de información y/o activos de información utilizados o almacenados en las áreas seguras se encuentran ubicados y protegidos de tal forma que se reducen los

riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.

**Trabajo en las áreas seguras**

2. Las actividades realizadas en las áreas identificadas como seguras, se registrarán en un formato de Lista de Áreas Seguras y deben ser supervisadas.

**Ubicación y protección del equipamiento**

3. Los equipos deben estar ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.

**Servicios/Instalaciones de apoyo**

4. Se debe contar con un sistema que brinde soporte a los equipos electrónicos, a fin de asegurar la continuidad de las operaciones, mientras se restablece el suministro de energía eléctrica.
5. Los servicios de soporte se deben inspeccionar una vez al año, para asegurar su correcto funcionamiento.

**Seguridad en el cableado**

6. El cableado de energía o de telecomunicaciones se encuentra protegido de cualquier intercepción o daño.
7. El cableado de suministro de energía eléctrica y telecomunicaciones en las zonas de tratamiento de información debe contar con un sistema de puesta a tierra (pozo a tierra), el que debe ser revisado anualmente para garantizar su adecuado funcionamiento.

**Mantenimiento de equipos**

1. El mantenimiento de los equipos se realizará bajo procedimiento establecido de Mantenimiento de Equipos.

**Retiro de activos de información de propiedad de la ACFFAA y Seguridad de equipos fuera del local**

2. Se encuentran prohibido la salida de activos de información fuera de las instalaciones de la ACFFAA, sin embargo, excepcionalmente el Secretario General de la ACFFAA podrá emitir autorizaciones para la salida de dichos

activos, siempre que dicha acción conlleve a la correcta ejecución de las funciones a cargo de la ACFFAA.

3. Los equipos de procesamiento de información (PC, Laptops, Discos externos, etc.) que son propiedad de la ACFFAA deben contar con la autorización del área de Control Patrimonial para su retiro de las instalaciones de la ACFFAA, para tal fin se utilizará una Guía de Desplazamiento Interno y/o Externo de Bienes Patrimoniales.

**Disposición o reutilización segura de equipos**

4. Se deben de verificar todos los equipos para asegurar que cualquier dato sensible se haya eliminado antes de su reutilización o cuando se disponga a eliminarse, lo cual se debe realizar un procedimiento de Borrado y Eliminación Seguro.

**Equipo desatendido por el usuario y Pantalla y escritorios limpios**

5. Se debe contar con una Política específica de pantallas y escritorios limpios**,** en donde se dan los lineamientos para la protección de la información.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 9 Política Específica de Seguridad Física y Ambiental ISO 27001 – Elaboración Propia

<table>
<tr><td rowspan="3"></td><td colspan="2">POLÍTICA ESPECÍFICA DE SEGURIDAD DE LAS OPERACIONES</td></tr>
<tr><td>CODIGO:<br>PO-SGSI-007</td><td>Versión:<br>001</td></tr>
<tr><td>Fecha de Aprobación:</td></tr>
<tr><td>OBJETIVO:</td><td colspan="2">Establecer un marco de gestión para asegurar la correcta operación y proteger las instalaciones de procesamiento de información de la Agencia de Compras de las Fuerzas Armadas (ACFFAA).</td></tr>
<tr><td>ALCANCE:</td><td colspan="2">El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA.</td></tr>
<tr><td>CONTROLES:</td><td colspan="2">1.<br>2. Procedimientos documentados de operación<br>3. Gestión de Cambios<br>4. Gestión de la Capacidad<br>5. Separación de los ambientes para Desarrollo, Pruebas y Producción<br>6. Protección Ante Código Malicioso<br>7. Respaldo<br>8. Respaldo de la información<br>9. Registros y seguimiento<br>10. Registro de eventos<br>11. Protección de la información de registros (Logs)<br>12. Sincronización de relojes<br>13. Control de software en producción<br>14. Instalación de software en los sistemas operativos.<br>15. Gestión de vulnerabilidad técnicas<br>16. Gestión de vulnerabilidades técnicas<br>17. Restricciones en la instalación de software por los usuarios<br>18. Consideraciones sobre la auditoría de sistemas de información<br>19. Controles de auditoría de sistemas de información</td></tr>
<tr><td colspan="3">CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:</td></tr>
<tr><td colspan="3">Procedimientos documentados de operación</td></tr>
</table>

20. La Oficina de Planeamiento y Presupuesto, registra los lineamientos, directivas, procedimientos, manuales, entre otros documentos que regulan las operaciones de la ACFFAA, haciendo uso de un formato para la Lista Maestra de Documentos Internos.

21. Adicionalmente, la Oficina de Informática se encargará de registrar la documentación de los Sistemas de Información que administra tales como manuales, guías, entre otros que describan el funcionamiento y/o usabilidad de estos, para tal fin se utiliza formato FOR-SGSI-044 Documentación de los Sistemas de Información.

22. La documentación relacionada la operatividad de entidad, deben ponerse a disposición de los servidores de la ACFFAA.

**Gestión de Cambios**

23. Los cambios en la organización, procesos de negocio y servicios de tecnología de la información que afecten la seguridad de la información, serán realizados de acuerdo con el procedimiento PRO-SGSI-009 Gestión de Cambios Organizacionales, Procesos de Negocio y Servicios de Tecnología de la Información.

24. Las implementaciones y/o cambios de servicio de Tecnología de la Información, que comprometan la continuidad de las operaciones de la ACFFAA, deberán realizarse fuera del horario de trabajo.

**Gestión de la Capacidad**

25. La Oficina de Informática es la encargada de la gestión de los servidores físicos y lógicos de la ACFFAA.

26. La Oficina de Informática debe gestionar la proyección de la capacidad de sus servidores administrados y su afinamiento, con la finalidad de evitar la interrupción en los servicios de TI, dicha proyección se realiza en el FOR-SGSI-052 Registro de Capacidad de Servidores u otras herramientas informáticas implementadas.

27. La Oficina de Informática empleará el uso de herramientas informática para el monitoreo a tiempo real de los estados de los servidores.

28. Como parte del afinamiento de los servidores, se deben realizar actividades de depuración de datos obsoletos en los servidores (Log, aplicaciones,

instaladores, etc.) y otras que permitan optimizar la performance de los servidores, dichas actividades se registran en el FOR-SGSI-052 Registro de Capacidad de Servidores u otras herramientas informáticas implementadas.

**Separación de los ambientes para Desarrollo, Pruebas y Producción**

29. Los ambientes para desarrollo, pruebas y producción, se despliegan de la siguiente forma:

| Producción | Pruebas | Desarrollo |
|---|---|---|
| Segmento de red:<br>Red LAN – DMZ | Segmento de red:<br>Red de pruebas | Segmento de red:<br>Red de Desarrollo |

30. Los ambientes de desarrollo, pruebas y producción se encuentran con un nivel de separación necesario para prevenir problemas operacionales, así como los controles de acceso adecuados para cada uno de ellos.

El acceso a los ambientes de desarrollo, pruebas y producción se encuentran únicamente habilitados para el personal autorizado por la Oficina de Informática de la ACFFAA.

La Oficina de Informática es responsable de la administración, mantenimiento, operatividad continua, seguridad y rendimiento aceptable de los ambientes de desarrollo, pruebas y producción.

Las pruebas deben realizarse utilizando datos de prueba. En los casos en los que no se pueda recrear los datos de prueba y la entidad así lo requiera, la copia de datos de producción puede ser usada para las pruebas, siempre y cuando el uso de esta información sea autorizado.

**Protección Ante Código Malicioso**

1. La Oficina de Informática es responsable de la implementación del sistema de antivirus en los equipos de TI, que permita detección, previsión y recuperación ante código malicioso.

2. El sistema de antivirus se debe actualizar periódicamente y configurado para realizar revisiones programadas para la detección de virus en los equipos de TI de la ACFFAA.

**Respaldo de la información**

3. El proceso de respaldo de la información es gestionado por la Oficina de Informática.

4. El respaldo de la información se realiza de acuerdo con la Política Específica de Respaldo de la Información.

**Registros y seguimiento**

**Registro de eventos**

5. Los eventos generados por el tráfico de red, usuarios (operadores y administradores), sistemas de información y servidores deben generar un registro y son monitoreados (Ver tabla 36).
6. La Oficina de Informática deberá gestionar el monitoreo de dichos eventos, con la finalidad de asegurar la integridad y confidencialidad de la información lógica de la ACFFAA.

**Protección de la información de registros (Logs)**

7. Los archivos de registros (Log), deben ser protegidos contra el acceso no autorizado y su alteración.
8. Los archivos de registros (Log), deben ser respaldados con la finalidad de evitar la pérdida de información.

**Sincronización de relojes**

9. La hora y fecha de los equipos dentro del dominio son sincronizados a través del controlador del dominio.
10. La hora y fecha de los servidores independientes, que no pertenecen al dominio, cuentan con un servidor Network Time Protocol (NTP) para su sincronización.

**Instalación de software en los sistemas operativos**

11. La política específica y procedimiento de gestión de accesos establece las disposiciones que deben cumplir los usuarios, en cuanto a los accesos asignados.
12. La Oficina de Informática debe realizar como mínimo dos (02) veces al año, la revisión del software instalado y sus licencias, con la finalidad de asegurar el uso de software autorizado y se deberá emitir un informe de los hallazgos al Jefe de la Oficina de Informática.
13. La Oficina de Informática debe contar un registro del software autorizado y sus licencias.
14. Se encuentra prohíbo la instalación de software no autorizado.
15. El software que sea utilizado por la ACFFAA, se debe adquirir a través de un proceso de compra formal.

**Gestión de vulnerabilidades técnicas**

16. Se debe realizar como mínimo una vez al año un análisis externo de vulnerabilidades técnicas de los sistemas de información en uso y de la infraestructura tecnológica.

17. Los hallazgos y recomendaciones de esta revisión deben ser analizadas e implementadas, de ser el caso.

**Restricciones en la instalación de software por los usuarios**

18. La instalación de software solo es realizado por el personal autorizado.
19. Los usuarios no cuentan con permisos para instalación de aplicativos en sus equipos.
20. La Oficina de Informática gestiona la administración de permisos para los usuarios de la ACFFAA, empleando políticas, privilegios, entre otros.

**Controles de auditoría de sistemas de información**

21. Se debe realizar como mínimo una (01) al año la auditoria a los sistemas de información utilizado para las operaciones de la ACFFAA.
22. Las auditorias de sistemas de información, deberán cumplir con los siguientes requisitos:

1. Responsabilidad
    1. La auditoría de sistemas es programada y supervisada por la Oficina de Informática, pudiendo ser interna y/o externa.

2. Alcance de auditoría de sistemas:
    1. Sistemas de Información utilizados por la ACFFAA para sus operaciones.

3. Acciones de verificación y/o consideraciones:
    1. Privilegios de usuario
    2. Confiabilidad de infraestructura de despliegue
    3. Capacidad de infraestructura
    4. Mantenimiento, monitoreo y gestión
    5. Archivos de Registro
    6. Otras que permitan verificar la performance de los aplicativos, con la finalidad de garantizar la continuidad de los procesos de negocio.

4. Informe de Auditoría:
    1. Se deberá emitir un informe de auditoría a la Oficina de Informática detallando los hallazgos, acciones correctivas y recomendaciones para la mejora.

| | |
|---|---|
| 5. | En caso de generar accesos para la ejecución de auditoría interna, solo se deberán otorgar permiso de lectura. |
| 6. | Las acciones de auditoría de sistemas que puedan comprometer la disponibilidad de la aplicación, se deberán realizar fuera del horario de labores. |

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 10 Política Específica de Seguridad de las Operaciones ISO 27001 - Elaboración Propia

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE SEGURIDAD DE LAS COMUNICACIONES** | |
| | **CODIGO:** **PO-SGSI-008** | **Versión:** **001** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | Establecer un marco de gestión para asegurar la información de la Agencia de Compras de las Fuerzas Armadas (ACFFAA) en las redes y su infraestructura donde se procesa. | |
| **ALCANCE:** | El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA. | |
| **CONTROLES:** | 1. Política sobre el uso de controles criptográficos.<br>2. Gestión de claves. | |
| **CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:** | | |

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 11 Política Específica de Seguridad de las Comunicaciones - Elaboración Propia

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS** | |
| | **CODIGO:** **PO-SGSI-009** | **Versión:** **001** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | Garantizar que la seguridad de la información sea parte integral de los sistemas de información en todo el ciclo de vida. Incluyendo los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas | |
| **ALCANCE:** | El alcance de la presente política se aplica a todo el personal o proveedor de la ACFFAA que participa en la adquisición, desarrollo o mantenimiento de los Sistemas de Información. | |
| **CONTROLES:** | 1. Análisis y Especificación de los Requisitos de Seguridad de la Información<br>2. Aseguramiento de los Servicios de Aplicación en las Redes Públicas<br>3. Protección de las Transacciones de los Servicios de Aplicación<br>4. Política de Desarrollo Seguro<br>5. Procedimiento de Control de Cambio del Sistema<br>6. Revisión Técnica de Aplicaciones después de Cambios en la Plataforma Operativa<br>**7.** Restricciones en Cambios a Paquetes de Software | |
| **CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:** | | |
| **Análisis y Especificación de los Requisitos de Seguridad de la Información**<br>8. La ACFFAA cuenta con el procedimiento PRO-SGSI-008 Desarrollo de Software, en este se establecen las actividades del ciclo de desarrollo de software. | | |

9. Para todos los sistemas desarrollados por la ACFFAA, se determinan los requerimientos de seguridad de información, antes del inicio de fase de desarrollo y/o cambio de la aplicación, con el fin de evitar o minimizar las vulnerabilidades de seguridad de la información.

**Aseguramiento de los Servicios de Aplicación en las Redes Públicas**

10. La información involucrada en los servicios de aplicación que pasan a través de redes públicas es protegida de acuerdo con los requisitos de seguridad definidos en el punto anterior.

**Protección de las Transacciones de los Servicios de Aplicación**

11. La información implicada en las transacciones de los servicios de aplicación se protege para prevenir la transmisión incompleta, la omisión de envío, la alteración del mensaje, la divulgación, la duplicación o repetición del mensaje no autorizados.

**Política de Desarrollo Seguro**

12. El desarrollo o mantenimiento de las aplicaciones de la ACFFAA, se realizarán considerando los requisitos establecidos en la política específica PO-SGSI-013 Política Específica de Ingeniera de Software.

**Procedimiento de Control de Cambio del Sistema**

13. Los cambios solicitados por las áreas usuarias y/o modificaciones realizadas a los aplicativos de la ACFFAA, con la finalidad de asegurar su correcto funcionamiento, así como, el registro de versiones, que es realizado antes de su pase a producción, se realizará de acuerdo con el PRO-SGSI-008 Desarrollo de Software.

**Revisión Técnica de Aplicaciones después de Cambios en la Plataforma Operativa**

14. Se debe verificar y garantizar que los cambios realizados en las aplicaciones de la ACFFAA, no comprometan las actividades y operaciones críticas del negocio.
15. Se deben realizar pruebas con la finalidad de evidenciar el cumplimiento de los requerimientos solicitados por el área usuaria y los requisitos de seguridad de la información definidos por el Oficial de Seguridad de la Información.

**Restricciones en Cambios a Paquetes de Software**

| |
|---|
| 16. Las modificaciones a paquetes de software deben limitarse solo a cambios necesarios y estos deberán ser controlados.<br>17. Se debe considerar el impacto ocasionado a la continuidad de las operaciones e implementar los requisitos de seguridad necesarios para evitar y/o minimizar estos. |

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 12 Política Específica de Adquisición, Desarrollo y Mantenimiento de los Sistemas -

Elaboración Propia

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE RELACIÓN CON PROVEEDORES** | |
| | **CODIGO:**<br>**PO-SGSI-010** | **Versión:**<br>**001**<br>**Fecha de Aprobación:** |
| **OBJETIVO:** | Garantizar la protección de los activos de la Agencia de Compras de las Fuerzas Armadas (ACFFAA) que son accesibles por los proveedores y terceros. | |
| **ALCANCE:** | El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA. | |
| **CONTROLES:** | 1. Política de seguridad de la información para las relaciones con los proveedores.<br>2. Abordar la seguridad dentro de los acuerdos con proveedores.<br>3. Cadena de suministro de tecnología de información y comunicación.<br>4. Monitoreo y revisión de servicios de los proveedores. | |

| | |
|---|---|
| | 5. Gestión de cambios a los servicios de proveedores. |

**CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:**

1. Todo proveedor contratado por la ACFFAA deberá cumplir con las disposiciones establecidas en la Política Específica de Relación con Proveedores y conocer la Política de Seguridad de la Información y remitir al personal de logística de la Oficina General de Administración un formato de Constancia Recepción de Documentos, mediante el cual se hace constancia de la entrega de dicha documentación.

