UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
FACULTAD DE INGENIERÍA ELÉCTRICA, ELECTRÓNICA, INFORMÁTICA Y MECÁNICA
ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

TESIS

DISEÑO E IMPLEMENTACIÓN DE UN PLAN DE GESTIÓN DE SEGURIDAD INFORMÁTICA A TRAVÉS DEL ÁREA FUNCIONAL DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE CHALLHUAHUACHO

PRESENTADO POR:
BR. LIMA RAMOS, Anibal

PARA OPTAR AL TÍTULO PROFESIONAL DE
INGENIERO INFORMÁTICO Y DE SISTEMAS

ASESOR:
DR. RONY VILLAFUERTE SERNA

Cusco - Perú
2024

INFORME DE ORIGINALIDAD

(Aprobado por Resolución Nro.CU-303-2020-UNSAAC)

El que suscribe, **Asesor** del trabajo deinvestigación/tesis titulada: Diseño e implementación de un plan de gestión de seguridad informática a través del área funcional de tecnologías de la información de la Municipalidad distrital de Challhuahuacho

presentado por: Anibal Lima Ramos con DNI Nro.: 73737128 presentado por: ..... con DNI Nro.: ..... para optar el título profesional/grado académico de INGENIERO INFORMÁTICO Y DE SISTEMAS

Informo que el trabajo de investigación ha sido sometido a revisión por 6 veces, mediante el Software Antiplagio, conforme al Art. 6° del ***Reglamento para Uso de Sistema Antiplagio de la UNSAAC*** y de la evaluación de originalidad se tiene un porcentaje de 1 %.

Evaluación y acciones del reporte de coincidencia para trabajos de investigación conducentes a grado académico o título profesional, tesis

Porcentaje	Evaluación y Acciones	Marque con una (X)
Del 1 al 10%	No se considera plagio.	X
Del 11 al 30 %	Devolver al usuario para las correcciones.	
Mayor a 31%	El responsable de la revisión del documento emite un informe al inmediato jerárquico, quien a su vez eleva el informe a la autoridad académica para que tome las acciones correspondientes. Sin perjuicio de las sanciones administrativas que correspondan de acuerdo a Ley.	

Por tanto, en mi condición de asesor, firmo el presente informe en señal de conformidad y **adjunto** la primera página del reporte del Sistema Antiplagio.

Cusco, 23 de julio de 2024

Firma

Post firma. RONY VILLAFUERTE SERNA

Nro. de DNI. 23957778

ORCID del Asesor. 0000-0003-4607-522X

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema Antiplagio: **oid:** 27259:364603724

NOMBRE DEL TRABAJO
PlanSeguridadInfoV6.pdf

AUTOR
Anibal Lima

RECUENTO DE PALABRAS
28132 Words

RECUENTO DE CARACTERES
164530 Characters

RECUENTO DE PÁGINAS
154 Pages

TAMAÑO DEL ARCHIVO
6.2MB

FECHA DE ENTREGA
Jul 23, 2024 10:39 AM GMT-5

FECHA DEL INFORME
Jul 23, 2024 10:41 AM GMT-5

1% de similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para cada base de datos.

- 1% Base de datos de Internet
- 0% Base de datos de publicaciones
- Base de datos de Crossref
- Base de datos de contenido publicado de Crossref
- 0% Base de datos de trabajos entregados

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Coincidencia baja (menos de 20 palabras)
- Bloques de texto excluidos manualmente

Dedicatoria

A mis padres por haberme forjado como la persona que soy, por sus consejos, por su apoyo en todo aspecto, sobre todo su incondicional comprensión, ellos han dado razón a mi vida; la mayoría de mis logros se los debo a ustedes. Me formaron con valores de casa, me motivaron constantemente para alcanzar mis anhelos.

A toda mi familia que es lo más maravilloso que Dios me ha dado.

Agradecimientos

Gracias a Dios por permitirme tener y disfrutar mi vida, gracias a toda mi familia, gracias a la universidad por la experiencia dentro de las aulas, por permitirme convertirme en un profesional en lo que más me apasiona; a los maestros por si sabía enseñanza en todo como recuerdo y prueba viviente en la historia. Gracias a mi familia, a mi hija Melany razón de mi vida por su apoyo fundamental para cumplir con excelencia con el desarrollo de esta tesis, gracias totales por creer en mí, les agradezco y hago presente mi aprecio hacia ustedes.

Resumen

La seguridad de la información es crucial para las organizaciones, siendo la gestión de la seguridad de la información (SGSI) un proceso clave para enfrentar amenazas y gestionar riesgos de manera efectiva. En el caso de la Municipalidad Distrital de Challhuahcho, las diversas áreas interconectadas por una red de comunicaciones manejan información digital para ofrecer servicios oportunos a los usuarios. Sin embargo, se enfrentan a problemas significativos como la pérdida y alteración de información debido a vulnerabilidades en el acceso a través de la red, debido a la falta de protocolos adecuados para establecer accesos restringidos. El problema central identificado es la falta de seguridad informática en el área de tecnologías de la información de la Municipalidad, lo cual compromete la protección e integridad de los datos. El objetivo general propuesto es diseñar e implementar un plan de gestión de seguridad informática para mejorar esta situación. Se adopta el ciclo Deming (PDCA: Planificar, Hacer, Verificar, Actuar) como metodología para el desarrollo del proyecto, asegurando un enfoque sistemático y cíclico para implementar un sistema de gestión de seguridad informática efectivo. El resultado obtenido incluye el diseño detallado del plan de gestión de seguridad informática, que define acciones concretas para mejorar la protección de la información. Este plan se implementará con revisiones y actualizaciones periódicas para garantizar su eficacia continua. En conclusión, se destaca la importancia crucial de contar con un plan de gestión de seguridad informática para proteger los activos informáticos de la Municipalidad ante diversas amenazas. Esta versión condensada debería ajustarse a una página, manteniendo los puntos clave del texto original.

Palabras Clave. Gestión de seguridad informática, normas de seguridad informática

Abstract

Information security is crucial for organizations, with information security management (ISMS) being a key process to face threats and manage risks effectively. In the case of the District Municipality of Challhuahcho, the various areas interconnected by a communications network handle digital information to offer timely services to users. However, they face significant issues such as the loss and alteration of information due to vulnerabilities in access through the network, due to the lack of adequate protocols to establish restricted access. The central problem identified is the lack of computer security in the area of information technologies of the Municipality, which compromises the protection and integrity of data. The proposed general objective is to design and implement a computer security management plan to improve this situation. The Deming cycle (PDCA: Plan, Do, Verify, Act) is adopted as the methodology for the development of the project, ensuring a systematic and cyclical approach to implementing an effective IT security management system. The result obtained includes the detailed design of the IT security management plan, which defines concrete actions to improve information protection. This plan will be implemented with regular reviews and updates to ensure its continued effectiveness. In conclusion, the crucial importance of having a computer security management plan to protect the Municipality's computer assets against various threats is highlighted. This condensed version should fit one page, keeping the key points of the original text.

Keywords. IT security management, IT security standards

Introducción

En este proyecto se exponen los diversos problemas identificados relacionados con la seguridad informática en la Municipalidad Distrital de Challhuahuacho. Con el avance de la tecnología y la falta de capacidad para gestionar planes de control y seguridad, se ha observado un grado muy alto de perdida de información y su manipulación debido a la ausencia de protocolos necesarios para establecer accesos restringidos tanto a la red como a la información de la institución. Debido a los problemas identificados, se propone el diseño e implementación de un plan de gestión de seguridad informática a través del área funcional de tecnologías de información en la Municipalidad Distrital de Challhuahuacho. Este proyecto consta de los siguientes capítulos:

Capítulo I: En este apartado se describirá el problema abordado en este proyecto. Se formulará el problema y se expondrán los objetivos, tanto generales como específicos del proyecto: Además, se presentará la justificación del trabajo y se detallará el método de investigación.

Capitulo II: Se procederá a la revisión del marco teórico, en la cual se citarán tanto los antecedentes nacionales como internacionales que servirán de base para el desarrollo del proyecto. Además, se definirán las bases teóricas relacionadas con las variables que componen la investigación.

Capitulo III: En este capítulo se llevará a cabo el análisis de los resultados obtenidos y se discutirán en comparación con los antecedentes citados. Por último, se tiene

Conclusiones: A las que se llegaron al desarrollar este proyecto

Recomendaciones: Donde se señala una serie de medidas que se debe de tomar en consideración con los resultados obtenidos.