2. Todo proveedor que para el desempeño de sus funciones requiera acceso a las instalaciones y/o activos de información de la ACFFAA tales como, documentación, información, aplicaciones, equipos informáticos, entre otros; deberá firmar un formato de Acuerdo de Confidencialidad para Proveedores, comprometiéndose a remitir dicho documento a la ACFFAA, antes del inicio de sus actividades, sin perjuicio del cumplimiento de las condiciones contractuales.

3. Para los casos que por la naturaleza de la contratación de un proveedor, este requiera que sus trabajadores o terceros subcontratados tengan acceso a las instalaciones de la ACFFAA, como por ejemplo servicio de limpieza, seguridad y/o especialistas, se deberá informar al personal de logística la relación de trabajadores o terceros subcontratados (alta, bajas y/o sustitución) haciendo uso de un formato de Relación de trabajadores de proveedores, dichos trabajadores o terceros subcontratados deberán firmar un formato de Acuerdo de Confidencialidad para Trabajadores de Proveedores, antes del inicio de sus labores, con excepción de aquellos que realicen funciones entrega de bienes como consecuencia de contrataciones que solo contemplen adquisiciones de bienes, los cuales solo tendrán autorización para el acceso a la zona de entrega de los bienes establecida por la ACFFAA, siendo obligatorio su registro de entrada y salida por parte del área de seguridad y en todo momento deberá estar acompañado por un personal autorizado.

4. De ser el caso, el proveedor proporcionará los datos completos de la persona de contacto, quien será el encargado de recibir todo tipo de políticas, procedimientos y/o controles de seguridad de la información, para que asegure su cumplimiento durante la ejecución de sus labores (Ver tabla 35).

5. Los proveedores sólo podrán desarrollar para la ACFFAA, aquellas actividades contempladas bajo los términos de referencia establecidos.

6. Todo proveedor de servicios deberá velar porque su personal que presta los servicios directamente a la organización cumpla con las políticas de seguridad de la información mencionadas en el presente documento. La

ACFFAA se reserva el derecho de solicitar al Proveedor el cambio de personal.

7. El proveedor deberá garantizar que sus trabajadores o terceros subcontratados que realizan labores para la ACFFAA, cuenten con formación y capacitación apropiada para el desarrollo de sus labores, a nivel específico en las materias correspondientes a la denominación de la contratación y conocimiento de las políticas relacionadas de seguridad de la información de la ACFFAA que deberá cumplir.

8. Cualquier tipo de intercambio de información que se produzca entre la ACFFAA y el proveedor, se entenderá que ha sido realizado dentro del marco establecido por la contratación realizada y no podrá ser utilizada en ningún caso fuera de dicho marco.

9. El Comité de Gobierno Digital centraliza los esfuerzos globales de gestión de accesos y protección de activos de la organización, a fin de asegurar el correcto funcionamiento de las tecnologías de la información que soportan los procesos de la organización.

10. Ningún proveedor podrá utilizar la información de la ACFFAA para beneficio propio o de terceros. La información a la que tenga acceso el Proveedor únicamente podrá ser utilizada para los fines específicamente indicados en los Términos de Referencia establecidos.

11. Toda información proporcionada y/o generada durante la ejecución de las actividades para de los Términos de Referencia establecidos es propiedad de ACFFAA

12. El proveedor deberá garantizar que a la culminación del servicio o ante el pedido efectuado por la ACFFAA, cesará inmediatamente el uso de toda información proporcionada, debiendo entregar toda la información que obre en su poder y destruir toda copia que se haya realizado, cualquier sea el medio en el que se encuentre.

13. Cuando el proveedor conozca de cualquier pérdida, uso no autorizado o revelación de la Información proporcionada o de propiedad de la ACFFAA, deberá comunicarlo inmediatamente al área de logística.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 13 Política Específica de Relación con Proveedores –

Elaboración Propia

| | | |
|---|---|---|
| | **POLÍTICA ESPECÍFICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | |
| | **CODIGO:** **PO-SGSI-016** | **Versión:** **001** |
| | | **Fecha de Aprobación:** |
| **OBJETIVO:** | Garantizar un enfoque consistente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación de eventos de seguridad y debilidades de la información. | |
| **ALCANCE:** | El alcance de la presente política abarca todos los aspectos administrativos y de control que deben ser conocidos y cumplidos por todos los servidores y proveedores de la ACFFAA. | |
| **CONTROLES:** | 1. Responsabilidades y procedimientos<br>2. Reporte de eventos y debilidades de seguridad de la información<br>3. Evaluación, decisión y respuesta sobre los eventos de seguridad de información<br>4. Aprender de los incidentes de seguridad de la información<br>**5.** Recolección de evidencia | |

**CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:**

**1.1 Responsabilidades y procedimientos**

Las responsabilidades y procedimientos de gestión de incidentes se encuentran en el procedimiento PRO-SGSI-006 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

**1.2 Reporte de eventos y debilidades de seguridad de la información**

Todo servidor o proveedor de la ACFFAA deberá comunicar los incidentes, eventos y/o debilidades de seguridad de la información que comprometan la integridad, confidencialidad y

disponibilidad de los activos de información de la ACFFAA.

Dicha comunicación deberá realizarse mediante los canales establecidos la ACFFAA.

**1.3 Evaluación, decisión y respuesta sobre los eventos de seguridad de información**

Los incidentes, eventos y/o debilidades de seguridad de la información son registrados, clasificados, evaluados y atendidos de acuerdo con el procedimiento PRO-SGSI-006 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

**1.4 Aprender de los incidentes de seguridad de la información**

Se ha establecido el registro de lecciones aprendidas en el FOR-SGSI-025 Registro de Incidentes de Seguridad de la Información, con él se busca generar una fuente de conocimientos en base a los incidentes presentados, con la finalidad de brindar solucionar futuros incidentes en base a las acciones ya realizadas.

**1.5 Recolección de evidencia**

El Oficial de Seguridad de la Información podrá solicitar a las dependencias de la ACFFAA la documentación, registros, accesos y/o cualquier otra información que permita realizar el análisis, evaluación, solución de los incidentes, eventos y/o debilidades de seguridad de la Información reportados y/o evidenciar incumplimiento de los controles de seguridad establecidos por SGSI por parte de los servidores de la ACFFAA o proveedores.

La ACFFAA ha definido un procedimiento para la identificación, recolección y conservación de la información que puede servir como evidencia para el análisis, evaluación propósitos de acción disciplinaria y legal. Se describe dicho procedimiento en el documento PRO-SGSI-006 Procedimiento de Gestión de Incidentes de Seguridad de la Información.

Las evidencias de los incidentes de seguridad de la información serán conservadas en un repositorio físico y/o virtual.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 14 Política Específica de Gestión de Incidentes de la Información -

Elaboración Propia

<table>
<tr><td rowspan="3"></td><td colspan="2">POLÍTICA ESPECÍFICA DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTION DE LA CONTINUIDAD DEL NEGOCIO</td></tr>
<tr><td>CODIGO:<br>PO-SGSI-017</td><td>Versión:<br>001</td></tr>
<tr><td></td><td>Fecha de Aprobación:</td></tr>
<tr><td>OBJETIVO:</td><td colspan="2">Establecer los lineamientos para la gestión de la Seguridad de la Información en función a la continuidad del negocio de la Agencia de Compras de las Fuerzas Armadas (ACFFAA).</td></tr>
<tr><td>ALCANCE:</td><td colspan="2">El alcance de la presente política abarca la plataforma tecnológica que brinda soporte a los sistemas de información utilizados en los procesos de negocio.</td></tr>
<tr><td>CONTROLES:</td><td colspan="2">1. Responsabilidades y procedimientos<br>2. Reporte de eventos y debilidades de seguridad de la información<br>3. Evaluación, decisión y respuesta sobre los eventos de seguridad de información<br>4. Aprender de los incidentes de seguridad de la información<br>5. Recolección de evidencia</td></tr>
<tr><td colspan="3">CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:</td></tr>
<tr><td colspan="3">1. La plataforma tecnológica que brinda soporte a los servicios de tecnología de la información (TI) y a los sistemas de información, deben contar con una infraestructura que garantice su disponibilidad y adecuados controles de seguridad que garantice su integridad y confidencialidad de la información.</td></tr>
</table>

2. Los servidores físicos de la ACFFAA, se deben configuran en un clúster de alta disponibilidad con tolerancia a fallos a discos e indisponibilidad de servidor.

3. El sistema de alimentación ininterrumpida (UPS), cuenta con una configuración redundante, el cual brinda tolerancia a fallas e indisponibilidad.

4. La ACFFAA cuenta con el procedimiento PRO-SGSI-010 Plan de contingencias, donde se detallan las acciones a tomar para restablecer la disponibilidad de la información ante situaciones adversas que comprometan la continuidad de las operaciones de la ACFFAA, de los siguientes componentes tecnológicos:

    1. Servidor de Archivos
    2. Base de datos de producción
    3. Servidores Virtuales
    4. Equipo de Seguridad Perimetral

5. El plan de contingencias deberá ser activado, al haber transcurrido al menos una (01) hora de la inactividad de uno o más de los componentes tecnológicos anteriormente mencionados y al haberse realizado todas las acciones posibles para la operatividad de los mismo en el menor tiempo posible.

6. Para todos los casos, en los que sea aplicado el plan de contingencias, se aplicaran los controles de seguridad aprobados en el Sistema de Gestión de Seguridad de la Información (SGSI) de la ACFFAA.

7. El Procedimiento de Plan de Contingencias, debe ser evaluado de forma semestral por la Oficina de Informática para identificar deficiencias y mejoras.

8. Las copias de seguridad y respaldo de la información deben ser almacenadas en un arreglo de disco con tolerancia a fallos u otra tecnología que garantice su protección.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 15 Política Específica de Seguridad de la Información en la Gestión de la Continuidad del Negocio –

Elaboración Propia

<table>
<tr><td rowspan="3"></td><td colspan="2">POLÍTICA ESPECÍFICA DE CUMPLIMIENTO</td></tr>
<tr><td rowspan="2">CODIGO:<br>PO-SGSI-018</td><td>Versión:<br>001</td></tr>
<tr><td>Fecha de Aprobación:</td></tr>
<tr><td>OBJETIVO:</td><td colspan="2">Establecer los lineamientos para la gestión de la Seguridad de la Información en función a la continuidad del negocio de la Agencia de Compras de las Fuerzas Armadas (ACFFAA).</td></tr>
<tr><td>ALCANCE:</td><td colspan="2">El alcance de la presente política abarca la plataforma tecnológica que brinda soporte a los sistemas de información utilizados en los procesos de negocio.</td></tr>
<tr><td>CONTROLES:</td><td colspan="2">1. Responsabilidades y procedimientos<br>2. Reporte de eventos y debilidades de seguridad de la información<br>3. Evaluación, decisión y respuesta sobre los eventos de seguridad de información<br>4. Aprender de los incidentes de seguridad de la información<br>5. Recolección de evidencia</td></tr>
<tr><td colspan="3">CRITERIOS PARA LA IMPLEMENTACION DE LA POLITICA:</td></tr>
<tr><td colspan="3">6. La plataforma tecnológica que brinda soporte a los servicios de tecnología de la información (TI) y a los sistemas de información, deben contar con una infraestructura que garantice su disponibilidad y adecuados controles de seguridad que garantice su integridad y confidencialidad de la información.<br>7. Los servidores físicos de la ACFFAA, se deben configuran en un clúster de alta disponibilidad con tolerancia a fallos a discos e indisponibilidad de servidor.</td></tr>
</table>

8. El sistema de alimentación ininterrumpida (UPS), cuenta con una configuración redundante, el cual brinda tolerancia a fallas e indisponibilidad.
9. La ACFFAA cuenta con el procedimiento PRO-SGSI-010 Plan de contingencias, donde se detallan las acciones a tomar para restablecer la disponibilidad de la información ante situaciones adversas que comprometan la continuidad de las operaciones de la ACFFAA, de los siguientes componentes tecnológicos:

    1. Servidor de Archivos
    2. Base de datos de producción
    3. Servidores Virtuales
    4. Equipo de Seguridad Perimetral

10. El plan de contingencias deberá ser activado, al haber transcurrido al menos una (01) hora de la inactividad de uno o más de los componentes tecnológicos anteriormente mencionados y al haberse realizado todas las acciones posibles para la operatividad de los mismo en el menor tiempo posible.
11. Para todos los casos, en los que sea aplicado el plan de contingencias, se aplicaran los controles de seguridad aprobados en el Sistema de Gestión de Seguridad de la Información (SGSI) de la ACFFAA.
12. El Procedimiento de Plan de Contingencias, debe ser evaluado de forma semestral por la Oficina de Informática para identificar deficiencias y mejoras.
13. Las copias de seguridad y respaldo de la información deben ser almacenadas en un arreglo de disco con tolerancia a fallos u otra tecnología que garantice su protección.

| DETALLE | VERSIÓN | FECHA | RESPONSABLE |
|---|---|---|---|
| Versión inicial del documento | 001 | | Oficial de Seguridad de la Información |

Tabla 16 Política Específica de Cumplimiento –

Elaboración Propia

## 5.2. Especificación y desarrollo en base a estudio, análisis y diagrama de flujo.

Los lineamientos de las políticas se encuentran en cambios constantes, las cuales pueden ser modificadas, de acuerdo con normas, leyes.

La ACFFAA se acoge a políticas de seguridad ya establecidas, con la finalidad de proteger la integridad, confidencialidad y disponibilidad de la información, dichas políticas son evaluadas e implementadas por el Comité de Gobierno Digital. Y se tiene que acoplar a las modificaciones guiadas por entidades del estado líderes. También se respetan los lineamientos de Ciberseguridad que refuerzan las capacidades de la ACFFAA para enfrentar las amenazas que atentan contra su seguridad y ciberseguridad, creando un entorno y las condiciones necesarias que permitan brindar protección en el ciberespacio.

Para la Agencia de Compras de las Fuerzas Armadas, la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual declara los siguientes compromisos con la seguridad de la información física o digital que está bajo su competencia:

• Proteger los activos de información del sistema de gestión de seguridad de la información de la ACFFAA, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar su confidencialidad, integridad y disponibilidad.

• Proporcionar los recursos necesarios para asegurar la implementación de las medidas de control necesarias para evitar que los riesgos de la seguridad de la información se materialicen

**Con la ISO 27001:**

La ISO 27001 no tiene un proceso fijo, solo es una guía para la implementación del SGI, los lineamientos se adecuan conforme a las necesidades de la empresa, de acuerdo la seguridad y prevención. Por lo cual se seguirá supervisando el buen funcionamiento del proceso de aprobación de una Política de SGSI en las ACFFAA, que se lleva a cabo en la actualidad.

## 5.3 Operación para la realización de la matriz de Riesgos

**Con la ISO 27001:**

Se planea presentar una matriz de Riesgos y dar seguimiento a la mejora continua, basado en la frecuencia, revisión y actualización que evalúe la eficacia de las actualizaciones mediante la comparación de medidas de seguridad de la información antes y después de las actualizaciones (Ver Tabla 17).

| ACTIVO | AMENAZA | VULNERABILIDAD | ¿Qué afecta en los activos de información? | | | RIESGO EFECTIVO | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | C | I | D | VALOR CID | IMPACTO | PROBABILIDAD | NIVEL DE RIESGO | NOMBRE DEL RIESGO | PROPIETARIO DEL RIESGO | CÓDIGO DE RIESGO |
| **Información Documento en papel** | AM21 - **Causas naturales** | VU23 – Falta de establecimiento de prácticas de control de documentos y registros | 3 | 1 | 2 | Alto | 5 | 2 | Alto | Causas Naturales | Jefe de Informática | SGSI-TI-001 |
| | AM36 - **Eliminación inadecuada** | VU88 – Falta de Clasificación y manejo de la información | 1 | 3 | 2 | Alto | 4 | 4 | Muy Alto | Eliminación Inadecuada de Documentos | Jefe de Informática | SGS-TI-002 |

Tabla 17 Matriz de Riesgos - ISO 27001 –

Elaboración Propia

En esta matriz (Tabla 18) se identificará y registrará el activo, midiendo su Confidencialidad, Integridad y Disponibilidad, en las siguientes tablas se encuentran plasmados los valores correspondientes a Impacto, Probabilidad y Niveles de Riesgo, con los cuales

se llenará esta matriz.

| ACTIVO | AMENAZA | VULNERABILIDAD | ¿Qué afecta en los activos de información? | | | | RIESGO EFECTIVO | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | C | I | D | VALOR CID | IMPACTO | PROBABILIDAD | NIVEL DE RIESGO | NOMBRE DEL RIESGO | PROPIETARIO DEL RIESGO | CÓDIGO DE RIESGO |
| Información Documento en papel | AM21 - **Causas naturales** | VU23 – Falta de establecimiento de prácticas de control de documentos y registros | 3 | 1 | 2 | Alto | 5 | 2 | Alto | Robo de medios o documentos por falta de políticas de identificación y autentificación de usuarios | Jefe de Informática | SGSI-TI-001 |
| | AM36 - **Eliminación inadecuada** | VU88 – Falta de Clasificación y manejo de la información | 1 | 3 | 2 | Alto | 4 | 4 | Muy Alto | Corrupción de datos por no contar con encriptación o cifrado de HD | Jefe de Informática | SGS-TI-002 |

Tabla 18 Matriz de Riesgos – Elaboración Propia

La matriz de Confidencialidad nos ayuda a medir el nivel de confidencialidad de nuestra información. Lo que hacemos es identificar qué datos son más sensibles y asignarles un nivel de secreto. Por ejemplo, podemos clasificar la información en Alta, Media, o Baja, según lo delicada que sea (Ver Tabla 19).

| Niveles | CONFIDENCIALIDAD |
|---|---|
| **(3) Alta** | Su distribución debe estar restringida a un pequeño grupo de personas, pues revelarla sin permiso puede tener un impacto negativo de grandes alcances para la organización empleados y/o terceros.<br>Su acceso debe ser expresamente autorizado por el Propietario de la Información y restringido a un grupo reducido de usuarios que la necesite para el desarrollo de sus tareas habituales. Revelarla sin autorización puede repercutir negativamente, originando un impacto mayor en las operaciones. |
| **(2) Media** | La clasificación interna es la más común que se maneja en la organización. Su distribución está generalmente restringida a un grupo más grande de personas. Revelarla sin autorización puede repercutir negativamente, originando un impacto moderado en las operaciones. La información de uso interno se convertirá en pública solo con la autorización del propietario de la información, quién deberá autorizar cualquier difusión de esta. |
| **(1) Baja** | La información pública no es confidencial y está enfocada al uso general tanto dentro como fuera de la organización. Podrá ser revelada por el dueño o responsable de la misma que tenga dentro de sus funciones la autorización para revelarla al público. |

Tabla 19 Tabla de Confidencialidad –

Elaboración Propia

En esta matriz, la idea es evaluar cuán disponibles están nuestros datos. Miramos la importancia de cada tipo de información para que el negocio funcione sin problemas y le asignamos un nivel de disponibilidad. Es como asegurarnos de que podamos acceder a la información cuando la necesitemos sin contratiempos (Ver tabla 20).

| Niveles | DISPONIBILIDAD |
|---|---|
| **(3) Alta** | La no disponibilidad de la información puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdidas de imagen severas a la organización, impacta a terceros. |
| **(2) Media** | La no disponibilidad de la información puede conllevar un impacto negativo, retrasar sus funciones, o generar pérdida de imagen moderado a la organización, puede afectar a terceros. |
| **(1) Baja** | La no disponibilidad de la información puede afectar la operación normal de la organización o terceros, pero no conlleva implicaciones legales, económicas o de pérdida de imagen. |

Tabla 20 Tabla de Niveles de Disponibilidad –

Elaboración Propia

Esta matriz nos permite evaluar de manera sencilla los riesgos en la seguridad de la información.

**Aspecto de Seguridad Afectado por el Riesgo:**

Identificamos qué aspecto específico de la seguridad de la información está en juego. Puede ser desde la protección de datos personales hasta la integridad de los sistemas.

**VALOR CID:**

Asignamos un VALOR CID que refleja la importancia del aspecto de seguridad afectado. Este valor considera la Confidencialidad, Integridad y Disponibilidad. Por ejemplo, si estamos tratando con información altamente confidencial, asignamos un valor alto para destacar su relevancia (Ver tabla 21).

| Aspecto de Seguridad afectado por el riesgo | | | VALOR CID |
|---|---|---|---|
| C | I | D | |
| 1 | 1 | 1 | No significativo |
| 1 | 1 | 2 | Menor |
| 1 | 1 | 3 | Critico |
| 1 | 2 | 1 | Menor |
| 1 | 2 | 2 | Moderado |

| | | | |
|---|---|---|---|
| 1 | 2 | 3 | Critico |
| 1 | 3 | 1 | Critico |
| 1 | 3 | 2 | Critico |
| 1 | 3 | 3 | Muy Critico |
| 2 | 1 | 1 | Menor |
| 2 | 1 | 2 | Moderado |
| 2 | 1 | 3 | Critico |
| 2 | 2 | 1 | Moderado |
| 2 | 2 | 2 | Moderado |
| 2 | 2 | 3 | Critico |
| 2 | 3 | 1 | Critico |
| 2 | 3 | 2 | Critico |
| 2 | 3 | 3 | Muy Critico |
| 3 | 1 | 1 | Critico |
| 3 | 1 | 2 | Critico |
| 3 | 1 | 3 | Muy Critico |
| 3 | 2 | 1 | Critico |
| 3 | 2 | 2 | Critico |
| 3 | 2 | 3 | Muy Critico |

| | | | |
|---|---|---|---|
| 3 | 3 | 1 | Muy Critico |
| 3 | 3 | 2 | Muy Critico |
| 3 | 3 | 3 | Muy Critico |

Tabla 21 Afecto de Seguridad afectado por el Riesgo - Elaboración Propia

| | |
|---|---|
| No significativo | es cuando en el CID los valores son todos 1 |
| Menor | es cuando en el CID al menos tiene un valor 2 |
| Moderado | es cuando en el CID tiene dos valores 2 |
| Critico | es cuando en el CID al menos tiene un valor 3 |
| Muy Critico | es cuando en el CID tiene dos o tres valores 3 |

Ilustración 10 Tabla de Valores de Afectos de Seguridad.

Elaboración Propia

**Medición del Impacto y la probabilidad:**

Al combinar la probabilidad y el impacto en la tabla, obtenemos una visión clara de los riesgos. Si hay una probabilidad y un impacto altos, estamos tratando con un riesgo significativo. Por otro lado, una baja probabilidad y bajo impacto indican riesgos menores (Ver tabla 22 y tabla 23).

| IMPACTO | | |
|---|---|---|
| Nivel | Descripción | Impacto |
| 5 | Muy Alto | Impacta de forma trágica la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio. El impacto es a todo la empresa y su efecto se siente en todo el personal involucrado. |
| 4 | Alto | Impacta de forma alta, comprometiendo los objetivos o activos de información de la empresa o la continuidad de las operaciones por paralización de los procesos de soporte, o de alguna unidad. |
| 3 | Medio | Impacta de forma moderada sobre los objetivos, procesos o activos de la empresa comprometiendo varias actividades. |
| 2 | Bajo | El impacto es leve y se puede prescindir del mismo en un tiempo limitado. |
| 1 | Muy Bajo | No representa un impacto importante para empresa |

Tabla 22 Medición del Impacto y la probabilidad.
Elaboración Propia.

| PROBABILIDAD | | |
|---|---|---|
| Nivel | Descripción | Probabilidad |
| 5 | Muy Alto | Se espera que ocurra en la mayoría de las circunstancias (Todos los días) |
| 4 | Alto | Puede ocurrir en la mayoría de las circunstancias (1 a la semana) |
| 3 | Medio | Probablemente ocurriría en la mayoría de las circunstancias (1 vez al mes) |
| 2 | Bajo | Puede ocurrir solo en circunstancias excepcionales (1 vez cada 6 meses) |
| 1 | Muy Bajo | Puede ocurrir en algún momento (Cada año o más) |

Tabla 23 Probabilidad-
Elaboración Propia

1. **Tabla de valorización de Riesgo:**

Esta tabla es una herramienta práctica para entender y gestionar riesgos.

**Identificación de Riesgos:**

En esta tabla, identificamos los posibles problemas o eventos que podrían afectar nuestros objetivos. Esto podría ser desde problemas técnicos hasta cambios en el mercado.

**Probabilidad de Ocurrencia:**

Evaluamos cuán probable es que ocurra cada riesgo. ¿Es algo que podría suceder con frecuencia, o es más una posibilidad remota? Utilizamos una escala para calificar la probabilidad, desde bajo hasta Muy Alto.

**Impacto en el Negocio:**

Ahora, consideramos qué tan grave sería cada riesgo si realmente ocurriera. ¿Tendría un impacto menor o podría ser un desafío significativo? Usamos una escala similar para evaluar el impacto, desde bajo hasta alto.

**Valoración del Riesgo:**

Al combinar la probabilidad y el impacto, obtenemos una valoración general del riesgo. Los riesgos con una alta probabilidad y un impacto significativo se consideran más críticos y requieren una atención especial. (Ver tabla 24).

| Tabla de Valorización de Riesgos | | | | | |
|---|---|---|---|---|---|
| **Impacto** | **Calificación** | **Probabilidad** | **Calificación** | **Riesgo** | **Valor** |
| Muy Alto | 5 | Muy Alta | 5 | Muy Alto | 25 |
| Alto | 4 | Muy Alta | 5 | Muy Alto | 20 |
| Medio | 3 | Muy Alta | 5 | Muy Alto | 15 |
| Bajo | 2 | Muy Alta | 5 | Alto | 10 |

| | | | | | |
|---|---|---|---|---|---|
| Muy Bajo | 1 | Muy Alta | 5 | Medio | 5 |
| Muy Alto | 5 | Alta | 4 | Muy Alto | 20 |
| Alto | 4 | Alta | 4 | Muy Alto | 16 |
| Medio | 3 | Alta | 4 | Alto | 12 |
| Bajo | 2 | Alta | 4 | Medio | 8 |
| Muy Bajo | 1 | Alta | 4 | Bajo | 4 |
| Muy Alto | 5 | Media | 3 | Muy Alto | 15 |
| Alto | 4 | Media | 3 | Alto | 12 |
| Medio | 3 | Media | 3 | Alto | 9 |
| Bajo | 2 | Media | 3 | Medio | 6 |
| Muy Bajo | 1 | Media | 3 | Bajo | 3 |
| Muy Alto | 5 | Baja | 2 | Alto | 10 |
| Alto | 4 | Baja | 2 | Medio | 8 |
| Medio | 3 | Baja | 2 | Medio | 6 |
| Bajo | 2 | Baja | 2 | Bajo | 4 |
| Muy Bajo | 1 | Baja | 2 | Muy Bajo | 2 |
| Muy Alto | 5 | Muy Baja | 1 | Medio | 5 |
| Alto | 4 | Muy Baja | 1 | Bajo | 4 |
| Medio | 3 | Muy Baja | 1 | Bajo | 3 |
| Bajo | 2 | Muy Baja | 1 | Muy Bajo | 2 |
| Muy Bajo | 1 | Muy Baja | 1 | Muy Bajo | 1 |

Tabla 24 Tabla de valorización de Riesgo - Elaboración Propia

**Tratamiento de Riesgos**

El tratamiento de riesgos será como un escudo para la ACFFAA.

**Identificación de Riesgos:**

El tratamiento de riesgos comenzará identificando posibles problemas que

podrían afectar las metas.

**Análisis de Consecuencias y Probabilidades:**

No todos los riesgos son iguales. Algunos podrían ser más probables, mientras que otros podrían tener consecuencias más graves. Se analizará y clasificará para priorizar la atención.

**Estrategias de Tratamiento:**

Aquí es donde entra en juego la creatividad. Se desarrollará estrategias para abordar cada riesgo identificado.

**Aceptación o Rechazo:**

Algunos riesgos son simplemente parte del juego empresarial. Decides conscientemente aceptar ciertos riesgos que no pueden evitarse y rechazar aquellos que podrían ser perjudiciales.

Monitoreo Continuo:

La gestión de riesgos no es un proceso de una sola vez. Se establecerá un sistema para monitorear continuamente los riesgos y ajustar las estrategias según sea necesario (Ver Ilustración 11).

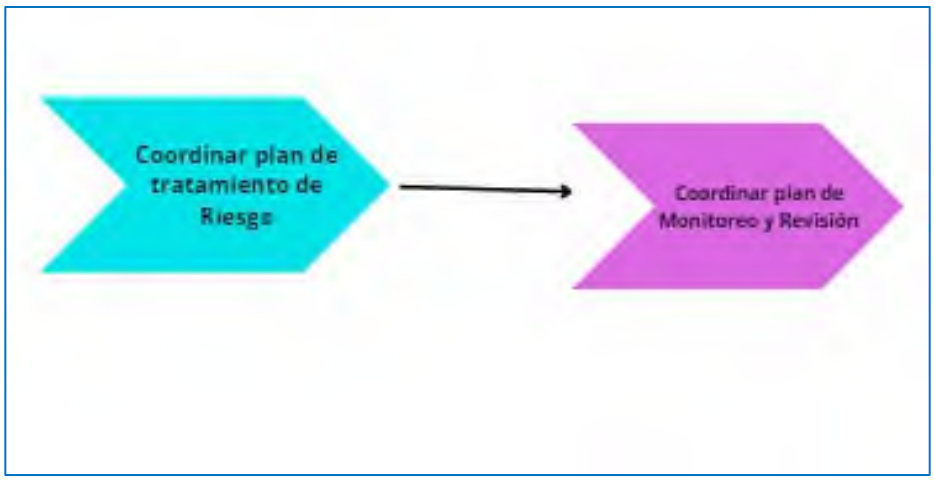


Ilustración 11 Fase de Monitoreo y Revisión –

Elaboración Propia

Después de finalizar la evaluación de riesgos, se deberá ver la solución para tratar el riesgo. A continuación, se presentan formas del tratamiento del Riesgo:

1. Prevenir el Riesgo
2. Aplicar controles de acuerdo con análisis para reducir el riesgo.
3. Informar el riesgo
4. Afrontar el riesgo

Los riesgos residuales requieren evaluación y categorización como aceptables o no-aceptables. Se requiere la creación de un comité que decida su aceptación y establezca qué controles deben ser implementados en el futuro.

## 5. Guía de Inventario de Activos

Un inventario de Activos es el primer paso de acuerdo con el SGSI.

Es importante identificar todos los activos posibles en una organización, de ese modo se podrá identificar cuáles son los activos más críticos y cuales no son un riesgo para la organización (Tabla 25).