Listado de abreviaturas

1. **ISACA**: Asociación de auditoría y control de sistemas de información.
2. **ISO**: Organización internacional de estandarización.
3. **IEC**: La Seguridad de la información y de las comunicaciones.
4. **MAGER**IT: Metodología de análisis y gestión de riesgos de los sistemas de información
5. **PDCA**: Plan Do-Check-act planificar, hacer, comprobar y actuar.
6. **PDA**: Ciclo Deming
7. **SGSI:** Sistema de Gestión de Seguridad Informática.
8. **SIGA:** Sistema Integrado de Gestión Administrativa
9. **SIAF**: Sistema Integrado de Administración Financiera

INDICE

Índice de tablas

Índice de figuras

Capítulo 1

Aspectos Generales

1.1. Planteamiento del problema

1.1.1. Descripción del problema

Mantener la seguridad de la información es crucial en las organizaciones, convirtiéndose en un tema estratégico de gran importancia. La Gestión de la Seguridad de la Información (SGSI) se establece como un proceso sistemático diseñado para enfrentar eficazmente las amenazas y gestionar los riesgos relacionados con la seguridad dentro de la organización. En la actualidad, los sistemas de información son considerados activos que incluyen datos e información valiosa para las organizaciones. Es fundamental proporcionarles una protección adecuada.

La globalización ha impactado significativamente la seguridad informática a nivel mundial. Este tema ha ganado relevancia tanto en organizaciones públicas como privadas debido a la crítica importancia de la información que manejan, ya sea propia de la institución o de sus usuarios y empleados. Esto es especialmente crucial para aquellas organizaciones con presencia a nivel global, nacional o regional. En este contexto, varios países han comenzado a implementar prácticas de gestión, control y monitoreo de riesgos en seguridad informática. Como parte de estas iniciativas, la norma ISO/IEC 27001:2013 se ha convertido en una opción preferida para asegurar la protección de la información (Noticias, 2024).

Así es como en Latinoamérica surge la iniciativa de fortalecer todo lo relacionado con la seguridad informática y la seguridad de la información. Esta iniciativa comienza con la apli- acción de estándares de la familia ISO 27000 y la ISO 31000,

centrándose principalmente en la gestión de riesgos, como se describe en la primera norma. Según Mesa (2018), se afirma que la implementación de sistemas de seguridad de la información en Chile tiene un ´éxito del 93 por ciento, mientras que en Ecuador se sitúa en un 65 por ciento y en Venezuela en un 63 por ciento de efectividad. En Perú´, las empresas no están exentas de unirse a las diversas organizaciones que ya han implementado políticas relacionadas con la gestión de la seguridad de la información. Estas políticas se basan en las normas ISO/IEC 27001:2013, con el objetivo de controlar los riesgos a los que están expuestas y los posibles efectos que podrían generar. Debido a estas razones, muchas empresas, tanto públicas como privadas, que operan en el territorio peruano han iniciado la implementación de sistemas de gestión de seguridad de la información (SGSI) y de seguridad informática. Esta estrategia se utiliza para garantizar la reducción de riesgos y asumir la responsabilidad de la gestión de la seguridad de manera documentada, enfocándose en la calidad y la eficacia.

La Municipalidad Distrital de Challhuahuacho cuenta con diversas áreas que prestan servicios a la población. Estas áreas están interconectadas a través de una red de comunicaciones. Con el avance de la tecnología, se han implementado sistemas para la digitalización de la organización y la información. En la actualidad, la información se almacena de manera digital y se utiliza para brindar una atención oportuna a los usuarios. Sin embargo, se ha identificado un problema significativo dentro de la Municipalidad: existe un alto grado de pérdida de información, y se ha observado que la información ha sido alterada debido a las vulnerabilidades en el acceso a través de la red. Esto se debe a la falta de protocolos necesarios para establecer accesos restringidos tanto a la red como a la información de la organización. Asimismo, se ha identificado que en la Municipalidad no se

lleva a cabo una adecuada gestión en materia de seguridad. No se han establecido lineamientos específicos relacionados con la seguridad, ya que no existen políticas de seguridad definidas. Además, el personal carece de conocimientos adecuados en lo que respecta a la seguridad de la información. Estas vulnerabilidades ponen en riesgo la integridad de la información y los datos, lo que aumenta la probabilidad de manipulación y la posibilidad de pérdida de información importante, tanto de los usuarios como de las áreas que conforman la Municipalidad. Esta situación podría exponer información confidencial de los usuarios a posibles amenazas y riesgos.

Basado en todo lo mencionado, surge la siguiente interrogante: ¿Cómo se puede mejorar el Sistema de Gestión de Seguridad Informática (SGSI) para garantizar la protección de la información en el área funcional de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho? Para abordar esta interrogante, es necesario diseñar un plan de gestión de seguridad informática (SGSI) basado en las normas estandarizadas ISO/IEC 27001:2013. Este enfoque se respalda en la aplicación de políticas destinadas a la protección de redes y la infraestructura informática de la Municipalidad.

1.1.2. Identificación del problema

Con este proyecto se propone la implementación de un plan de seguridad informática que contribuya a proteger la información y los datos en el área funcional de tecnologías de la información de la Municipalidad Distrital de Challhuahuacho. Para lograr este objetivo, se aplicarán diferentes normas de seguridad informática. Como se menciona en la Norma ISO/IEC 27002 (Norma Española, 2017)*"Las organizaciones deberían definir una política de seguridad de la información al más alto nivel, que sea aprobada por la dirección y establezca*

el enfoque de la organización para gestionar sus objetivos de seguridad de la información". Esta norma internacional se reconoce como un estándar global que establece buenas prácticas para la seguridad de la información, y su cumplimiento en las organizaciones ayuda a cumplir con sus responsabilidades en este ámbito.

En concordancia con esta norma, propongo la implementación de la ISO/IEC 27001:2013 a través de este proyecto. Esta norma se presenta como una solución para mejorar de manera continua la seguridad de la información. Como se menciona en ISO (2019, pág. 4), el diseño y desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI) permite evaluar los diferentes riesgos y amenazas que puedan poner en peligro los datos y la información, y también facilita la implementación de controles y estrategias necesarias para minimizar estos peligros.

1.2. Formulación del problema

1.2.1. Problema general

La falta de un plan de seguridad informática en el área funcional de tecnologías de la información de la Municipalidad Distrital de Challhuahuacho pone en riesgo que exista vulnerabilidades en la protección e integridad de datos e información.

1.2.2. Problemas específicos

- ¿Cuál es el estado actual de la seguridad de la información en el área funcional de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho?
- ¿Qué riesgos y amenazas de seguridad de la información se presentan en el área funcional de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho?

- ¿Cómo se puede mejorar la seguridad de los datos en el área funcional de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho?

1.3. Objetivos

1.3.1. Objetivo general

Diseñar e implementar un plan de gestión de seguridad informática para mejorar la protección de la información a través del área de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho.

1.3.2. Objetivos específicos

- Identificar las vulnerabilidades existentes en la seguridad de información a través del área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.
- Identificar los riesgos y las amenazas existen en la seguridad de información a través del área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.
- Diseñar políticas de seguridad informática para la protección de información a través del ´área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.
- Implementar políticas de seguridad informática para la protección de información a través del área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.

1.4. Justificación

1.4.1. Conveniencia

Los avances actuales están centrados en mejorar la calidad de las medidas de seguridad, las cuales son cruciales para el desarrollo de la sociedad. Al mismo tiempo, se reconoce que este ámbito es vulnerable y peligroso. Por lo tanto, la seguridad de la información se ha convertido en un tema de gran relevancia.

La gestión de la seguridad de la información ha sido diseñada para hacer frente de manera efectiva a amenazas y riesgos. Estos desafíos son razones fundamentales para considerar la implementación de sistemas de gestión de seguridad informática que contribuyan a la protección de la información. Esto implica definir procedimientos adecuados e implementar controles de seguridad después de realizar una evaluación de riesgos, junto con la medición de la efectividad en el manejo de los datos.

1.4.2. Relevancia

La información manejada en las diversas áreas de la Municipalidad Distrital de Challhuahuacho está expuesta y, por lo tanto, vulnerable a diversas amenazas, incluyendo intrusiones no autorizadas. Esta situación es especialmente preocupante cuando involucra al personal interno que podría acceder y manipular los datos de manera indebida. Por lo tanto, es evidente la necesidad de considerar alternativas para abordar este problema, y una solución viable es la implementación de sistemas de gestión de seguridad de la información.

El diseño e implementación de un Sistema de Gestión de Seguridad Informática (SGSI) permitirá que la Municipalidad establezca una estructura organizativa con roles y responsabilidades definidos, junto con políticas coherentes alineadas con los objetivos de seguridad en todos los niveles de la institución. Este SGSI estará

basado en la norma ISO/IEC 27001:2013, la cual proporciona los medios necesarios para garantizar la seguridad de la información. Esto contribuirá a la viabilidad en la dirección y al logro de los objetivos de las diferentes áreas de la Municipalidad.

1.4.3. Implicancias prácticas

El propósito fundamental de este proyecto es profundizar en el ámbito de la seguridad informática, proporcionando una explicación detallada sobre los riesgos y amenazas a los que podría estar expuesta la información de la Municipalidad. Además, se busca ofrecer soluciones concretas para reducir estos riesgos y proteger efectivamente la información. En este sentido, es prioritario ofrecer herramientas disponibles que permitan elevar los niveles de seguridad informática de la institución.