**Categorías de activos**

Los activos deben ordenarse por categorías:

| Categoría | Ejemplos de Activos | | | |
|---|---|---|---|---|
| Activos de Software | Aplicaciones Desarrolladas | Herramientas de encriptación | Aplicaciones Especializadas | Licencias de Software |
| | | | | |
| | | | | |
| | Aplicaciones estándares (Word, Excel, etc.) | Herramientas de desarrollo | Antivirus | Sistema operativo |
| | | | | |
| Activos Físicos (no digitales) | Celulares | Cables | Edificios | Periféricos |
| | Módems | CD's | Aire acondicionado | Tarjetas magnéticas |
| | Redes | USB's | UPS | Tabletas |
| | Routers | Computadoras | Fotocopiadoras | Switches |
| | Cintas | Laptops | Impresoras | Libros |
| | Teléfonos | | | |

| | | | | |
|---|---|---|---|---|
| Activos (personal) | Administradores | Practicantes | Personal de seguridad | Desarrolladores |
| | Personal de limpieza | Gerentes | Personal temporal | Terceros |
| | Personal de comunicaciones | Personal de redes | Personal informático | Personal de otras áreas |
| Activos Intangibles | Nombre de la Marca | Copyright | Patentes Reputación | |
| **Columna1** | **Columna2** | **Columna3** | **Columna4** | **Columna5** |
| Categoría | Ejemplos de Activos | | | |
| Activos de Software | Aplicaciones Desarrolladas | Herramientas de encriptación | Aplicaciones Especializadas | Licencias de Software |
| | | | | |
| | | | | |
| | Aplicaciones estándares (Word, Excel, etc) | Herramientas de desarrollo | Antivirus | Sistema operativo |
| | | | | |
| Activos Físicos (no digitales) | Celulares | Cables | Edificios | Periféricos |
| | Módems | CD's | Aire acondicionado | Tarjetas magnéticas |
| | Redes | USB's | UPS | Tabletas |
| | Routers | Computadoras | Fotocopiadoras | Switches |
| | Cintas | Laptops | Impresoras | Libros |
| | Teléfonos | | | |
| Activos (personal) | Administradores | Practicantes | Personal de seguridad | Desarrolladores |
| | Personal de limpieza | Gerentes | Personal temporal | Terceros |
| | Personal de comunicaciones | Personal de redes | Personal informático | Personal de otras áreas |

Tabla 25 Guía de Categorías de Inventarios.

Elaboración Propia

## 6. Registro de Activos

Se deberá registrar todos los activos de la organización en una matriz con código R001 - 2023 para poder identificarlos y tener un control sobre éstos (Ver tabla 26).

| N° | Código | Nombre | Descripción | Categoría | Ubicación | Información Almacenada | Tipo de Acceso | Confidencialidad | Disponibilidad | Integridad | Nivel de Disponibilidad |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 5 | | | | | | | | | | | |
| 6 | | | | | | | | | | | |
| 7 | | | | | | | | | | | |
| 8 | | | | | | | | | | | |
| 9 | | | | | | | | | | | |

Tabla 26 Tabla de Registro de Activos –

Elaboración Propia

A continuación, se detallan los campos de la matriz:

1. **Código:** Identificador único del activo.
2. **Nombre:** Denominación de un activo.
3. **Descripción**: Explicar detallada y ordenada, las características del
4. activo.
5. **Categoría:** Clasificar al activo según la categoría a la que pertenece (ver
6. "Categorías de activos").
7. **Ubicación:** Indicar la localización geográfica en la que se encuentra el activo de
8. información.
9. **Información almacenada:** Indicar la información que se encuentra en el activo de
10. información registrado.
11. **Tipo de acceso:** Indicar el nivel de acceso requerido por el activo, estos pueden ser:

- Público: Puede ser accesible por cualquier persona, ya sea interna o externa a la organización.
- Interno: Solamente puede ser accesible a personal interno de la organización.
- Restringido: Información accesible solamente a personal establecido por las políticas
de la organización.

82

- Confidencial: Información disponible solamente bajo autorización o a personal con cargos altos en la organización.
- Seguridad de la información: Indicar el nivel de sensibilidad de acuerdo con los siguientes

**Guía del plan de tratamiento de riesgos**

Una vez identificados los riesgos de la empresa a través del proceso de evaluación de se deberá tomar decisiones para las acciones a realizar para el tratamiento de riesgos. Se deberá estructurar un "Plan de tratamiento del riesgo". Este proceso se encarga de seleccionar e implementar las medidas o decisiones acordadas para modificar el nivel e impacto del riesgo. El plan de tratamiento del riesgo es un documento que define las acciones específicas que van a ser o han sido adoptadas por la organización, para garantizar que los activos se encuentran protegidos y los

riesgos asociados a éstos se puedan mitigar. Las actividades para realizar durante el proceso de tratamiento de riesgo son las siguientes:

1. Aplicación de garantías son apropiadas para reducir el nivel del
2. riesgo identificado (reducir o mitigar el riesgo).
3. Identificar y eliminar la actividad que origina el riesgo.
4. El riesgo pueda ser atendido por un tercero
5. Aceptar el riesgo

De este modo, un riesgo puede ser aceptado por la empresa, si éste no es aceptado se procede a decidir la implementación de alguna actividad para tratar o mitigar el riesgo identificado. Sin embargo, el riesgo residual debe de ser aceptado por la empresa para garantizar que la actividad implementada ha tenido la efectividad que se esperaba.

**Estableciendo el plan de tratamiento de riesgos**

El plan debe mostrar cada riesgo identificado en el proceso de evaluación de riesgos será tratado para ser reducido o mitigado, las garantías que ya se han implementado, las garantías adicionales a considerar y los tiempos para la implementación de estas. Una vez que el plan de tratamiento de riesgos se ha culminado, los recursos pueden ser asignados a sus correspondientes asignaciones para comenzar su implementación (Ver Figura 27).

| Plan de tratamiento de riesgos | | | | |
|---|---|---|---|---|
| **Riesgo** | Nivel de maduración A S-IS | Nivel de madurez TO-BE | Plan de Acción | Responsable |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

Tabla 27 Plan de Tratamiento de Riesgos –

Elaboración Propia

**Tabla de Controles del Anexo A**

La Tabla de Controles del Anexo A es la brújula que guía la nave de la seguridad de la información. Cada control es como una estrella que asegura un viaje seguro en el vasto océano digital (Ver tabla 28).

| Cláusula N° | Objetivos de Control | Control |
|---|---|---|
| **A.5** | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** | |
| | A.5.1 Dirección de Gestión para la Seguridad de Información | A.5.1.1 Políticas de seguridad de información |
| | | A.5.1.2 Revisión de las políticas de seguridad de información |
| **A.6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | |
| | A.6.1 Organización Interna | A.6.1.1 Funciones de seguridad de información y responsabilidades |
| | | A.6.1.2 Separación de funciones |
| | | A.6.1.3 Contacto con autoridades |
| | | A.6.1.4 Contacto con grupos de interés especial |
| | | A.6.1.5 Seguridad de información en gestión de proyectos |
| | A.6.2 Equipos Móviles y trabajo a distancia | A.6.2.1 Política de los equipos móviles |
| | | A.6.2.2 Trabajo a distancia |

| | | |
|---|---|---|
| **A.7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | |
| | A.7.1 Antes del Empleo | A.7.1.1 Selección |
| | | A.7.1.2 Términos y condiciones de empleo |
| | A.7.2 Durante el Empleo | A.7.2.1 Responsabilidades de la gerencia |
| | | A.7.2.2 Conciencia de seguridad de información, educación y capacitación |
| | | A.7.2.3 Proceso disciplinario |
| | A.7.3 Términos y Cambio de Empleo | A.7.3.1 Término o cambio de las responsabilidades de empleo |
| **A.8** | **GESTIÓN DE ACTIVOS** | |
| | A.8.1 Responsabilidad por Activos | A.8.1.1 Inventario de activos |
| | | A.8.1.2 Propiedad de activos |
| | | A.8.1.3 Uso aceptable de activos |
| | | A.8.1.4 Retorno de activos |
| | A.8.2 Clasificación de la Información | A.8.2.1 Clasificación de información |
| | | A.8.2.2 Etiquetado de información |
| | | A.8.2.3 Manejo de activos |
| | A.8.3 Manejo de Medios | A.8.3.1 Gestión de medios removibles |
| | | A.8.3.2 Disposición de medios |
| | | A.8.3.3 Transferencia de medios físicos |
| **A.9** | **CONTROL DE ACCESOS** | |
| | A.9.1 Requisitos de Negocio para el Control de Acceso | A.9.1.1 Política de control de acceso |
| | | A.9.1.2 Acceso a redes y servicios de red |

| | | |
|---|---|---|
| | A.9.2 Gestión de Acceso de Usuario | A.9.2.1 Registro y baja de usuarios |
| | | A.9.2.2 Provisión del acceso de usuario |
| | | A.9.2.3 Gestión de derechos de acceso privilegiados |
| | | A.9.2.4 Gestión de la información de autenticación secreta de los usuarios |
| | | A.9.2.5 Revisión de derechos de acceso de usuarios |
| | | A.9.2.6 Eliminación o ajuste de derechos de acceso |
| | A.9.3 Responsabilidades de Usuarios | A.9.3.1 Uso de información de autenticación secreta |
| | A.9.4 Control de Acceso a sistema y aplicación | A.9.4.1 Restricción de acceso a la información |
| | | A.9.4.2 Procedimientos seguros de inicio de sesión |
| | | A.9.4.3 Sistema de gestión de contraseña |
| | | A.9.4.4 Uso de programas utilitarios privilegiados |
| | | A.9.4.5 Control de acceso al código fuente de los programas |
| **A.10** | **CRIPTOGRAFIA** | |
| | A.10.1 Controles criptográficos | A.10.1.1 Política de uso de los controles criptográficos |
| | | A.10.1.2 Gestión de claves |
| **A.11** | **SEGURIDAD FÍSICA Y AMBIENTAL** | |
| | A.11.1 Áreas de Seguridad | A.11.1.1 Perímetro de seguridad física |
| | | A.11.1.2 Controles de entrada física |
| | | A.11.1.3 Seguridad de oficinas, salas |
| | | A.11.1.4 Protección contra amenazas externas y ambientales |

| | | |
|---|---|---|
| | | A.11.1.5 Trabajo en áreas seguras |
| | | A.11.1.6 Áreas de despacho y carga |
| | A.11.2 Equipos | A.11.2.1 Situar los equipo y protección |
| | | A.11.2.2 Servicios públicos de apoyo |
| | | A.11.2.3 Seguridad del cableado |
| | | A.11.2.4 Mantenimiento de los equipos |
| | | A.11.2.5 Retiro de los activos |
| | | A.11.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones |
| | | A.11.2.7 Eliminación segura o reúso de equipos |
| | | A.11.2.8 Equipos de usuarios no atendidos |
| | | A.11.2.9 Política de escritorio y pantalla limpia |
| **A.12** | **SEGURIDAD DE LAS OPERACIONES** | |
| | A.12.1 Procedimientos y Responsabilidades operativas | A.12.1.1 Procedimientos de operación documentados |
| | | A.12.1.2 Gestión de cambio |
| | | A.12.1.3 Gestión de capacidad |
| | | A.12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones |
| | A.12.2 Protección contra Malware | A.12.2.1 Control contra malware |
| | A.12.3 Respaldo | A.12.3.1 Copia de información |

| | | |
|---|---|---|
| | A.12.4 Registro y Monitoreo | A.12.4.1 Registro de eventos |
| | | A.12.4.2 Protección de información de registro |
| | | A.12.4.3 Registros de administrador y operador |
| | | A.12.4.4 Sincronización de reloj |
| | A.12.5 Control del Software Operativo | A.12.5.1 Instalación de software en sistemas operacionales |
| | A.12.6 Gestión de Vulnerabilidad Técnica | A.12.6.1 Gestión de vulnerabilidades técnicas |
| | | A.12.6.2 Restricciones en la instalación de software |
| | A.12.7 Consideraciones para la Auditoría de Sistemas de Información | A.12.7.1 Controles de auditoría de sistemas de información |
| **A.13** | **SEGURIDAD DE LAS COMUNICACIONES** | |
| | A.13.1 Gestión de Seguridad de Redes | A.13.1.1 Controles de redes |
| | | A.13.1.2 Seguridad de los servicios de redes |
| | | A.13.1.3 Separación en redes |
| | A.13.2 Transferencia de Información | A.13.2.1 Procedimientos y políticas de transferencia de información |
| | | A.13.2.2 Acuerdos sobre transferencia de información |
| | | A.13.2.3 Mensajería electrónica |
| | | A.13.2.4 Acuerdo de confidencialidad o de no divulgación |
| **A.14** | **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** | |
| | A.14.1 Requisitos de Seguridad de los Sistemas de Información | A.14.1.1 Análisis y especificaciones de los requisitos de seguridad de la información |
| | | A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas |
| | | A.14.1.3 Protección de las transacciones en servicios de aplicación |
| | A.14.2 Seguridad en los Procesos de Desarrollo y Soporte | A.14.2.1 Política de desarrollo seguro |
| | | A.14.2.2 Procedimientos de control de cambios del sistema |

| | | |
|---|---|---|
| | | |
| | | A.14.2.3 Revisión técnica de aplicaciones después de los cambios en la plataforma de operación |
| | | A.14.2.4 Restricciones a los cambios en los paquetes de software |
| | | A.14.2.5 Principios de ingeniería de sistemas seguros |
| | | A.14.2.6 Entorno de desarrollo seguro |
| | | A.14.2.7 Desarrollo contratado externamente |
| | | A.14.2.8 Pruebas de seguridad del sistema |
| | | A.14.2.9 Pruebas de aceptación del sistema |
| | A.14.3 Datos de Pruebas | A.14.3.1 Protección de datos de prueba |
| **A.15** | **RELACIONES CON LOS PROVEEDORES** | |
| | A.15.1 Seguridad de la Información en la Relación con los Proveedores | A.15.1.1 Política de seguridad de información para la relación con los proveedores |
| | | A.15.1.2 Abordar la seguridad dentro de acuerdos con proveedores |
| | | A.15.1.3 Cadena de suministro de tecnología de información y comunicaciones |
| | A.15.2 Entrega de servicios del proveedor | A.15.2.1 Monitoreo y revisión de los servicios de proveedores |
| | | A.15.2.2 Gestión de cambios de los servicios del proveedor |
| **A.16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | |
| | A.16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras | A.16.1.1 Responsabilidades y procedimientos |
| | | A.16.1.2 Informe de eventos de seguridad de información |
| | | A.16.1.3 Informes de debilidades de seguridad de información |
| | | A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información |

| | | |
|---|---|---|
| | | A.16.1.5 Respuesta a los incidentes de seguridad de información |
| | | A.16.1.6 Aprendiendo de los incidentes de seguridad de la información |
| | | A.16.1.7 Recolección de evidencia |
| **A.17** | **SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** | |
| | A.17.1 Continuidad de Seguridad de Información | A.17.1.1 Planificación de la continuidad de seguridad de información |
| | | A.17.1.2 Implementación de la continuidad de seguridad de información |
| | | A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información |
| | A.17.2 Redundancias | A.17.2.1 Instalaciones de procesamiento de la información |
| **A.18** | **CUMPLIMIENTO** | |
| | A.18.1 Cumplimiento de los Requisitos Legales y Contractuales | A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales |
| | | A.18.1.2 Derechos de propiedad intelectual |
| | | A.18.1.3 Protección de registros |
| | | A.18.1.4 Privacidad y protección de datos personales |
| | | A.18.1.5 Regulación de los Controles Criptográficos |
| | A.18.2 Revisiones de Seguridad de Información | A.18.2.1 Revisión independiente de seguridad de la información |
| | | A.18.2.2 Cumplimiento de las políticas y normas de seguridad |
| | | A.18.2.3 Revisión de cumplimiento técnico |

Tabla 28 Anexo A de ISO 27001.