Es crucial que las diferentes organizaciones e instituciones implementen políticas de seguridad de datos e información para prevenir problemas de seguridad. Por lo tanto, el diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) demostrará el compromiso de la organización con la seguridad de la información. Además, facilitará la gestión eficiente de riesgos. Un SGSI permite a las organizaciones establecer estructuras organizativas con roles y responsabilidades definidos, promoviendo así una cultura de seguridad en todos los niveles y facilitando la adecuada gestión de la seguridad de la información."

1.4.4. Valor teórico

La presente investigación tiene como objetivo contribuir al conocimiento existente sobre los sistemas de gestión de seguridad informática como herramienta para proteger los datos e información en una institución u organización específica.

Los resultados obtenidos en este proyecto podrían servir como propuestas que pueden considerarse como antecedentes en estudios relacionados con la seguridad informática. Estos estudios demuestran que la implementación de sistemas de seguridad informática dentro de las organizaciones beneficia significativamente la protección de la información.

1.4.5. Utilidad metodológica

Para alcanzar los objetivos planteados en este proyecto, es fundamental emplear métodos y técnicas de investigación adecuadas al desarrollo del mismo. En este caso, nos encontramos en el nivel de investigación aplicativa, y el objetivo es diseñar e implementar un plan de gestión de seguridad informática para mejorar la protección de la información en el área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho. Para ello, se propone el uso del método PDCA (Plan-Do-Check-Act). El método PDCA se estructura en diferentes etapas que deben cumplirse para identificar adecuadamente las debilidades y problemas informáticos, asegurando la implementación de mejoras correspondientes. Este método ha demostrado su efectividad en diversas circunstancias e instituciones, obteniendo resultados positivos." (Irurita Alzueta & Villanueva Roldan, 2019).

1.5. Delimitación de estudio

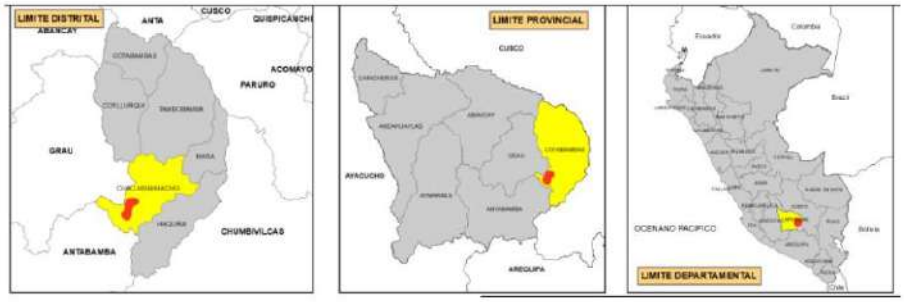
1.5.1. Delimitación espacial

El proyecto se realizará´ en la Municipalidad Distrital de Challhuahuacho, Provincia de Cotabambas, región Apurímac, cuya ubicación geográfica se visualiza en la figura 1.

1.5.2. Delimitación temporal

La duración del desarrollo del proyecto es de 8 meses, comenzando en noviembre de 2022 y planificado para analizar en julio de 2023 incluyendo la etapa de definición de conclusiones.

Figura 1
Ubicación del Distrito de Challhuahuacho



1.6. Método

1.6.1. Alcance

El proyecto considera la implementación del sistema de gestión de seguridad de la información en el área funcional de tecnologías de la información, aplicando el estándar ISO/IEC 27001:2013.

1.6.2. Investigación aplicada

La investigación práctica o empírica, también conocida como investigación aplicada, se caracteriza por buscar la aplicación de los conocimientos adquiridos mientras se genera nuevo conocimiento. Este tipo de investigación se fundamenta en la sistematización e implementación de prácticas desarrolladas a partir de la investigación. Aborda el concepto del problema de investigación como una situación deficiente susceptible de mejora. El objetivo principal es resolver problemas prácticos y generar soluciones concretas aplicables en la realidad. La investigación práctica o empírica se centra en aplicar conocimientos teóricos en contextos reales para mejorar la situación o resolver problemas específicos,

obteniendo resultados aplicables que contribuyan al desarrollo y avance en áreas específicas del conocimiento (Murillo, 2008).

Fomentar la utilización de saberes y la creatividad para abordar desafíos concretos de manera efectiva es fundamental en este nivel de investigación, que busca mejorar situaciones deficitarias y generar soluciones concretas beneficiosas para la sociedad. La investigación aplicada tiene como objetivo principal desarrollar proyectos que apliquen los conocimientos adquiridos en la solución de problemas específicos. Esto implica la implementación y sistematización de prácticas basadas en la investigación, orientadas a mejorar la situación actual y generar un impacto positivo en la sociedad. Además, este tipo de investigación se enfoca en la innovación tecnológica y su aplicación en las ciencias de la ingeniería, buscando crear o modificar procesos y desarrollar nuevas tecnologías que contribuyan a cumplir objetivos beneficiosos para la sociedad (Vargas Cordero, 2019).

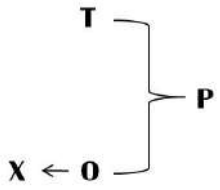
La norma ISO/IEC 27001:2013 y ISO/IEC 27002:2013 son estándares reconocidos internacionalmente para la gestión de la seguridad de la información. Estas normas proporcionan un marco de referencia para establecer, implementar, mantener y mejorar un sistema de gestión de seguridad de la información en una organización. Al aplicar las directrices y normas establecidas en estos estándares, el proyecto tiene como objetivo mejorar la seguridad informática en el área funcional de tecnologías de la información de la Municipalidad Distrital de Challhuahuacho, mitigando los riesgos y fortaleciendo la protección de la información.

Es crucial realizar un análisis detallado de la situación actual de la Municipalidad y asignar los recursos necesarios, así como contar con la participación activa de los responsables de la seguridad informática. Se recomienda contar con un equipo multidisciplinario que incluya expertos en seguridad informática, personal de TI y

otros profesionales relevantes para llevar a cabo la implementación efectiva de las directrices y normas establecidas. La implementación de la norma implica evaluar y mejorar continuamente los procesos y controles de seguridad de la información, identificar activos de información, evaluar riesgos, implementar medidas de seguridad adecuadas y revisar y mejorar el sistema de gestión de seguridad de la información. Elaborar un plan de acción basado en la norma ISO/IEC 27001:2013 permitirá abordar los problemas identificados e implementar cambios y mejoras en los procesos existentes, fortaleciendo así la seguridad de la información y previniendo problemas futuros.

1.6.3. Diseño

Para esta investigación, el diseño es no experimental, ya que no se realiza manipulación alguna de variables. Según (Hernandez Sampieri, Fernadez Collado, & Baptista Lucio, 2018) en este tipo de diseño no se tiene control directo sobre las variables y no es posible influir en ellas. A continuación, se presenta el esquema correspondiente a este diseño.



Donde:

X = Realidad de la institución

O = Observación

T = Modelo teórico

P = Propuesta de soluciones y recomendaciones basadas en la norma ISO/IEC 27001:2013

1.6.4. Metodología de desarrollo

1.6.4.1. Método PDCA (Plan Do-Check-Act)

El Ciclo Deming, también conocido como el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), es un método cíclico de cuatro pasos para la solución de problemas y la mejora constante de procesos. Este ciclo es reconocido por la norma ISO/IEC 27001:2014 y la asociación de auditoría y control de sistemas de información (ISACA). Que es una asociación profesional internacional centrada en las tecnologías de la información (TI). El ciclo Deming consta de cuatro etapas y 11 fases que ayudan a implementar un sistema de gestión de seguridad informática (SGSI) y a mejorar la eficiencia en términos de tiempo y costos, cada etapa del ciclo contribuye al propósito de identificar los diferentes procesos, evaluar su funcionamiento y determinar áreas de mejora, este enfoque también ayuda a remediar errores recurrentes en diferentes operaciones. El ciclo PDCA es una poderosa herramienta de gestión que permite a las organizaciones obtener mejoras progresivas y controlar los cambios en los procesos. Contribuye a la mejora continua y a la optimización de las operaciones en diferentes sectores. (Castillo Pineda, 2019).

1. **Etapas del PDCA**

   Este método está compuesto por cuatro etapas o pasos PDCA (Planificar, Hacer, Comprobar y Actuar), diseñado con el propósito de resolver problemas y aplicar cambios de manera sistemática (Route, 2022).

Figura 2
Ciclo PDCA

a) **Etapa 1: Planificar**

- **Fase 1: Identificar los objetivos de negocio.**

  Se realiza la identificación y priorización de los objetivos en conjunto con las partes interesadas, con el propósito de respaldar el proyecto. Estos objetivos pueden derivarse de la misión y visión de la organización, el plan estratégico y los objetivos de TI. Además, estos objetivos pueden facilitar la identificación de evaluaciones de riesgo (Route, 2022)

- **Fase 2: Obtener apoyo de la administración.**

  Durante el desarrollo del proyecto, es crucial que las partes comprometidas incluyan la gerencia y/o el área administrativa. Se requiere un monitoreo continuo y la implementación de políticas de seguridad efectivas. Además, es fundamental realizar capacitaciones periódicas para los empleados. Mantener una cultura de seguridad de la información es esencial, dado que esta área se considera la más vulnerable (Route, 2022).

- **Fase 3: Seleccionar el alcance adecuado.**

  Se selecciona un alcance adecuado para la implementación según la norma ISO/IEC 27001:2013. Es crucial considerar cualquier ámbito de aplicación que afecte parcial o totalmente a la organización donde se aplique el proyecto. Además, es importante definir claramente el alcance específico del Sistema de Gestión de Seguridad, especificando los procesos incluidos dentro del alcance establecido para la implementación (Cruz Díaz, (Route, 2022).

- **Fase 4: Definir un método de evaluación.**

  La norma ISO/IEC 27001:2013 establece requisitos que deben cumplirse para la gestión de la seguridad de la información. Para satisfacer estos requisitos, es fundamental definir y documentar un método de evaluación de riesgos. Aunque la norma no especifica un método de evaluación de riesgos en particular, se espera que las organizaciones elijan un método adecuado basado en niveles que consideren la confidencialidad, integridad y disponibilidad de la información. Es importante destacar que la elección del método de evaluación de riesgos debe ser coherente con los objetivos y la naturaleza de la organización, así como con la información y los activos que se desean proteger. Algunos métodos comunes de evaluación de riesgos incluyen (Route, 2022) .

- **Fase 5: Preparar un inventario de los activos de información.**

  La definición de una lista de activos de la información es una parte crucial del proceso de gestión de la seguridad de la información. Esta lista permite identificar y priorizar los activos que deben protegerse, así como los riesgos asociados con cada uno de ellos (Route, 2022).

b) Etapa 2: Hacer

- **Fase 6: Gestionar los riesgos, crear un plan de tratamiento de riesgos.**

  La aceptación del riesgo es una decisión estratégica que debe tomarse con pleno conocimiento de sus implicaciones. Es crucial que la alta dirección y otros responsables estén involucrados en este proceso de toma de decisiones, y que las decisiones sean documentadas y comunicadas claramente en relación con la gestión de riesgos. Además, es esencial realizar evaluaciones periódicas y revisiones continuas de los riesgos, dado que las condiciones pueden cambiar con el tiempo y lo que era aceptable en un momento dado podría no serlo en el futuro. La gestión de riesgos es un proceso dinámico y en constante evolución (Route, 2022).

- **Fase 7: Establecer políticas y procedimientos para controlar los riesgos.**

  Esta fase implica adaptar los controles de seguridad de acuerdo con las necesidades específicas de la organización, establecer políticas y procedimientos claros, definir responsabilidades y

asegurar una implementación efectiva. Un enfoque centrado en la seguridad de la información es fundamental para proteger los activos de la organización y cumplir con los estándares y normativas aplicables, como la ISO/IEC 27001:2013 (Route, 2022).

- **Fase 8: Asignar recursos y capacitar al personal.**

  Es fundamental comprometer recursos suficientes para la gestión de la seguridad de la información con el fin de proteger los activos y datos críticos de la organización. Este compromiso debe ser sostenible a lo largo del tiempo y respaldado por un enfoque integral en la seguridad de la información a nivel de toda la organización (SGSI) (Route, 2022).

c) Etapa 3: Revisión

- **Fase 9: Supervisar la implementación del sistema de seguridad informática SGSI.**

  La auditoría interna periódica es necesaria para el monitoreo y revisión del sistema, lo cual implica la implementación de acciones correctivas y/o preventivas. Para asegurar la eficacia del sistema de gestión de seguridad informática, la administración debe realizar revisiones regulares. Los resultados de estas auditorías se documentan y se les da seguimiento adecuado (Route, 2022).

- **Fase 10: Prepararse para la auditoria de certificación.**

  Para obtener la certificación, es crucial realizar un ciclo completo de auditorías internas, revisando la gestión y conservando evidencias de

las respuestas obtenidas como resultado de estas revisiones y auditorías (Route, 2022).

d) Etapa 4: Actuar

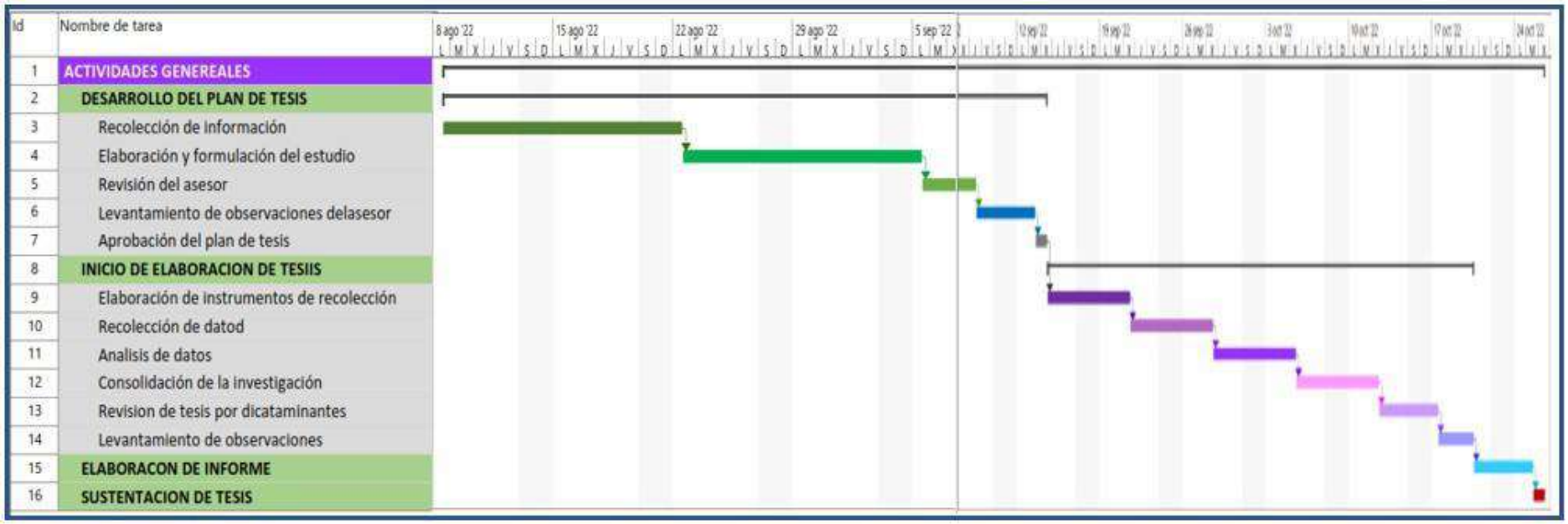
- **Fase 11: Realizar auditorías periódicas de re evaluación.**

  El seguimiento y las auditorías periódicas confirmarán que la organización está cumpliendo con la norma, además de realizar reevaluaciones para asegurar que el sistema de gestión de seguridad informática (SGSI) continúe operando según la norma ISO/IEC 27001:2013, siguiendo el ciclo PDCA (Route, 2022).

Cronograma de actividades

Figura 3

Cronograma



Capítulo 2

Marco Teórico

2.1. Antecedentes

2.1.1. Antecedentes internacionales

(Remolina Becerra, 2019) Diseño de un modelo de seguridad informática a una empresa en su sistema de monitoreo del área de tecnología. Esta tesis fue presentada en la Universidad Cooperativa de Colombia como parte de los requisitos para optar al título de ingeniero de telecomunicaciones, en Bogotá, Colombia.

Conclusiones:

- Aunque la recopilación de valores de los activos no fue precisa, se logró completar el análisis necesario para extraer los resultados que muestran los riesgos en la seguridad.
- El análisis de riesgos ha proporcionado una visión precisa del estado actual de la empresa en cuanto a seguridad en el área de tecnología.
- Desarrollar políticas de seguridad en la organización abarca la mayoría de los diversos aspectos que forman parte del sistema de gestión de seguridad de la información.

Comentario:

- Estas tesis subrayan la importancia de realizar un análisis preliminar para obtener una comprensión del estado actual de la organización. Este es un punto crucial a considerar al llevar a cabo la propuesta de implementar un Sistema de Gestión de Seguridad de la Información, tal como se plantea en este proyecto.

  Aquí tienes una versión mejorada del texto:

(Guarnizo Arias & Prieto Sarmiento, 2018) presentó el trabajo titulado “Diseño de un sistema de gestión de seguridad de la información (SGSI) en la empresa Agility S.A.S.” como requisito para optar al título de ingeniero de telecomunicaciones en la Universidad Distrital Francisco José de Caldas, Bogotá, Colombia.

Conclusiones:

- Se utilizaron instrumentos para recopilar información con el fin de identificar los diferentes riesgos y amenazas dentro de la empresa. Se encontró que existía desconocimiento sobre metodologías para la gestión de la seguridad de la información.
- Con base en los resultados obtenidos en la identificación de problemas, se pudo determinar qué controles y políticas de seguridad podrían aplicarse para reducir los riesgos existentes en la empresa Agility. Al implementar acciones dirigidas a la prevención y corrección en cada área, se asegura un alto porcentaje de funcionamiento de la información.
- El sistema de gestión de seguridad diseñado en la empresa proporciona herramientas específicas para cada uno de los activos en las áreas que requieren el uso de tecnologías de la información. Estas herramientas ayudan en el desarrollo de la gestión de cada uno de los procesos, con el objetivo de mitigar el riesgo existente y proporcionar una mayor confiabilidad en las operaciones.