Elaboración propia

### 5.3.2 Implementación de la Declaración de Aplicabilidad

**DECLARACIÓN DE APLICABILIDAD**

Luego de identificar los controles para los riesgos no aceptables para la ACFFAA, se detallará que controles aplican en la denominada Declaración de Aplicabilidad SOA (Ver tabla 29).

| Cláusula N° | Objetivos de Control | Control | Aplica SI/NO | Justificación de la Exclusión o Inclusión |
|---|---|---|---|---|
| **A.5** | **POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN** | | | |
| | A.5.1 Dirección de Gestión para la Seguridad de Información | A.5.1.1 Políticas de seguridad de información | **SI** | Requisito 5.2 de la ISO 27001:2013, otras políticas del SGSI. |
| | | A.5.1.2 Revisión de las políticas de seguridad de información | **SI** | Al ser un Sistema de Gestión debe soportar la Mejora Continua, es por ello por lo que se ha implementado los procedimientos necesarios para soportar la mejora en nuestras políticas, procedimientos e indicadores. |
| **A.6** | **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN** | | | |
| | A.6.1 Organización Interna | A.6.1.1 Funciones de seguridad de información y responsabilidades | SI | En la implementación del SGSI se ha visto la importancia de identificar Roles y Funciones para los diferentes involucrados. |
| | | A.6.1.2 Separación de funciones | **SI** | En la implementación del SGSI no solo se identificó Roles y Funciones, se ha cubierto las diferentes responsabilidades asociadas. |
| | | A.6.1.3 Contacto con autoridades | **SI** | Definir un flujo de comunicación con las personas identificadas como autoridades y grupos de interés es vital en la organización del SGSI. |

| | | | | |
|---|---|---|---|---|
| | | A.6.1.4 Contacto con grupos de interés especial | **SI** | Definir un flujo de comunicación con las personas especializadas en el sector para incrementar el conocimiento sobre las mejores prácticas en seguridad de la información y temas relacionados |
| | | A.6.1.5 Seguridad de información en gestión de proyectos | **SI** | Permitirá determinar los riesgos de seguridad de la información en los proyectos que puedan afectar la confidencialidad, disponibilidad e integridad de la información. |
| | A.6.2 Equipos Móviles y trabajo a distancia | A.6.2.1 Política de los equipos móviles | **SI** | Permitirá controlar los diversos dispositivos móviles que se entregan a los servidores de la ACFFAA |
| | | A.6.2.2 Trabajo a distancia | **SI** | Permitirá controlar las labores a distancia que realiza el personal |
| **A.7** | **SEGURIDAD DE LOS RECURSOS HUMANOS** | | | |
| | A.7.1 Antes del Empleo | A.7.1.1 Selección | **SI** | Se ha solicitado a Recursos Humanos incluir en la política de Selección de Personal, la verificación de Antecedentes Policiales, Judiciales y/o Penales. |
| | | A.7.1.2 Términos y condiciones de empleo | **SI** | Se cuenta con un acuerdo de confidencialidad que firman todos los trabajadores al momento de ingresar a la organización. Para los proveedores el acuerdo de confidencialidad se encuentra suscrito como cláusula en los contratos. |
| | A.7.2 Durante el Empleo | A.7.2.1 Responsabilidades de la gerencia | **SI** | Requisito 5.1 de la ISO 27001:2013 |
| | | A.7.2.2 Conciencia de seguridad de información, educación y capacitación | **SI** | Se cuenta con el documento Plan de Capacitaciones SGSI para el monitoreo de las capacitaciones al equipo de Seguridad de la Información |
| | | A.7.2.3 Proceso disciplinario | **SI** | Se ha establecido un proceso disciplinario para los servidores que incumplan la política de Seguridad de la Información |
| | A.7.3 Términos y Cambio de Empleo | A.7.3.1 Término o cambio de las responsabilidades de | **SI** | Asegurar el cumplimiento de responsabilidades de seguridad de la información |

| | | | | |
|---|---|---|---|---|
| | | empleo | | en la rotación, cese y/o término del servicio del personal de la organización y/o terceros. |
| **A.8** | **GESTIÓN DE ACTIVOS** | | | |
| | A.8.1 Responsabilidad por Activos | A.8.1.1 Inventario de activos | **SI** | Se ha realizado un inventario de activos de la información. |
| | | A.8.1.2 Propiedad de activos | **SI** | Se identificó a los propietarios de los activos de información |
| | | A.8.1.3 Uso aceptable de activos | **SI** | Asignar responsabilidad para la protección adecuada de los activos de la organización |
| | | A.8.1.4 Retorno de activos | **SI** | Asegurar que los servidores y/o terceros devuelvan todos los activos asignados de la organización una vez terminado su empleo y/o contrato |
| | A.8.2 Clasificación de la Información | A.8.2.1 Clasificación de información | **SI** | Asignar la clasificación de la información para su protección |
| | | A.8.2.2 Etiquetado de información | **SI** | Es necesario establecer procedimientos para el etiquetado de información y los activos relacionados |
| | | A.8.2.3 Manejo de activos | **SI** | Asignar responsabilidad para la protección adecuada de los activos de la organización |
| | A.8.3 Manejo de Medios | A.8.3.1 Gestión de medios removibles | **SI** | Controlar y proteger adecuadamente los medios removibles contra la divulgación, eliminación o modificación no autorizada |
| | | A.8.3.2 Disposición de medios | **SI** | Controlar y proteger adecuadamente los medios removibles contra la divulgación, eliminación o modificación no autorizada |
| | | A.8.3.3 Transferencia de medios físicos | **SI** | Asignar responsabilidad para la transferencia de medios físicos |
| **A.9** | **CONTROL DE ACCESOS** | | | |
| | A.9.1 Requisitos de Negocio para el Control de Acceso | A.9.1.1 Política de control de acceso | **SI** | Controlar el nivel de acceso para el uso adecuado de los activos y recursos de información |
| | | A.9.1.2 Acceso a redes y servicios de red | **SI** | Prevenir el acceso no autorizado a los equipos informáticos y sistemas de información |
| | A.9.2 Gestión de Acceso de Usuario | A.9.2.1 Registro y baja de usuarios | **SI** | Prevenir el acceso no autorizado a los equipos informáticos y sistemas de información |
| | | A.9.2.2 Provisión del acceso de usuario | **SI** | Asignar responsabilidad para el aprovisionamiento de acceso a usuarios |

| | | | | |
|---|---|---|---|---|
| | | A.9.2.3 Gestión de derechos de acceso privilegiados | **SI** | Prevenir el acceso no autorizado a los equipos informáticos y software |
| | | A.9.2.4 Gestión de la información de autenticación secreta de los usuarios | **SI** | Prevenir el acceso no autorizado a la información considerada como confidencial |
| | | A.9.2.5 Revisión de derechos de acceso de usuarios | **SI** | Prevenir el acceso no autorizado a los equipos informáticos y software de aplicación |
| | | A.9.2.6 Eliminación o ajuste de derechos de acceso | **SI** | Asegurar el retiro de los derechos de acceso de los servidores y/o terceros una vez concluido su empleo y/o contrato |
| | A.9.3 Responsabilidades de Usuarios | A.9.3.1 Uso de información de autenticación secreta | **SI** | Prevenir el acceso no autorizado a la información considerada como confidencial |
| | A.9.4 Control de Acceso a sistema y aplicación | A.9.4.1 Restricción de acceso a la información | **SI** | Prevenir el acceso no autorizado a los equipos informáticos y software |
| | | A.9.4.2 Procedimientos seguros de inicio de sesión | **SI** | |
| | | A.9.4.3 Sistema de gestión de contraseña | **SI** | |
| | | A.9.4.4 Uso de programas utilitarios privilegiados | **SI** | Prevenir los cambios no autorizados sobre los paquetes de software |
| | | A.9.4.5 Control de acceso al código fuente de los programas | **SI** | Restringir el accesos lógicos al código fuente de los programas y/o aplicaciones de la organización |
| **A.10** | **CRIPTOGRAFIA** | | | |
| | A.10.1 Controles criptográficos | A.10.1.1 Política de uso de los controles criptográficos | Si | La organización tiene implementado certificados digitales para sus aplicaciones públicas (HTTPS) |
| | | A.10.1.2 Gestión de claves | SI | |
| **A.11** | **SEGURIDAD FÍSICA Y AMBIENTAL** | | | |
| | A.11.1 Áreas de Seguridad | A.11.1.1 Perímetro de seguridad física | **SI** | Identificar los ambientes, donde se procese o almacene información |
| | | A.11.1.2 Controles de entrada física | **SI** | Asegurar los ambientes, donde se procese o almacene información, del ingreso y/o trabajos realizados por servidores y/o terceros. |
| | | A.11.1.3 Seguridad de oficinas, salas | **SI** | |

| | | | | |
|---|---|---|---|---|
| | | A.11.1.4 Protección contra amenazas externas y ambientales | **SI** | |
| | | A.11.1.5 Trabajo en áreas seguras | **SI** | |
| | | A.11.1.6 Áreas de despacho y carga | **NO** | La ACFFAA no cuenta con área de despacho y carga |
| | A.11.2 Equipos | A.11.2.1 Situar los equipo y protección | **SI** | Protección de los activos usados en el procesamiento de la información |
| | | A.11.2.2 Servicios públicos de apoyo | **SI** | Los equipos deben estar protegidos contra fallas de electricidad y otras alteraciones causadas por fallas en los servicios de suministros |
| | | A.11.2.3 Seguridad del cableado | **SI** | El cableado debe ser revisado para garantizar su funcionamiento |
| | | A.11.2.4 Mantenimiento de los equipos | **SI** | Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad. |
| | | A.11.2.5 Retiro de los activos | **SI** | Se cuenta con autorización formal para el retiro de activos físico y lógicos. |
| | | A.11.2.6 Seguridad de los equipos y de los activos fuera de las instalaciones | **SI** | Protección de los activos usados en el procesamiento de la información |
| | | A.11.2.7 Eliminación segura o reúso de equipos | **SI** | Protección de los activos usados en el procesamiento de la información |
| | | A.11.2.8 Equipos de usuarios no atendidos | **SI** | Asegurar que los equipos desatendidos se encuentran debidamente protegidos |
| | | A.11.2.9 Política de escritorio y pantalla limpia | **SI** | Proteger los recursos de procesamiento de información |
| **A.12** | **SEGURIDAD DE LAS OPERACIONES** | | | |
| | A.12.1 Procedimientos y Responsabilidades operativas | A.12.1.1 Procedimientos de operación documentados | **SI** | Uso adecuado de los recursos y sistemas de información |
| | | A.12.1.2 Gestión de cambio | **SI** | Controlar los cambios en los sistemas y los recursos de tratamiento de información |
| | | A.12.1.3 Gestión de capacidad | **SI** | Gestionar la capacidad de los sistemas de información y proyecciones futuras para asegurar su disponibilidad |

| | | | | |
|---|---|---|---|---|
| | | A.12.1.4 Separación de los entornos de desarrollo, pruebas y operaciones | **SI** | Los ambientes de Desarrollo, Prueba y Producción cuentan con el nivel de separación necesario para prevenir problemas operacionales, así como los controles de acceso adecuados para cada uno de ellos. |
| | A.12.2 Protección contra Malware | A.12.2.1 Control contra malware | **SI** | Proteger el software y equipos informáticos para prevenir y detectar la propagación de código malicioso |
| | A.12.3 Respaldo | A.12.3.1 Copia de información | **SI** | Asegurar la realización de respaldos y pruebas de restauración de la información crítica |
| | A.12.4 Registro y Monitoreo | A.12.4.1 Registro de eventos | **SI** | Los eventos son registrados y monitoreados |
| | | A.12.4.2 Protección de información de registro | **SI** | Monitorear y registrar la ejecución de actividades de procesamiento de información |
| | | A.12.4.3 Registros de administrador y operador | **SI** | Las actividades son registradas y protegidas y se almacenan en el log de auditoría del sistema. |
| | | A.12.4.4 Sincronización de reloj | **SI** | Se cuenta con servidores confiables para la sincronización de reloj. |
| | A.12.5 Control del Software Operativo | A.12.5.1 Instalación de software en sistemas operacionales | **SI** | Restringir y controlar la utilización de programas y/o aplicaciones instaladas en los equipos informáticos |
| | A.12.6 Gestión de Vulnerabilidad Técnica | A.12.6.1 Gestión de vulnerabilidades técnicas | **SI** | Obtener información oportuna de nuevas vulnerabilidades y evaluar el nivel de exposición de las aplicaciones de la organización |
| | | A.12.6.2 Restricciones en la instalación de software | **SI** | Restringir y controlar la utilización de programas y/o aplicaciones instaladas en los equipos informáticos |
| | A.12.7 Consideraciones para la Auditoría de Sistemas de Información | A.12.7.1 Controles de auditoría de sistemas de información | **SI** | Brindar protección a los sistemas de información y herramienta de auditoría |
| **A.13** | **SEGURIDAD DE LAS COMUNICACIONES** | | | |
| | A.13.1 Gestión de Seguridad de Redes | A.13.1.1 Controles de redes | **SI** | Gestionar y controlar de forma adecuada la infraestructura de red. |
| | | A.13.1.2 Seguridad de los servicios de redes | **SI** | |

| | | | | |
|---|---|---|---|---|
| | | A.13.1.3 Separación en redes | **SI** | Segmentar las redes y servicios de información de acuerdo con la criticidad de la información almacenada |
| | A.13.2 Transferencia de Información | A.13.2.1 Procedimientos y políticas de transferencia de información | **SI** | Proteger el intercambio de información con otras instituciones |
| | | A.13.2.2 Acuerdos sobre transferencia de información | **SI** | |
| | | A.13.2.3 Mensajería electrónica | **SI** | |
| | | A.13.2.4 Acuerdo de confidencialidad o de no divulgación | **SI** | Los servidores de la ACFFAA y terceros deben firmar un acuerdo de confidencialidad |
| **A.14** | **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS** | | | |
| | A.14.1 Requisitos de Seguridad de los Sistemas de Información | A.14.1.1 Análisis y especificaciones de los requisitos de seguridad de la información | **SI** | Establecer requisitos de seguridad como parte de las especificaciones para los nuevos sistemas de información |
| | | A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas | **SI** | Establecer requisitos de seguridad para las aplicaciones y servicios en redes públicas |
| | | A.14.1.3 Protección de las transacciones en servicios de aplicación | **SI** | Proteger la información implicada de los servicios de aplicación ante la duplicación o repetición del mensaje no autorizado |
| | A.14.2 Seguridad en los Procesos de Desarrollo y Soporte | A.14.2.1 Política de desarrollo seguro | **SI** | Establecer requisitos de seguridad como parte de las especificaciones para el desarrollo de software |
| | | A.14.2.2 Procedimientos de control de cambios del sistema | **SI** | Establecer procedimientos formales de control de cambios para prevenir los cambios no autorizados a las aplicaciones |
| | | A.14.2.3 Revisión técnica de aplicaciones después de los cambios en la plataforma de operación | **SI** | Establecer revisiones en aplicaciones críticas para asegurar que los cambios establecidos no impacten negativamente en la operación |
| | | A.14.2.4 Restricciones a los cambios en los paquetes de software | **SI** | Prevenir los cambios no autorizados sobre los paquetes de software |
| | | A.14.2.5 Principios de ingeniería de | **SI** | Establecer requisitos de seguridad como parte de las |

| | | | | |
|---|---|---|---|---|
| | | sistemas seguros | | especificaciones para los nuevos sistemas de información, análisis de riesgos y amenazas potenciales |
| | | A.14.2.6 Entorno de desarrollo seguro | **SI** | Proteger los datos de pruebas para evitar la pérdida de la confidencialidad de datos sensibles de la organización |
| | | A.14.2.7 Desarrollo contratado externamente | **SI** | La institución contrata proveedores para el desarrollo de software. |
| | | A.14.2.8 Pruebas de seguridad del sistema | **SI** | Obtener información oportuna de nuevas vulnerabilidades y evaluar el nivel de exposición de las aplicaciones de la organización |
| | | A.14.2.9 Pruebas de aceptación del sistema | **SI** | Validar los datos de entrada de las aplicaciones para asegurar que sean procesados correctamente |
| | A.14.3 Datos de Pruebas | A.14.3.1 Protección de datos de prueba | **SI** | Proteger los datos de pruebas para evitar la pérdida de la confidencialidad de datos sensibles de la organización |
| **A.15** | **RELACIONES CON LOS PROVEEDORES** | | | |
| | A.15.1 Seguridad de la Información en la Relación con los Proveedores | A.15.1.1 Política de seguridad de información para la relación con los proveedores | **SI** | Establecer los lineamientos de Seguridad de la Información con los proveedores |
| | | A.15.1.2 Abordar la seguridad dentro de acuerdos con proveedores | **SI** | Proteger la información de la Organización de los servicios prestados por los proveedores |
| | | A.15.1.3 Cadena de suministro de tecnología de información y comunicaciones | **SI** | |
| | A.15.2 Entrega de servicios del proveedor | A.15.2.1 Monitoreo y revisión de los servicios de proveedores | **SI** | |
| | | A.15.2.2 Gestión de cambios de los servicios del proveedor | **SI** | |
| **A.16** | **GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN** | | | |
| | A.16.1 Gestión de Incidentes de Seguridad de la Información y Mejoras | A.16.1.1 Responsabilidades y procedimientos | **SI** | Establecer las responsabilidades y procedimientos que permitan el reporte de manera oportuna de los eventos de Seguridad de la Información |