Comentario:

- En relación con esta tesis, se optó por utilizar instrumentos que faciliten la recopilación de datos y apoyen la identificación de riesgos y amenazas en la Municipalidad de Challhuahuacho. Esta medida es efectiva para comprender y abordar los desafíos de seguridad de la información en la organización, permitiendo tomar acciones adecuadas para mitigarlos.

(Alfaro Vina & Vargas Lón, 2021) “Diseño del Plan de Seguridad Informática del Sistema de Información Misional de la Procuraduría General de la Nación”, trabajo para optar al título de especialista en seguridad informática, Bogotá - Colombia.

Conclusiones:

- Es crucial reconocer la importancia de emplear metodologías para evaluar el estado real de seguridad de los activos. En el caso del sistema misional de la Procuraduría, se lograron identificar diversos riesgos y debilidades. Estos hallazgos se consideraron como puntos de partida esenciales para proponer planes destinados a mejorar la seguridad.
- Es crucial reconocer la importancia de comprender la necesidad de proteger la información. Para lograrlo, es fundamental identificar qué información es sensible y confidencial dentro de la organización. Este conocimiento permite definir los diversos controles necesarios para aplicar una protección adecuada a dicha información, asegurando su integridad, confidencialidad y disponibilidad.
- Es crucial establecer relaciones efectivas entre diversos factores para que un plan de seguridad pueda ser efectivo. Deben considerarse elementos como la tecnología, las políticas de seguridad, las personas y los recursos financieros como componentes interconectados. Cada uno de estos elementos desempeña un papel crucial en la implementación de estrategias de seguridad y contribuye al éxito general de la gestión de seguridad de la información.

Comentario:

- De acuerdo con esta tesis, se reconoce la gran importancia de mantener la información protegida, identificando de manera precisa la información sensible y, especialmente, la información confidencial. En este contexto, se respalda el

propósito de implementar sistemas de gestión de seguridad de datos informáticos y de aplicar diversas estrategias para proteger distintos tipos de datos e información. Esto es fundamental para garantizar la integridad, confidencialidad y disponibilidad de los activos de información de la organización.

(Bojaca Garavito, 2021) en su proyecto de grado titulado "Diseño de un sistema de gestión de seguridad informática basado en las normas ISO/IEC 27001-27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gacheta", realizado en la Universidad Nacional Abierta y a Distancia, Escuela de Ciencias Básicas e Ingeniería, Gacheta, Cundinamarca.

Conclusiones:

- El diseño de un sistema de gestión de seguridad ha permitido identificar las vulnerabilidades y amenazas a las que están expuestos los activos de información del área administrativa del Hospital San Francisco. En consecuencia, es crucial proponer medidas de protección de la información.
- Se concluye que los procesos de seguridad establecidos antes del desarrollo del proyecto fueron insuficientes, ya que carecían de protocolos adecuados de autenticación de usuarios, lo cual permitía el acceso a la información por parte de cualquier persona. Con el diseño del sistema de seguridad, se propone implementar procesos más robustos y seguros.
- Las propuestas respecto a las medidas de control que deben implementarse requieren un análisis detallado de su ejecución. Es fundamental considerar una inversión de capital que asegure la implementación efectiva del proyecto.

Comentario:

- Según lo desarrollado en esta tesis, se destaca la necesidad de aplicar diversos protocolos de seguridad, cada uno adaptado al tipo de información que se debe proteger. Además, es crucial considerar el presupuesto disponible, ya que toda propuesta presentada requiere una inversión adecuada. Este aspecto es fundamental en el desarrollo de nuestra propuesta.

2.1.2. Antecedentes nacionales

(Villo Guerrero, 2021) desarrolló la tesis titulada 'Modelo de gestión de riesgo para seguridad informática bajo ISO/IEC 27001:2013 en empresa de entretenimiento y juegos de azar', en la Universidad 'Señor de Sipan', perteneciente a la Facultad de Ingeniería y Urbanismo, Escuela de Ingeniería de Sistemas, ubicada en Lima, Perú.

Conclusiones:

- El trabajo realizado ha permitido diagnosticar que la empresa carece de medidas de control que aseguren la seguridad informática, lo que impide la consolidación de una cultura organizacional, así como la implementación de políticas y procedimientos documentados para proteger los equipos y sistemas informáticos.
- El modelo propuesto se diseñó para la gestión de riesgos en la seguridad informática, basándose en la norma ISO/IEC 27001:2013 y aplicando la metodología MAGERIT y el modelo DEMING.
- La implementación progresiva ha demostrado una eficacia del 80% en la gestión para reducir los incidentes tecnológicos en la empresa, lo cual valida la hipótesis alterna propuesta en la investigación.

Comentario:

- Este proyecto reafirma que la implementación de sistemas de gestión de riesgos en seguridad informática es eficaz para la protección de datos. Se recomienda llevar a cabo esta implementación de manera progresiva, lo cual ayuda a reducir incidentes y eliminar vulnerabilidades existentes. Este punto es crucial al considerar la aplicación de la propuesta presentada.

(Fukusaki Infantas & Cruz Diaz, 2018) llevaron a cabo un proyecto titulado 'Diseño e Implementación de un Sistema de Gestión de Seguridad de la Información para proteger los activos de información de la Clínica MEDAM Perú S.A.C.', como parte de su trabajo en la Universidad San Martín de Porres, Escuela Profesional de Ingeniería de Computación y Sistemas, ubicada en Lima, Perú.

Conclusiones:

- Se logró mitigar los riesgos relacionados con los activos de la información clínica identificados, mediante el diseño e implementación de controles enfocados en los riesgos más críticos.
- La implementación del sistema de gestión sirvió como base para lograr el objetivo de implementar diversas políticas de gestión eficiente que aseguren la confidencialidad de los activos de la información.
- Llevar a cabo la sensibilización del personal en relación con la seguridad es crucial en la implementación de sistemas de seguridad. Esto asegura que los trabajadores sean conscientes de manejar la información con confidencialidad y garantizar la integridad de la misma.

Comentario:

- El uso de un sistema de seguridad en la gestión informática es fundamental para que las organizaciones cumplan con diversas políticas de seguridad. Es

crucial considerar estos aspectos durante la implementación de estas políticas al proponer soluciones relacionadas con la seguridad informática.

(Merino Rosas, 2021), “Implementación de un plan de seguridad informática con la norma ISO/TEC 27001 en la empresa Ransa Comercial S.A. Piura 2021”, tesis para optar el título de ingeniero de sistemas en la Universidad Católica los Ángeles Chimbote, Piura – Perú´.

Conclusiones:

- Gracias por compartirlo. Parece que estás hablando sobre la utilización de la norma ISO 27001 para evaluar los procesos de seguridad dentro de una empresa, lo que facilitó la identificación de problemas de seguridad. La evaluación de marcos de referencia ha permitido proponer mejoras significativas en la seguridad de la información de la empresa.
- Se logró mejorar la seguridad de la información en las diversas áreas tecnológicas de la empresa mediante la aplicación de la norma ISO/IEC 27001.

Comentario:

- En el ámbito de la seguridad, siempre se ha dado prioridad al uso de normas ISO. Dentro de toda la familia de normas ISO, destaca la ISO 27001, la cual es fundamental en la propuesta que estamos planteando, como se ha demostrado. Aquí tienes una versión mejorada:
- En las conclusiones mencionadas, se han obtenido resultados positivos al implementar esta norma. Una de sus características es la realización de evaluaciones precisas para identificar problemas y vulnerabilidades específicas en puntos determinados. Este aspecto es crucial y debe ser considerado.

(Arana Fernandez, 2019) “Seguridad en las tecnologías de la información”, Trabajo de suficiencia profesional de la Universidad José Carlos Mariátegui, vicerrectorado de investigación. Moquegua – Perú´.

Conclusiones:

- Se logró incrementar la seguridad de la información tras la implementación de un Data Center en la sede principal de la Municipalidad Provincial de Ilo.
- Se realizó un análisis de la infraestructura del centro de procesamiento de datos de la Municipalidad, el cual reveló las condiciones de seguridad en el procesamiento de la información.
- Mantener la red estructurada demostró una mejora en las condiciones del transporte de la información, lo que indirectamente también fortaleció la seguridad de los datos.

Comentario:

- Se debe considerar que, para poder implementar propuestas relacionadas con la seguridad de datos informáticos, es necesario realizar análisis de los diferentes puntos de interconexión entre la infraestructura y la forma en que se comparten los datos. Es importante tener en cuenta este punto, como se muestra en la tesis citada, ya que, al haber identificado las diferentes vulnerabilidades, es posible aplicar los cambios necesarios que ayuden a mejorar las condiciones en el transporte de la información y fortalezcan la seguridad.