| | | | | |
|---|---|---|---|---|
| | | A.16.1.2 Informe de eventos de seguridad de información | **SI** | Asegurar que se reporten de manera oportuna los eventos de Seguridad de la Información |
| | | A.16.1.3 Informes de debilidades de seguridad de información | **SI** | |
| | | A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información | **SI** | |
| | | A.16.1.5 Respuesta a los incidentes de seguridad de información | **SI** | |
| | | A.16.1.6 Aprendiendo de los incidentes de seguridad de la información | **SI** | |
| | | A.16.1.7 Recolección de evidencia | **SI** | |
| **A.17** | **SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO** | | | |
| | A.17.1 Continuidad de Seguridad de Información | A.17.1.1 Planificación de la continuidad de seguridad de información | **SI** | Protección de los activos de información ante diversos escenarios que comprometan la continuidad de las operaciones de la ACFFAA |
| | | A.17.1.2 Implementación de la continuidad de seguridad de información | **SI** | |
| | | A.17.1.3 Verificar, revisar y evaluar la continuidad de seguridad de la información | **SI** | |
| | A.17.2 Redundancias | A.17.2.1 Instalaciones de procesamiento de la información | **SI** | Asegurar la disponibilidad de los sistemas de información |
| **A.18** | **CUMPLIMIENTO** | | | |
| | A.18.1 Cumplimiento de los Requisitos Legales y Contractuales | A.18.1.1 Identificación de la legislación aplicable y los requisitos contractuales | **SI** | Cumplir los requisitos legales, reglamentarios o contractuales a los que está obligado la organización |
| | | A.18.1.2 Derechos de propiedad intelectual | **SI** | Cumplir los requisitos legales, reglamentarios o contractuales a los que está obligado la organización |
| | | A.18.1.3 Protección de registros | **SI** | Brindar protección a los sistemas de información y herramienta de auditoría |

| | | | | |
|---|---|---|---|---|
| | | A.18.1.4 Privacidad y protección de datos personales | **SI** | Cumplimiento regulatorio respecto a la Ley de Protección de Datos Personales |
| | | A.18.1.5 Regulación de los Controles Criptográficos | **SI** | La organización establecerá normativas referente a criptografía. |
| | A.18.2 Revisiones de Seguridad de Información | A.18.2.1 Revisión independiente de seguridad de la información | **SI** | Se realizan revisiones a las políticas, procedimientos, directivas para verificar su cumplimiento |
| | | A.18.2.2 Cumplimiento de las políticas y normas de seguridad | **SI** | Cumplir con los requisitos legales, reglamentarios o contractuales |
| | | A.18.2.3 Revisión de cumplimiento técnico | **SI** | Verificar el cumplimiento técnico con las normas de implementación de seguridad de los sistemas de información |

Tabla 29 Declaración de Aplicabilidad –

Elaboración Propia

## 5.3 Pruebas bajo el método GAP (Análisis de Brecha)

Las pruebas bajo el método GAP, también conocido como Análisis de Brecha, implementar los cambios recomendados es crucial para mejorar y alinearse con los objetivos. Se deberá tener claro qué esperar encontrar y cuáles son las metas. Las pruebas GAP ayudan a descubrir las diferencias entre el rendimiento esperado y el real. Estas diferencias son las "brechas".

### 5.3.1 ANÁLISIS DE BRECHA

Se realizó un estudio previo en la Oficina de Informática, identificándose que ningún control había sido aplicado de acuerdo con la norma ISO 27001 con los documentos y requisitos de acuerdo con las cláusulas correspondientes por lo tanto se encuentra actualmente en un porcentaje de 0% del nivel de Madurez (Véase Tabla 30).

### 5.3.2 NIVEL DE MADUREZ

El nivel de madurez en la implementación de un SGSI pasa por varias etapas, desde los cimientos hasta una fortaleza digital impenetrable,

siempre evolucionando y mejorando para enfrentar las crecientes amenazas digitales con Niveles del 1 al 5 (Ver tabla 30 y 31).

| Nivel | Porcentaje | Descripción | Característica |
|---|---|---|---|
| **0** | **0%** | **No existente** | No existe la aplicación de un control. |
| **1** | **20%** | **Inicial** | Inicio de implementación del control. |
| **2** | **40%** | **Implementado Parcial** | Se ha implementado el control y las responsabilidades Ha |
| **3** | **60%** | **Implementado Total** | Tiene el control implementado alineado con los programas de concientización en seguridad. |
| **4** | **80%** | **Probado** | Se realizan periódicamente análisis con el fin de mejorar la eficiencia del control |
| **5** | **100%** | **Optimizado** | Se realizan periódicamente de costo/beneficio para futuros cambios o mejoras de control. Puede impactar en objetivos estratégicos a nivel de Ti o negocio. |

Tabla 30 Nivel de Madurez - Elaboración Propia

| Nivel 0 | Nivel 1 | Nivel 2 | Nivel 3 | Nivel 4 | Nivel 5 |
|---|---|---|---|---|---|
| **No existente** | Inicial | Repetible pero intuitivo | Proceso definido | Gestionable y medible | Optimizado |
| **0%** | **20%** | **40%** | **60%** | **80%** | **100%** |
| **Nivel de Madurez Alcanzado** | | | | | |

Tabla 31 Porcentaje según Niveles.

Elaboración Propia.

### 5.3.3 TABLA DE CUMPLIMIENTO

Imagina que estás diseñando un mapa para asegurar la fortaleza digital de tu organización. La tabla de cumplimiento en la propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO 27001 es como ese mapa. En la siguiente tabla se verifican los campos: cláusula, nombre y Porcentaje de cumplimiento. (Ver tabla 32).

| CLAUSULA | NOMBRE | PORCENTAJE DE CUMPLIMIENTO |
|---|---|---|
| **4** | CONTEXTO DE LA ORGANIZACIÓN | |
| **5** | LIDERAZGO | |
| **6** | PLANIFICACIÓN | |
| **7** | SOPORTE | |
| **8** | OPERACIÓN | |
| **9** | EVALUACION DEL DESEMPEÑO | |
| **10** | MEJORAS | |

Tabla 32 Tabla de Cumplimiento – Elaboración Propia

# VI. DISCUSIÓN DE RESULTADOS

## 6.1 Contrastación y demostración de la hipótesis con los resultados.

Los resultados respaldan la hipótesis de que la implementación de la norma ISO en la agencia de compras mejorará la eficiencia y la calidad de los procesos, ya que una vez que ésta sea implementada tendrá que pasar por un proceso de auditoría que ameritará la certificación internacional, para ello se deberá tener en cuenta lo siguiente, según la fuente de la página de (secureframe):

- La ISO 27001 no emite un certificado específico para validar el éxito de la implementación de una organización. No obstante, existen medidas y procedimientos que una entidad puede seguir para demostrar eficacia en la implementación.

- Certificación ISO 27001: Buscar la certificación a través de organismos reconocidos implica una auditoría exhaustiva para asegurar que la implementación cumple con los requisitos de la norma.

- Auditorías Internas: Realizar auditorías internas periódicas permite evaluar continuamente el rendimiento del Sistema de Gestión de Seguridad de la Información (SGSI), sirviendo como indicador de efectividad y conformidad con ISO 27001.

- Seguimiento de Indicadores de Desempeño: Establecer y monitorear regularmente indicadores clave de desempeño relacionados con la seguridad de la información proporciona evidencia tangible de la eficacia de la implementación.

- Documentación Adecuada: Mantener documentación clara y completa, incluyendo políticas, procedimientos y registros del SGSI,

actúa como prueba tangible de una implementación exitosa.

- Es vital reconocer que la ISO 27001 implica un proceso continuo de mejora. La verificación exitosa no es un evento puntual, sino un compromiso constante con la seguridad de la información.

## 6.2 Contrastación de los resultados con otros estudios similares.

(Jacome Sanchez, 2022)en su tesis " Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001, para optar por el grado de Tesis de Maestría ", destacó que, aunque la implementación de todos los controles no es obligatoria, es crucial argumentar la no aplicabilidad de aquellos que no se implementan. Recomendó la aplicación del Ciclo Planificar - Ejecutar - Verificar - Actuar para el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI). En nuestra investigación, se propone la implementación de todos los controles utilizando la norma ISO 27001.

(Silva Guerrero, 2018), en su tesis “Propuesta de análisis y diseño de un sistema de gestión de seguridad de la información basado en la ISO/IEC 27001, para el proceso de ventas de la empresa “Energía Perú S.A.C.” ", resaltó la importancia de la Protección de Datos. Enfatizó la obligación de las empresas de mantener en secreto la información. Similarmente, en nuestro caso, se subraya la necesidad de mantener en secreto la información de los procesos internos de la Agencia de Compras de las Fuerzas Armadas del Perú.

## 6.3 Responsabilidad ética de acuerdo con los reglamentos vigentes (el autor de la investigación se responsabiliza por la información emitida en el informe)

Se adhiere a los reglamentos éticos vigentes, garantizando la integridad de la información presentada en el informe.

# VII. CONCLUSIONES

a) En resumen, se propone la implementación de un Sistema de Gestión de Seguridad de la Información aplicando la Norma ISO/IEC 27001. Se mantiene una metodología de mejora continua, esencial para ejecutar buenas prácticas alineadas con la ISO/IEC 27001, recomendadas para garantizar la Confidencialidad, Integridad y Disponibilidad de la información en los procesos y subprocesos institucionales.

b) Para asegurar el éxito, se destaca la importancia de obtener la aprobación de la Alta Gerencia. Su apoyo es crucial para la implementación del Sistema de Gestión, ya que, sin su intervención, la ejecución del SGSI sería inviable. Además, se subraya la concientización de los responsables del área y del proceso, participantes en las entrevistas de levantamiento de información.

c) Asimismo, se enfatiza la identificación de los activos de información y la comprensión de que la seguridad tiene como propósito resguardar dichos activos. Durante la evaluación del riesgo, se verifica que no existe seguridad absoluta; ningún sistema es 100% seguro, ya que el riesgo está presente en todos los procesos.

d) La valoración de los activos se realiza según un rango y criterio determinado. Los activos de mayor rango tienen un valor de criterio, y aquellos con criterio alto y mediano pasan a la evaluación de riesgos. Se protegen los activos de mayor valor de impacto para evitar consecuencias graves para la institución.

e) La evaluación de riesgo identifica que 100% de riesgo extremo representa el mayor porcentaje, con un impacto significativo en la reputación de la institución y costos elevados para la recuperación de activos y recursos.

f) Finalmente, se subraya la obligatoriedad del compromiso de la Alta Gerencia y la asignación de un fondo remunerativo dirigido a la implementación de controles del SGSI. Además, se destacan las formaciones de concientización y otras actividades dentro de la institución para garantizar la continuidad del sistema.

# VII. RECOMENDACIONES

a) Aprovechar la mejora continua para afianzar la cultura de seguridad. A fin de garantizar la sostenibilidad del SGSI y su arraigo en la institución, se recomienda capitalizar la metodología de mejora continua para evolucionar de un enfoque reactivo a uno proactivo en materia de seguridad de la información.

b) Se sugiere involucrar activamente a la alta gerencia en el despliegue del Sistema de Gestión de Seguridad de la Información. Para asegurar la comprensión y participación del personal institucional en la implementación del SGSI, es esencial llevar a cabo entrenamientos y programas de concientización de manera constante, utilizando diversas metodologías pedagógicas.

c) A pesar de que no existe un sistema 100% seguro, es fundamental implementar medidas de seguridad adecuadas para proteger los activos de información de la organización. Esto implica identificar y clasificar los activos de información, evaluar los riesgos a los que están expuestos, e implementar controles para mitigar esos riesgos.

d) Se recomienda realizar una valoración exhaustiva de los activos de información para identificar, clasificar y priorizar aquellos que requieren mayor protección. Esto permitirá enfocar los esfuerzos de seguridad en los activos más críticos y reducir el riesgo de incidentes de seguridad.

e) Dada la alta probabilidad de riesgos extremos que podrían afectar la reputación de la institución y generar costos elevados en la recuperación de activos y recursos, se recomienda enfocar los esfuerzos de seguridad en mitigar estos riesgos críticos

f) Se recomienda asegurar el compromiso explícito de la Alta Gerencia con el SGSI, asignando recursos financieros y humanos para su implementación efectiva.

# IX. REFERENCIAS BIBLIOGRACIAS

## Bibliografía


1. **ALVAREZ ZURITA, Flor María y GARCÍA GUZMAN, Pamela Anabel.** *IMPLEMENTACION DE UN SISGS "TESISI PARA OBTAR PARA EL TÍTULO DE INGENIERO DE SISTEMAS DE LA UNIVERSIDAD DE ECUADOR".*
2. **Ampuero, Chang. 2011.** *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros.* 2011.
3. **Arango, Paula Andrea Maya. 2016.** *PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013.* España : s.n., 2016.
4. **Brocca Castillo, Cesar Augusto. 2019.** *Sistema de gestión de seguridad de la información basado en la ISO/IEC 27001:2014 en un establecimiento de salud.* 2019.
5. **Burga Segovia, Jorge. 2022.** *Diseño de un sistema de Gestion de la seguridad de la Informacion (SGSI) para Edpyme Credivision, basado en la Norma ISO 27001:2013.* 2022.
6. **—. 2022.** *Diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI) Para Edpyme Credivisión, basado en la Norma ISO 27001:2013.* 2022.
7. **Cabrera Cubas, Henry Percy. 2018.** *Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazona.* 2018.
8. **Carol Estalla, Máximo Morales. 2023.** DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE INFORMACIÓN. Lima : s.n., 2023.
9. **Carvajal, D. L., Cardona, A. y Valencia, F. J. 2021.** *UNA PROPUESTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APLICADO A UNA ENTIDAD PÚBLICA COLOMBIANA.* 2021.
10. **Cazco, Rafael. 2016.** *Propuesta de implementación de un SGSI basado en la norma ISO 27001. (Caso práctico Universidad de El Salvador).* El Salvador : s.n., 2016.
11. **Center. 2014.** *ISO 27001: de qué se trata y cómo implementarla.* s.l. : https://www.piranirisk.com/es/academia/especiales/iso-27001-que-es-y-como-implementarla, 2014.
12. **Chang, Ampuero. 2011.** *Diseño de un sistema de gestión de seguridad de información para una compañía de seguros.* 2011.
13. **Chuna Chinga, Gerson Isaac Luciano. 2018.** *Propuesta de un sistema de gestión de seguridad de la información basado en la NTP ISO/IEC 27001:2014 para la DRTPE - filial Piura" , Tesis para obtener el grado de título de Ingeniería de Sistemas.* Piura, Lima, Perú : s.n., 2018.
14. **Coaguila Mamani, Maribel Estela. 2020.** *Diseño de un plan de gestión de seguridad de información alineado a la norma ISO/IEC 27001: Caso Universidad Nacional de Moquegua.* 2020.
15. **Cornejo Miranda, Alex Jhonatan y Lezama Calvo, Arturo Ramón. 2022.** *Propuesta de sistema de gestión de seguridad de la Información para garantizar la seguridad de la información en la sub gerencia de tecnología*