2.2. Bases teóricas

2.2.1. Sistema de gestión

Una herramienta que permite controlar y planificar las tareas administrativas de la organización, así como organizar y automatizar dichas tareas. Los sistemas de gestión analizan el rendimiento y los riesgos a los que se enfrenta la empresa, con

el fin de proporcionar un ambiente laboral eficiente y sostenible. El objetivo es unificar en un solo software todas las actividades de la compañía, facilitando así la toma de decisiones y el análisis de datos. (Reaño Rivera, 2022).

2.2.1.1.Propósito de un sistema de gestión

El propósito de implementar un sistema de gestión es agrupar y coordinar las operaciones de cada una de las áreas de una organización para ayudarlas a alcanzar sus objetivos de manera más organizada y eficiente. Esto no solo reduce costos, sino que también elimina gastos constantes. El éxito del buen funcionamiento de un sistema de gestión se basa en una planificación adecuada y en la ejecución de todas las actividades que forman parte del proceso, involucrando a todas las áreas correspondientes (Reaño Rivera, 2022).

2.2.1.2.Activos de la información

Los recursos del sistema de seguridad de la información son esenciales para el buen funcionamiento de la empresa y para alcanzar los objetivos propuestos. Los activos de la información están relacionados tanto de manera directa como indirecta con otras entidades. (Borrero Ochoa, 2019).

a) Características de los activos

Existen diferentes características para cada activo, dependiendo del estado de seguridad en cada uno de los niveles de los sub estados: confidencialidad, integridad y disponibilidad (Borrero Ochoa, 2019) Es crucial considerar los puntos de interconexión entre la infraestructura y la forma en que se comparten los datos. Este aspecto, como se muestra en la tesis citada, es fundamental ya que, al identificar las diferentes

vulnerabilidades, es posible aplicar los cambios necesarios que mejoren las condiciones en el transporte de la información y la seguridad.

- **subestadio A (Autenticación):** Se caracteriza por ofrecer y reconocer la autenticidad que tiene el activo de información, identificando a los actores y/o la autorización necesaria, que las personas con poder ofrecen, verificando las cuestiones anteriores (Borrero Ochoa, 2019).
- **Subestado C (Confidencialidad):** La característica encargada de prevenir la divulgación no autorizada de activos de la información es esencial para proteger la privacidad, especialmente cuando la información pertenece a personas (según la ley de protección de datos) (Borrero Ochoa, 2019).
- **Subestado I (Integridad):** Es la protección contra la destrucción no autorizada y la modificación de los activos de información. Esto se refiere a activos de información que pueden ser afectados, por ejemplo, por virus (Borrero Ochoa, 2019).
- **Subastado D (Disponibilidad):** Es la protección de accesos no autorizado a los activos de información del dominio, se relaciona con la fiabilidad de los componentes de manera técnica (Borrero Ochoa, 2019).

2.2.2. Estándar de gestión de seguridad de la información

2.2.2.1. Normas ISO

Se trata de un conjunto de estándares internacionales relacionados con la seguridad de la información. Contienen un conjunto de buenas prácticas

relacionadas con la implementación, el mantenimiento y la mejora de sistemas de gestión de la seguridad de la información.

Un Sistema de Gestión de Seguridad de la Información es un conjunto conformado por políticas y procedimientos que ayudan en la estandarización de la gestión de seguridad de la información (Medina Iriarte, 2020).

a) ISO 27000:

Son un conjunto de requisitos necesarios para poder implementar un SGSI (Sistema de Gestión de Seguridad de la Información). Esto incluye una parte enfocada en la mejora continua, detallando las líneas generales de controles propuestos por los (Medina Iriarte, 2020).

b) ISO 27002:

Se trata de una colección de buenas prácticas orientadas a la seguridad de la información que describe los controles y sus objetivos. Actualmente, consta de 14 dominios, 35 objetivos de control y 114 controles (Medina Iriarte, 2020).

c) ISO 27003:

Es una guía diseñada para asistir en la implementación de un sistema de gestión de seguridad de la información (SGSI) y funciona como apoyo para la norma ISO 27001. Contiene instrucciones detalladas para lograr una implementación exitosa del SGSI (Medina Iriarte, 2020).

d) ISO 27004:

Esta guía incluye recomendaciones para realizar mediciones de gestión de seguridad de la información. Específicamente, detalla la configuración de métricas para medir de forma regular, cómo medirlas y cómo alcanzar los objetivos relacionados con estas métricas (Medina Iriarte, 2020).

e) ISO 27005:

Esta guía contiene recomendaciones para abordar la gestión de riesgos en la seguridad de la información, lo cual es crucial para las organizaciones. Aunque no prescribe una metodología específica para el análisis y gestión de riesgos, proporciona acceso a ejemplos de posibles amenazas, vulnerabilidades y sus impactos (Medina Iriarte, 2020).

f) ISO 27006:

Contiene requisitos para acreditar las organizaciones que certifican.

g) ISO 27007:

Esta guía de auditoría de los sistemas de gestión de seguridad informática establece cómo llevar a cabo auditorías, cuándo realizarlas, cómo seleccionar auditores adecuados, cómo planificar y ejecutar la auditoría, así como sus actividades clave (Medina Iriarte, 2020).

h) ISO /IEC 27001 – 2013:

Considera a la información como un activo crítico dentro de las organizaciones sin distinción del tamaño o el rubro, por lo que es necesario protegerla de manera efectiva y eficiente (Medina Iriarte, 2020).

2.2.3. Gestión de riesgos

Este término se refiere al proceso utilizado para identificar y evaluar riesgos, y luego crear un plan para mitigar y/o controlar los riesgos identificados. Los riesgos pueden originarse por diversas causas, como errores en la gestión o diversas amenazas relacionadas con la ciberseguridad.

La gestión de riesgos generalmente se fundamenta en un documento detallado que abarca diversas técnicas y procesos ejecutados como parte de la metodología. Este documento describe cómo la organización identifica y aborda los riesgos, siguiendo estándares que garantizan la protección tanto de los datos de la empresa como de los clientes (Guevara, 2018).

2.2.3.1.Etapas de la gestión de riesgos

En los procesos de gestión de riesgos, se identifican varias etapas y actividades diferentes. Sin embargo, el ciclo de vida de la gestión de riesgos se puede dividir en cinco etapas, las cuales sirven como base para los principales reglamentos de la gestión de riesgos (Guevara, 2018).

Tenemos:

a) **Identificación.**

   Es el punto de inicio que nos ayuda a descubrir los diferentes riesgos para poder definirlos de manera estructurada.

b) **Evaluación.**

   Se evaluación los riesgos para identificar las probabilidades y el impacto que podría tener (Guevara, 2018).

c) **Tratamiento.**

   Se debe considerar el tratamiento que se debe aplicar para cada riesgo, según un análisis de aceptabilidad del riesgo, que determina la necesidad de implementar planes de acción para la prevención, reducción, o en caso necesario, la transferencia del riesgo (Guevara, 2018).

d) Monitorización.

Es la continua revisión y reevaluación de los posibles riesgos, junto con la monitorización del estado de los tratamientos y controles implementados (Guevara, 2018).

e) Comunicación.

La comunicación es primordial en cada etapa de un proceso de gestión y es crucial para la toma de decisiones efectivas en la gestión de riesgos (Guevara, 2018).

2.2.4. Seguridad informática.

2.2.4.1. Tipos de riesgos

(Muñoz Hernandez, 2019) En las organizaciones, se realizan una variedad de procesos que, si bien aumentan la productividad, también pueden estar expuestos a vulnerabilidades y problemas, lo que implica la existencia de riesgos que deben ser considerados. Los tipos de riesgos más comunes que se pueden identificar son:

- Sistemáticos
- No sistemáticos.
- Financieros.
- Económicos.
- Ambientales.
- Políticos.
- Legales.

2.2.4.2. Seguridad de la información

La seguridad de la información comprende el conjunto de medidas y técnicas empleadas para controlar y proteger los datos dentro de una empresa u

organización, garantizando que la información no salga del sistema. Es crucial para permitir que las empresas lleven a cabo sus operaciones de manera segura y eficiente. (Muñoz Hernandez, 2019).

a) Tipos de seguridad informática

Tenemos tres tipos de seguridad informática.

- **Seguridad de red.**

  La protección de la red es crucial, al igual que la seguridad de los equipos. Se centra en las acciones necesarias para asegurar el acceso, garantizar la seguridad y preservar la integridad de la red y los datos que se transmiten a través de ella (Muñoz Hernandez, 2019)

- **Seguridad de software.**

  Los softwares consisten en aplicaciones y programas instalados en diversos dispositivos, siendo vulnerables a diversos tipos de ataques que pueden afectar su funcionamiento o resultar en el robo de información. Por ello, es fundamental proteger este entorno para asegurar la seguridad de los datos dentro de la organización, garantizando la disponibilidad y autenticación de estos softwares (Muñoz Hernandez, 2019).

- **Seguridad de hardware.**

  Los sistemas de seguridad para el hardware ofrecen el más alto nivel de protección. Es posible evaluar los puntos débiles de los diferentes dispositivos desde el momento de su fabricación (Muñoz Hernandez, 2019).