*de la información del Gobierno regional de La Libertad.* 2022.
16. **Cosios Avila, Tania Verónica. 2021.** *Implementación de auditoría informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; 2020.* 2021.
17. *DESARROLLO DE UN SISTEMA DE GESTIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN BASADO EN METODOLOGÍA DE IDENTIFICACIÓN Y ANÁLISIS DE RIESGO EN BIBLIOTECAS UNIVERSITARIAS.* **Harold, Díaz, Jorge L. y Patiño, Janns. 2021.** 2021.
18. *DISEÑO E IMPLEMENTACIÓN DE UN SGSI ISO 27001 PARA LA MEJORA DE LA SEGURIDAD DEL AREA DE RECURSOS HUMANOS DE LA EMPRESA GEOSURVEY DE LA CIUDAD DE LIMA.* **Vilca Mosquera, Ehytel Celestino. 2016.** 2016.
19. **Echevarría, Luis Romero. 2005.** *Marco conceptual de los Delitos Informáticos.* 2005.
20. **Empresarial. 2016.** 2016.
21. **Flores Barrios, M. C. Leonardo, y otros. 2011.** *EVALUACIÓN DEL IMPACTO DE LOS SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BAJO LA SERIE ISO/IEC 27001 EN EMPRESAS DE LA CIUDAD DE TUXPAN, VERACRUZ.* VERACRUZ, MÉXICO : Revista de la Alta tecnología y sociedad, 2011.
22. **Francisco Javier Valencia-Duque 1, Mauricio Orozco-Alzate. 2017.** *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.* Colombia : Universidad Nacional de Colombia – Sede Manizales, 2017.
23. **G, Alexander. 2007.** *Sistema de Gestión de Seguridad de Información (SGSI) Basado en la Norma ISO/IEC27001 para mejorar la Seguridad del Área de Operaciones y Tecnología de Global BPO Center Allus Chiclayo .* 2007.
24. **Garcia Cruz, ROdolfo Augusto. 2020.** *Propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de Tecnologías de Información del gobierno regional Piura; 2020.* 2020.
25. **Giap, Risco Villarreal Eduardo. 2021.** *Sistema de gestión para la seguridad de la información basado en la Norma ISO/IEC 27001:2013 en la Empresa Constructora Pérez & Pérez SAC, Moyobamba, San Martín, 2021.* 2021.
26. **Hidalgo Narváez, Mónica Patricia. 2022.** *Influencia de un modelo del SGSI (norma ISO/IEC 27001:2013) en la eficacia de la administración de los recursos públicos. registro de la propiedad y mercantil del Cantón Pedro Moncayo, períodos 2019, 2020 y 2021.* 2022.
27. **Ibarra Caqui, Lucio. 2023.** *ISO 27001:2013 para la gestión del manejo de información en la UGEL Bolognesi, Ancash 2023.* 2023.
28. **—. 2023.** *La Implementación ISO 27001:2013 En La Gestión Del Manejo De Información En La UGEL Bolognesi Ancash 2023.* 2023.
29. **Isabel, Martha. 2011.** ISO 27001. Colombia : s.n., 2011.
30. **Jacome Sanchez, Alex Paul. 2022.** *Diseño de una propuesta sobre la aplicación de un SGSI para la empresa de transporte la Ecuatoriana bajo la norma ISO 27001, para obtar por el grado de Tesis de Maestría.* Ecuador : NEUMANN-Institucional, 2022.
31. **LOPEZ, Guillermo Roldan. 2016.** *Propuesta de un Sistema de Gestión de la Seguridad de la Información para organizaciones en Costa Rica.* Costa

Rica : ULACIT, 2016.
32. **Lopéz, Ricardo Alfredo. 2017.** Sistema de Gestión de la Informacion. Bogota : s.n., 2017.
33. **Luna Castillo, Henry Wiley. 2019.** *Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en la seguridad de la información en la Municipalidad Provincial de Recuay - 2015.* 2019.
34. **Martinez, García. 2006.** *Proyecto CAMERSEC - Implantación de Sistemas de Gestión de Seguridad de la Información en PYMES.* Perú : s.n., 2006.
35. **Mejía. 2014.** 2014.
36. **Neill, David Alan. 2017.** *Procesos y Fundamentos de la Investigación Científica.* s.l. : UTMACH, 2017.
37. **Nizo Mesa, David Steven. 2023.** *Propuesta para implementar el SGSI basada en la norma ISO 27001:2022 para la empresa ARIA PSW.* Bogotá, Colombia : s.n., 2023.
38. **Raúl J. Martelo, Jhonny E. Madera y Andrés D. Betín. 2015.** *Componente Modular del Sistema de Gestión de Seguridad de la Información (SGSI).* Cartagena-Colombia : La Serena, 2015.
39. **ROCHA CAHUEÑAS, Carlos David. 2019.** *MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR PÚBLICO Explotación de vulnerabilidades y análisis brecha de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en un proceso estratégico.* Quito : s.n., 2019.
40. **Rodriguez Baca, Liset Sulay, Cruzado Puente de la Vega, Carlos Francisco, Mejía Corredor, Carolina, Alarcón Diaz, Mitchell Alberto. 2020.** *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana.* 2020.
41. **Salamanca, Oscar. 2016.** *Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software.* Venezuela : Revista Venezolana de Información, Tecnología y Conocimiento, 2016. Vol. 13 Issue 3, p114-130.
42. **Sampieri, Roberto Hernandez.** *Metodología de la Inestigación.*
43. **Sandoval Alania, Jose Carlos. 2020.** *Propuesta de diseño de un sistema de gestión de seguridad de la información basado en la NTP-ISO/IEC 27001 para la Dirección Regional de Trabajo y Promoción del Empleo - Huánuco.* Huánuco, Perú : s.n., 2020.
44. **secureframe.** secureframe.com. *The ISO 27001 Certification Process: A Step-by-Step Guide.* [En línea] https://secureframe.com/hub/iso-27001/certification-process:.
45. **Silva Guerrero, Alex Richar. 2018.** *Propuesta de análisis y diseño de un sistema de gestión de seguridad de la información basado en la ISO/IEC 27001, para el proceso de ventas de la empresa "Energía Perú S.A.C.".* Perú : s.n., 2018.
46. **Standardization, International Organization for. 2022.** *Seguridad de la información, ciberseguridad y protección de la privacidad - Sistemas de gestión de la seguridad de la información - Requisitos.* SUIZA : ISO/IEC 2022 - Aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros , 2022.
47. **Sussy, Bayona, y otros. 2015.** *Implementación de la NTP ISO/IEC 27001 en las.* Perú : Conferência Ibérica de Sistemas e Tecnologias de Informação, 2015. Vol. 1, p410-415.
48. **Venemedia. 2014.** 2014.
49. **Vilca Mosquera, Ehytel Celestino. 2016.** *DISEÑO E IMPLEMENTACIÓN*

# ANEXOS

## ANEXO 1 “MATRIZ DE CONSISTENCIA”

| PROBLEMA GENERAL | OBJETIVO GENERAL | HIPOTESIS GENERAL | VARIABLE | OPERACIONALIZACIÓN DE VARIABLE | | TIPO DE INVESTIGACIÓN |
|---|---|---|---|---|---|---|
| | | | | DIMENSIÓN | INDICADORES | |
| **PA:** ¿Se puede desarrollar un Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 para la Agencia de Compras de las Fuerzas Armadas, 2023? | **OA:** Desarrollar un Sistema de Gestión de Seguridad de la Información basado en la ISO 27001 para la Agencia de Compras de las Fuerzas Armadas, 2023. | **HA:** La ISO 27001 permitirá desarrollar un Sistema de Gestión de Seguridad de la Información para la Agencia de Compras de las Fuerzas Armadas, 2023. | **VARIABLE INDEPENDIENTE:**<br><br>Sistema de Gestión de Seguridad de la Información. | | Duración Operativa= Tiempo en Minutos/Días/Semanas<br><br>Nivel de Implementación = (Numero de Procesos Implementados/Total de Procesos)x100 | |
| **Problemas Específicos** | **Objetivos Específicos** | **Hipótesis Específicos** | | | | |
| **P1:** ¿Se puede identificar el estado situacional de los procesos existentes en la Agencia de Compras de las Fuerzas Armadas en el Área de TI (Tecnologías de Información) | **O1:** Identificar el estado situacional actual de los procesos existentes en la Agencia de Compras de las Fuerzas Armadas en el Área de TI (Tecnologías de Información) | **H1:** La ISO 27001 permitirá definir el estado situacional permitirá conocer como están definidos los procesos actualmente existentes en la Agencia de Compras de las Fuerzas Armadas, 2023. | **VARIABLE DEPENDIENTE:**<br><br>ISO 27001 | Número de Procesos Implementados | Procesos en Desarrollo = Número de Procesos Implementados a Medias<br><br>Índice de Riesgo = Probabilidad x Impacto | 1. BÁSICA<br>2. Pre-experimental<br>3. Aplicada |
| **P2:** ¿En los procesos existentes se puede planificar un análisis de brecha para identificar la confidencialidad del Sistema de Gestión de Seguridad de la Información en la ACFFAA? | **O2:** Planificar un análisis de brecha para identificar la confidencialidad del Sistema de Gestión de Seguridad de la Información en la ACFFAA. | **H2:** La ISO 27001 permitirá establecer la brecha o comparación que nos ayudará a ver exactamente cómo estamos protegiendo nuestros datos ahora y cómo deberíamos hacerlo con el nuevo sistema de seguridad planteado basado en la ISO 27001. | | Tiempo de duración de la Implementación del proceso | % de Cumplimiento de Requisitos de Seguridad = (Número de requisitos cumplidos / Número total de requisitos) * 100 | |
| **P3:** ¿Se puede identificar qué controles se puede implementar en el Sistema de Gestión de Seguridad de la Información para resguardar la confidencialidad, la disponibilidad e integridad en los procesos de la Agencia de Compras de las Fuerzas Armadas? | **O3:** Identificar qué controles de acuerdo con la ISO 27001 se puede implementar en el Sistema de Gestión de Seguridad de la Información para resguardar la confidencialidad, la disponibilidad e integridad en los procesos de la Agencia de Compras de las Fuerzas Armadas | **H3:** La ISO 27001 permitirá establecer controles y responsabilidades para desarrollar el Sistema de Gestión de Seguridad de la Información para la Agencia de Compras de las Fuerzas Armadas, 2023. | | | | |

Tabla 33 Matriz de Consistencia. Elaboración Propia.

# ANEXO 2 "CONSENTIMIENTO INFORMADO"

**CARTA DE AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA**

Yo **MANUEL SANTIAGO VÁSCONES MOREY**
identificado con DNI , en mi calidad de **JEFE DE LA AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS** del área de DESPACHO JEFATURAL de la empresa/institución **AGENCIA DE COMPRAS DE LAS FUERZAS ARMADAS**
con R.U.C N° **20556939781** ubicada en la ciudad de Av. AREQUIPA 310 - Lima - Perú

**OTORGO LA AUTORIZACIÓN,**

Al señor MÁXIMO JHONN MORALES MEDINA
identificado con DNI N° **43335670** , egresado de la (x) Carrera profesional o ( ) Programa de Postgrado de Ingeniería de Sistemas para
*(Nombre de la carrera o programa).*

que utilice la siguiente información de la empresa:

**ACTIVOS DE INFORMACIÓN**

*(Detallar la información a entregar)*

con la finalidad de que pueda desarrollar su ( )Trabajo de Investigación, (X)Tesis o ( )Trabajo de suficiencia profesional para optar al grado de ( )Bachiller, ( )Maestro, ( )Doctor o (X)Título Profesional.

Recuerda que para el trámite deberás adjuntar también, el siguiente requisito según tipo de empresa:

- Vigencia de Poder. *(para el caso de empresas privadas).*
- ROF / MOF / Resolución de designación, u otro documento que evidencie que el firmante está facultado para autorizar el uso de la información de la organización. *(para el caso de empresas públicas)*
- Copia del DNI del Representante Legal o Representante del área para validar su firma en el formato.

Indicar si el Representante que autoriza la información de la empresa, solicita mantener el nombre o cualquier distintivo de la empresa en reserva, marcando con una "X" la opción seleccionada.
( ) Mantener en Reserva el nombre o cualquier distintivo de la empresa; o
(X) Mencionar el nombre de la empresa.

Manuel Vásconez Morey

**Firma y sello del Representante Legal o**

**DNI: 43310067**

El Egresado/Bachiller declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos. En caso de comprobarse la falsedad de datos, el Egresado será sometido al inicio del procedimiento disciplinario correspondiente; asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.

**Firma del Egresado**

**DNI: 43335670**

| CÓDIGO DE DOCUMENTO | | | | | |
|---|---|---|---|---|---|
| FECHA DE VIGENCIA | 30/11/2023 | NÚMERO VERSIÓN | 01 | PÁGINA | Página 1 de 1 |

## ANEXO 3 “Diagrama de Flujo Roles y Responsabilidades”

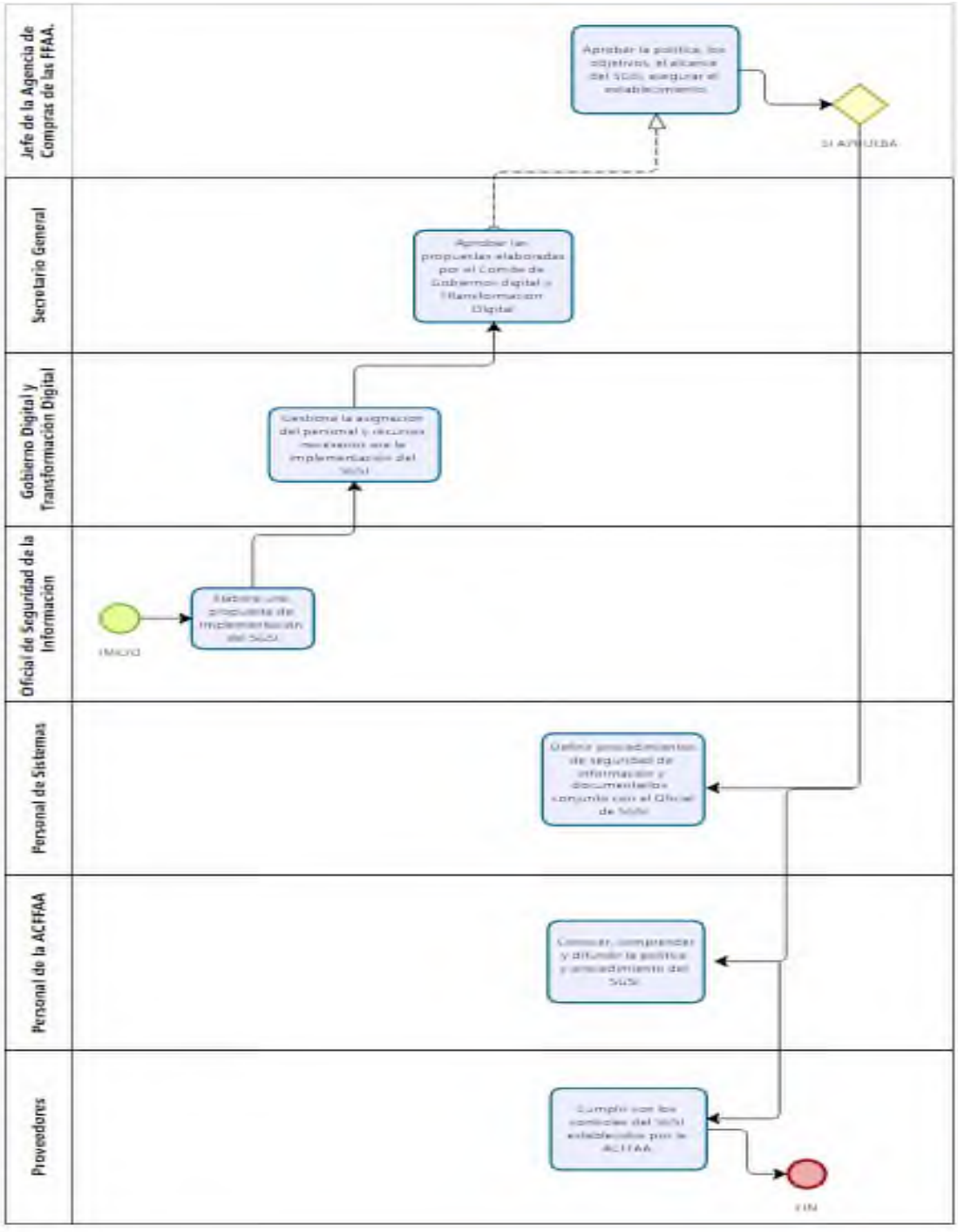


Ilustración 12 Diagrama de Flujo Roles y Responsabilidades. Elaboración propia.

## ANEXO 4 “Segregación de Funciones del SGSI”

| SEGREGACION DE FUNCIONES DEL SGSI | Código: FOR-SGSI-013<br>Versión: 001<br>Doc. de Aprob:<br>Fecha: |
|---|---|

| MATRIZ RACI<br><br>R=Responsable<br>A=Aprobador<br>C=Consultado<br>I = Informado | Comité de Gobierno Digital | Jefe de la ACFFAA | Secretario General | Oficial de Seguridad | Directores y jefes de la ACFFAA | Jefe de la Oficina de | Jefe de la Oficina General de Administración | Jefe de la Oficina de Asesoría Jurídica | Encargado de Logística | Encargado de Servicios Generales (OGA) | Encargado de Control Patrimonial (OGA) | Encargado de Seguridad (OGA) | Encargado de RRHH (OGA) |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Tipo / Código | | | | | | | | | | | | | |
| 6.1 Gestión de Riesgos de Seguridad de la Información | A | I | I | R | C | | | | | | | | |
| 9.1 Seguimiento, Monitoreo y Medición de Datos | A | I | I | R | C | | | | | | | | |
| A.5 Políticas de seguridad de la información | | | | | | | | | | | | | |
| A.5.1 Gestión de la Gerencia para la seguridad de la información | A | I | I | R | C | | | | | | | | |
| A.6 Organización de la seguridad de la información | | | | | | | | | | | | | |
| A.6.1 Organización interna | A | I | I | R | C | | | | | | | | |
| A.6.2.1 Dispositivos móviles | A | I | I | C | C | R | | | | | | | |
| A.7 Seguridad de los recursos humanos | | | | | | | | | | | | | |
| A.7.1 Antes de reclutarlo | A | I | I | R | | | C | C | | | | | R |
| A.7.2 Durante el trabajo | A | I | I | R | | | C | C | | | | | R |
| A.7.3 Término y cambio de empleo | A | I | I | R | | | C | C | | | | | R |
| A.8 Gestión de los Activos | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.8.1 Responsabilidades sobre los activos | A | I | I | R | C | | | | | | | | | |
| A.8.2 Clasificación de la información | A | I | I | R | C | | | | | | | | | |
| A.8.3 Gestión de los medios | A | I | I | R | C | | | | | | | | | |
| A.9 Control de acceso | | | | | | | | | | | | | | |
| A.9.1 Requisitos del negocio sobre control del acceso | A | I | I | R | | R | | | | | | | | C |
| A.9.2 Gestión del acceso al usuario | A | I | I | R | | R | | | | | | | | C |
| A.9.3 Responsabilidades del usuario | A | I | I | R | | R | | | | | | | | C |
| A.9.4 Control de acceso a sistemas y aplicaciones | A | I | I | R | | R | | | | | | | | C |
| A.10 Criptografía | | | | | | | | | | | | | | |
| A.10.1 Controles criptográficos | A | I | I | C | | R | | | | | | | | |
| A.11 Seguridad física y medioambiental | | | | | | | | | | | | | | |
| A.11.1 Áreas seguras | A | I | I | R | C | | R | | | | | | R | |
| A.11.2 Equipos | A | I | I | C | | R | | | | C | C | | | |
| A.12 Seguridad de las operaciones | | | | | | | | | | | | | | |
| A.12.1 Procedimientos y responsabilidades operaciones | A | I | I | C | | R | | | | | | | | |
| A.12.2 Protección contra el malware (programa malicioso) | A | I | I | C | | R | | | | | | | | |
| A.12.3 Backup | A | I | I | C | | R | | | | | | | | |
| A.12.4 Logeo y monitoreo | A | I | I | C | | R | | | | | | | | |
| A.12.5 Control del software operacional | A | I | I | C | | R | | | | | | | | |
| A.12.6 Gestión de las vulnerabilidades técnicas | A | I | I | C | | R | | | | | | | | |
| A.12.7 Consideraciones de las auditorías sobre los sistemas de información | A | I | I | C | | R | | | | | | | | |
| A.13 Seguridad de las comunicaciones | | | | | | | | | | | | | | |
| A.13.1 Gestión de la seguridad de las redes | A | I | I | C | | R | | | | | | | | |
| A.13.2. Transferencia de la información | A | I | I | C | | R | | | | | | | | |
| A.14. Adquisición, desarrollo y mantenimiento del sistema | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A.14.1 Requisitos de seguridad de los sistemas de información | A | I | I | C | | R | | | | | | | | |
| A.14.2 Seguridad en los procesos del programa de desarrollo y soporte | A | I | I | C | | R | | | | | | | | |
| A.14.3 Datos de prueba | A | I | I | C | | R | | | | | | | | |
| A.15 Relación con los proveedores | | | | | | | | | | | | | | |
| A.15.1 Seguridad de la información en las relaciones con los proveedores | A | I | I | R | | | R | C | R | | | | | |
| A.15.2 Gestión de la prestación del servicio por parte del proveedor | A | I | I | R | | | R | C | R | | | | | |
| A.16 Gestión de los incidentes de seguridad de la información | | | | | | | | | | | | | | |
| A.16.1 Gestión de los incidentes de la seguridad de la información y la mejora | A | I | I | R | C | | | | | | | | | |
| A.17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio | | | | | | | | | | | | | | |
| A.17.1 Continuidad de la seguridad de la información | A | I | I | R | | R | | | | | | | | |
| A.17.2 Redundancias | A | I | I | R | | R | | | | | | | | |
| A.18 Cumplimiento | | | | | | | | | | | | | | |
| A.18.1 Cumplimiento de los requisitos legales y contractuales | A | I | I | R | C | | | R | | | | | | |
| A.18.2 Revisiones de la seguridad de la información | A | I | I | R | C | | | R | | | | | | |

Tabla 34 Segregación de Funciones del SGSI –

Elaboración Propia

# ANEXO 4 “Segregación de Funciones del SGSI”

| LISTA DE CONTACTOS CON AUTORIDADES Y GRUPOS DE INTERES | | | | | | | Código: FOR-SGSI-011 |
|---|---|---|---|---|---|---|---|
| | | | | | | | Versión: 001 |
| | | | | | | | Doc. de Aprob: |
| | | | | | | | Fecha: |
| | | | | | | | |
| N.º | Tipo de Contacto (Autoridad-Grupo) | Entidad de Origen | Nombre de Autoridad o Grupo | Cargo o función | Correo | Teléfono | Observaciones |
| 1 | Autoridad | Presidencia de Consejo de Ministros | | Coordinador de Proyectos | | | * Servidor se encuentra a cargo de la emisión de disposiciones para la implementación de Sistemas de Gestión |
| 2 | Autoridad | Ministerio de Defensa | | Jefe de Sistemas de Información | | | * Servidor se encuentra a cargo de la implementación del a norma ISO 27001:2013, en el Sector Defensa |

Tabla 35 Cuadro Contacto de Interés –

Elaboración Propia

## ANEXO 5 “Cuadro Registro y Seguimiento de Proyectos”

| LISTADO DE PROYECTOS | | | | | | | | | | Código: FOR-SGSI-012<br>Versión: 001<br>Doc. de Aprob:<br>Fecha: |
|---|---|---|---|---|---|---|---|---|---|---|
| N° | Código de Proyecto | Tipo de Proyecto | Descripción del Proyecto | Documento de aprobación del proyecto | Encargado (s) del Proyecto | Fecha Inicio | Fecha Fin | Identificación de Riesgos | | Observaciones |
| | | | | | | | | Riesgo identificado | Tratamiento | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

Tabla 36 Cuadro Registro y Seguimiento de Proyectos –

Elaboración Propia

# ANEXO 6 “Dispositivos Móviles”

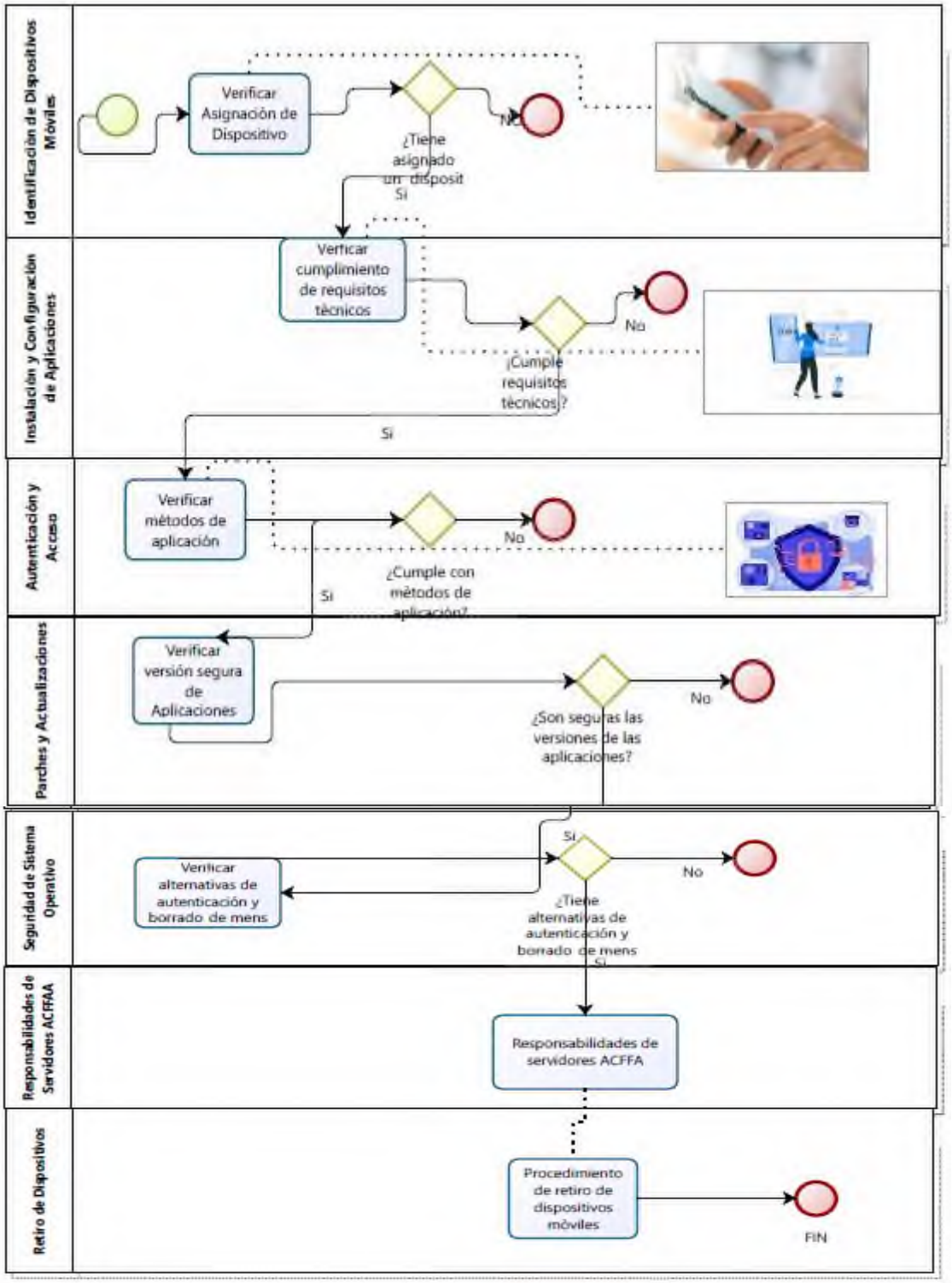


Ilustración 13 Ilustración Diagrama de Flujo - Dispositivos Móviles - Elaboración Propia

## ANEXO 7 “Establecer directrices para el trabajo remoto”

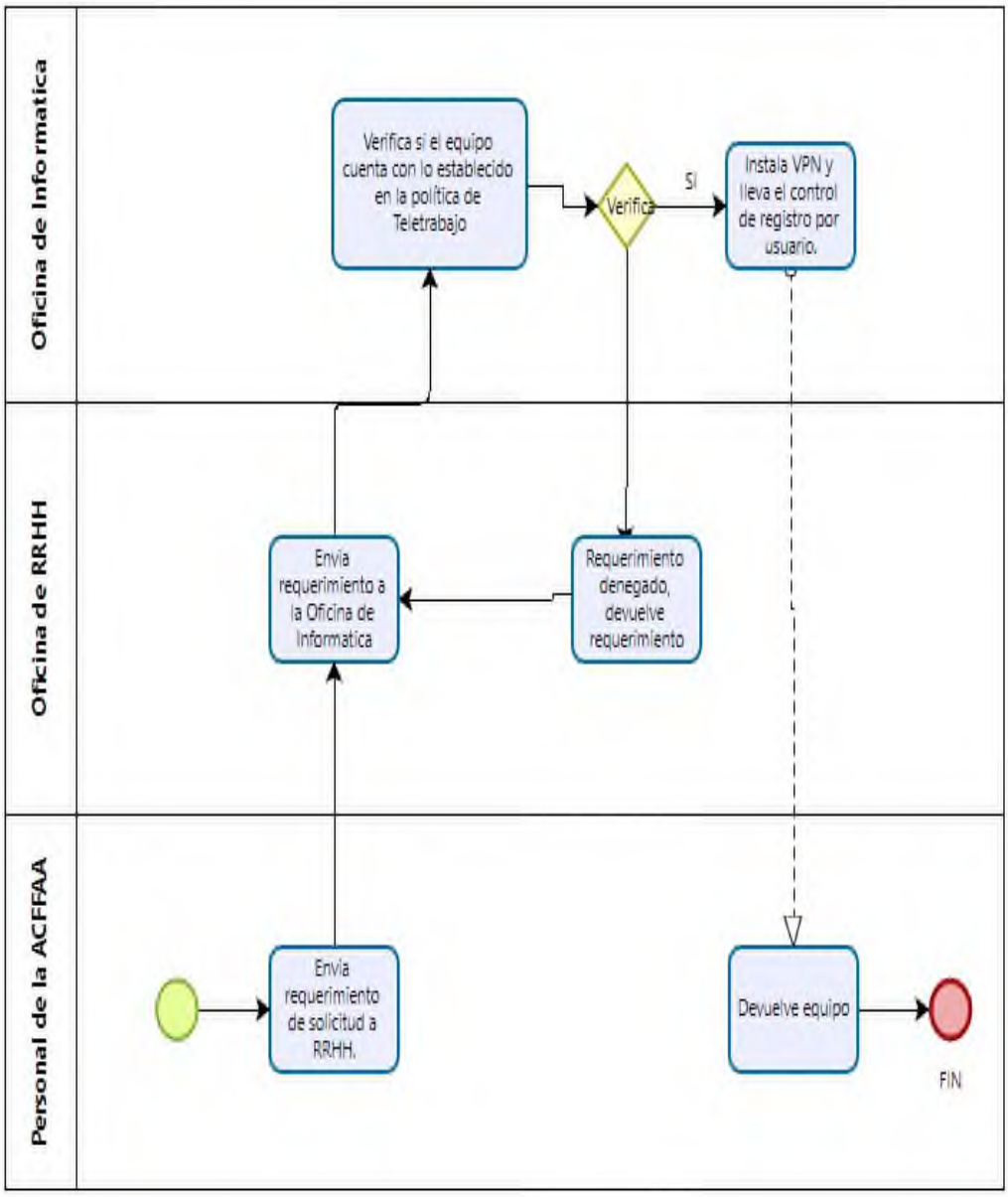


Ilustración 14 Diagrama de Fujo - Establecer directrices para el trabajo remoto. Elaboración Propia.

## ANEXO 8 “Certificado Internacional ISO 27001”

# CERTIFICATE

No. 1016974

ERCA

This is to certify that

Mr

MÁXIMO JHONN MORALES MEDINA

has completed the training

**Lead Implementer**

**ISO/IEC 27001:2013**

The training has covered the professional certification requirements related to knowledge practical experience in activities related to an Information Security Management System according to ISO/IEC 27001 2013 and the commitment to apply our code of ethics in his professional practice

The training was held from 12 November 2022 to 06 December 2022 in the duration of 40 hours. The final examination was successfully completed in accordance with the ERCA personal certification scheme

The training and certification scheme meets the formal requirements confirmed by the European Register of Certificated Auditors (ERCA)

The certificate has been issued under No. 1016974 for the registration period from 06 December 2022

GESCAM

validity code 1CBEFD6A-C06

www.erca.eu
www.erca-academy.com