2.2.4.3. Tecnologías de la información

En términos generales, las nuevas tecnologías en información y comunicación se apoyan en tres medios básicos: la informática, la microelectrónica y las telecomunicaciones. Estos no operan de manera aislada, sino que interactúan significativamente y están interconectados, lo que facilita la creación de nuevas realidades en la comunicación (yala Ñiquen, 2019)

Capítulo 3

Desarrollo del proyecto

3.1. Desarrollo del plan de gestión de seguridad in- formativa (SGSI)

Se aplicarán las cuatro etapas del método DEMING (Planificar-Hacer-Verificar-Actuar), en conjunto con las once fases establecidas por ISACA en Auditoría y Control de Sistemas de Información (ISO, 2014).

I Etapa 1: Planear

Esta etapa está conformada por cinco fases donde se identifican los objetivos y el alcance del proyecto. Se obtiene el apoyo del personal encargado de la organización y se realiza un inventario de los diferentes activos informáticos (ISO, 2014).

1) **Fase 1: Identificar los objetivos de negocio**

Considerando la misión, visión y los requerimientos de la Municipalidad de Challhuahuacho, se han determinado los objetivos que deben considerarse para el desarrollo del Plan de Seguridad Informática, los cuales se detallan en la Figura 4 y Figura 5

Figura 4

Misión y visión de la Municipalidad Distrital de Challhuahuacho

MISION INSTITUCIONAL
Promover el desarrollo integral del Distrito de Challhuahuacho brindando servicios de calidad de manera eficiente y eficaz con una gestión transparente con responsabilidad en el óptimo manejo de los recursos participativa y transparente
VISIÓN INSTITUCIONAL
Edificar una municipalidad transparente líder en la región y ser reconocidos por la mejora constante en nuestra labor proactiva y eficiente que nuestros trabajadores ofrecen en favor a la población

Figura 5

Objetivos identificados para SGSI

OBJRTIVOS IDENTIFICADOS PARA LA IMPLEMENTACIÓN DEL SSGI
- Asegurar que los activos de información de la Municipalidad Distrital de Challhuahuacho se encuentren debidamente protegidos y cuenten con respaldos. - Asegurar a los usuarios de la Municipalidad el compromiso de mantener la seguridad de información, su privacidad y protección a través de la protección informática - Implementación de políticas de seguridad informática para respaldar la protección de información y datos de los usuarios asi como los de la Municipalidad Distrital de Challhuahuacho.

2) **Fase 2: Obtener apoyo de la administración.**

Como primer paso, se elaboró un acta de constitución del proyecto para implementar el plan de seguridad informática, basándose en los objetivos y alcances identificados dentro de la Municipalidad. Este documento se presentó al área funcional de Tecnologías de la Información (ver Anexo 02). Además, se diseñó una política general de seguridad de la información en colaboración con el responsable del área funcional de Tecnologías de la Información de la Municipalidad de Challhuahuacho. Esta política define responsabilidades y sanciones que deben aplicarse en caso de violación de la seguridad, contribuyendo así a establecer compromisos claros.

3) Fase 3: Seleccionar el alcance adecuado

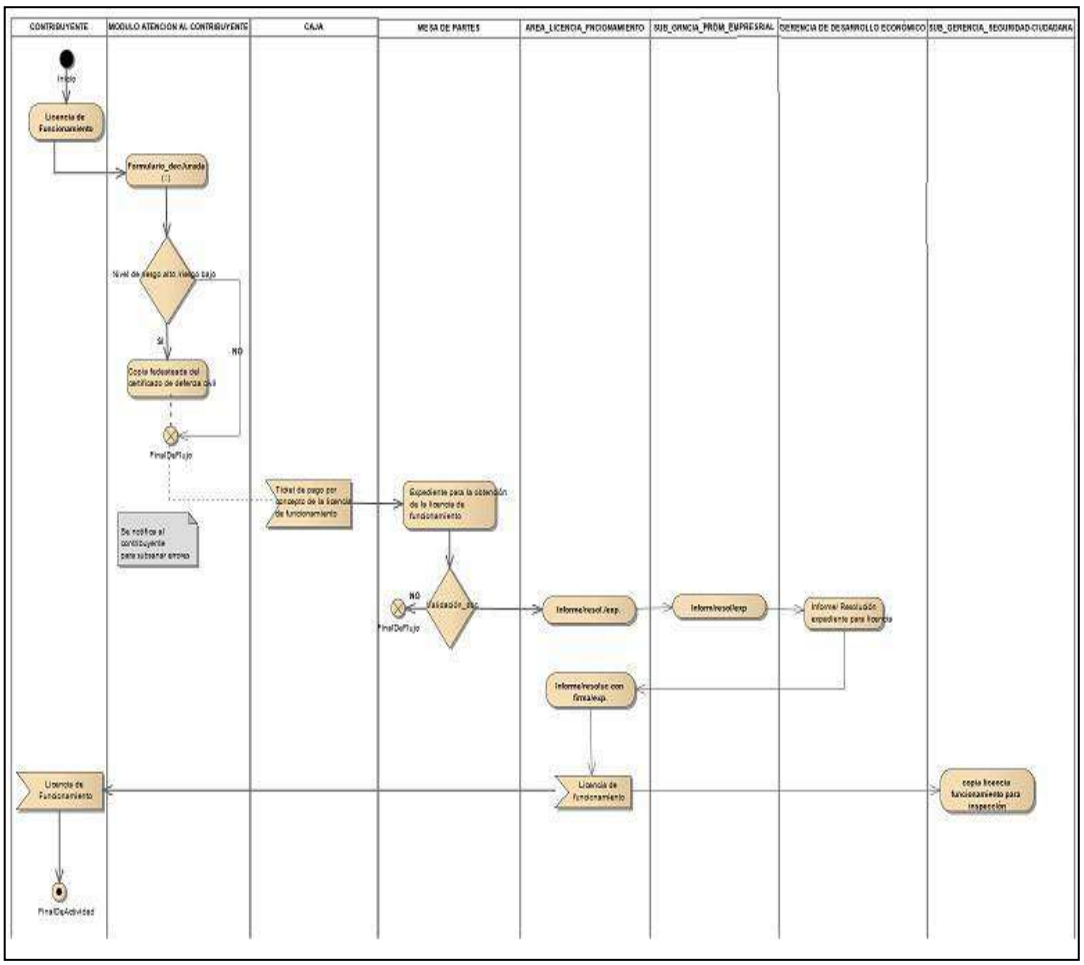
El alcance para la implementación del plan de gestión de seguridad informática se determinó en función de los objetivos establecidos según la misión y visión de la Municipalidad. Se identificaron los diferentes procesos que la Municipalidad lleva a cabo en sus funciones, los cuales

están expuestos a diversas amenazas y vulnerabilidades en la información que manejan. Estos procesos incluyen:

a. Diagrama de procesos de trámites municipales

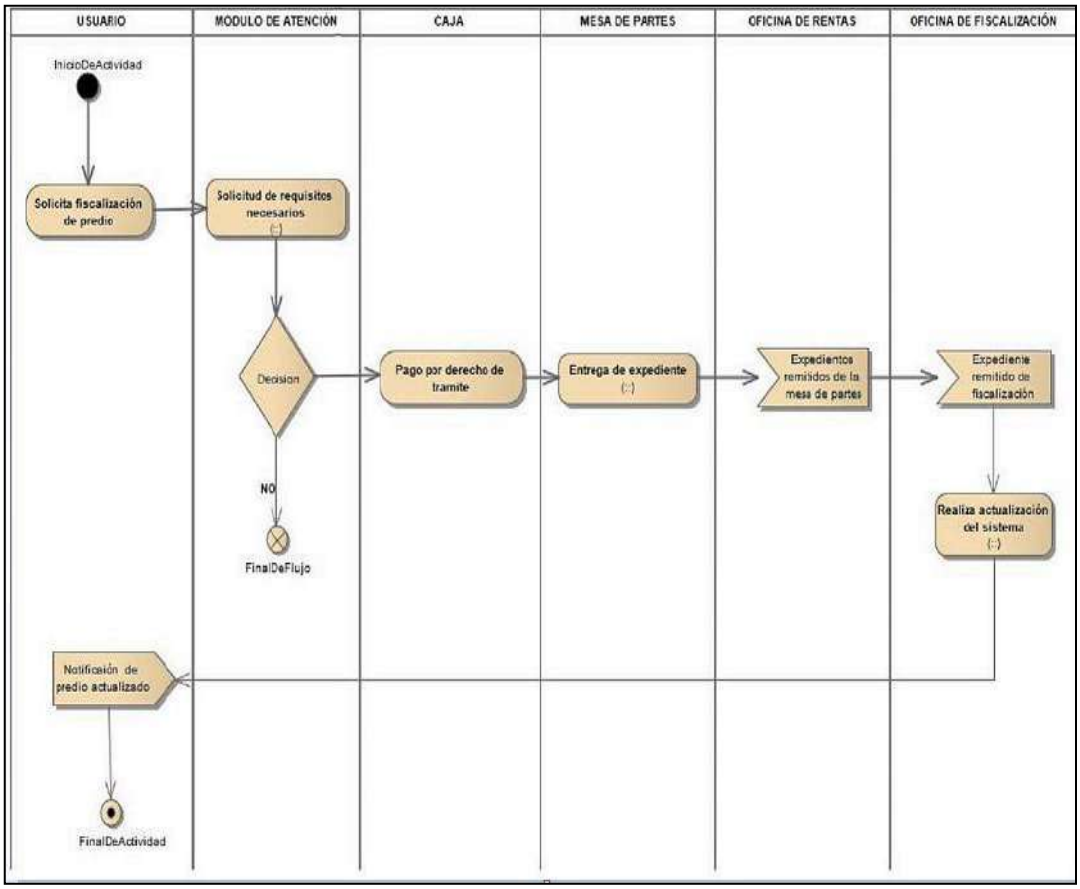
- Licencias de funcionamiento

Figura 6
Diagrama de procesos licencias de funcionamiento



- Licencias de edificación

Figura 7
Diagrama de procesos licencias de funcionamiento



b. Diagrama de procesos de registro y estado civil

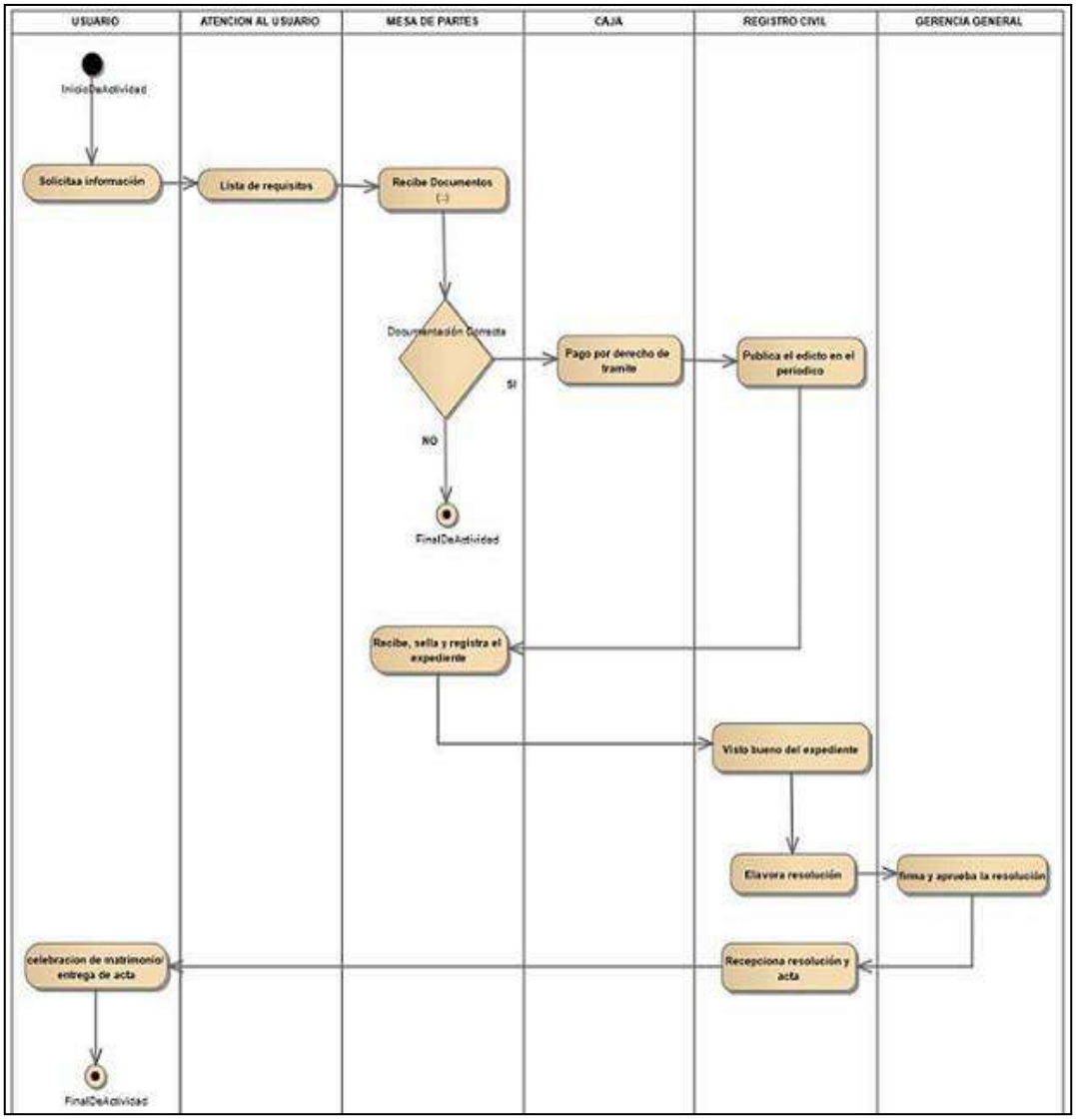
- Matrimonio civil

  Es necesario iniciar el proceso presentando una solicitud de matrimonio en la oficina de registro civil, donde se proporcionará al solicitante la lista de requisitos necesarios. Tras la revisión de los documentos y la confirmación de su conformidad, el solicitante deberá efectuar el pago correspondiente en caja. Posteriormente, se coordinará la fecha de la ceremonia de matrimonio civil y se procederá a la publicación del edicto a través del área de registro civil. Una vez completados estos pasos, se procede a la firma y el

sellado del registro de matrimonio en la mesa de partes. El área de registro civil otorgará su visto bueno y emitirá la resolución correspondiente, la cual será firmada por la gerencia general. Esto permitirá llevar a cabo la ceremonia de matrimonio. Finalmente, se obtendrá el certificado de matrimonio que servirá como prueba legal de la unión.

Figura 8

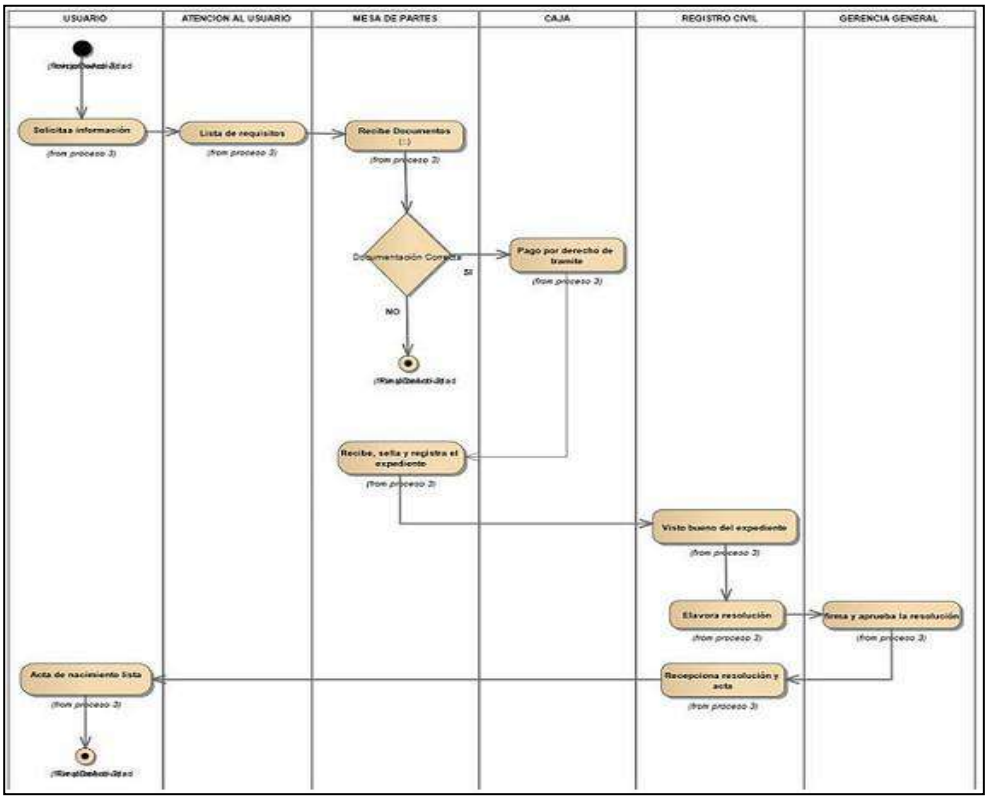
Diagrama de procesos registro *matrimonio civil*



- Registro de nacimiento

  El registro de nacimiento implica notificar oficialmente el nacimiento a las autoridades. En este proceso, se proporcionan documentos y detalles sobre el bebé, se visita la oficina de registro civil para solicitar la información necesaria y verificarla. Luego, se presenta la documentación requerida en mesa de partes, donde se verifica su precisión. Si toda la documentación es correcta, se realiza el pago correspondiente por el trámite. Los documentos son recibidos, sellados y firmados en mesa de partes. Posteriormente, se obtiene el visto bueno del área de registro civil y se elabora una resolución que, finalmente, es firmada por el gerente general. El resultado es la obtención de un certificado de nacimiento.

Figura 9
Diagrama de procesos registro de nacimiento

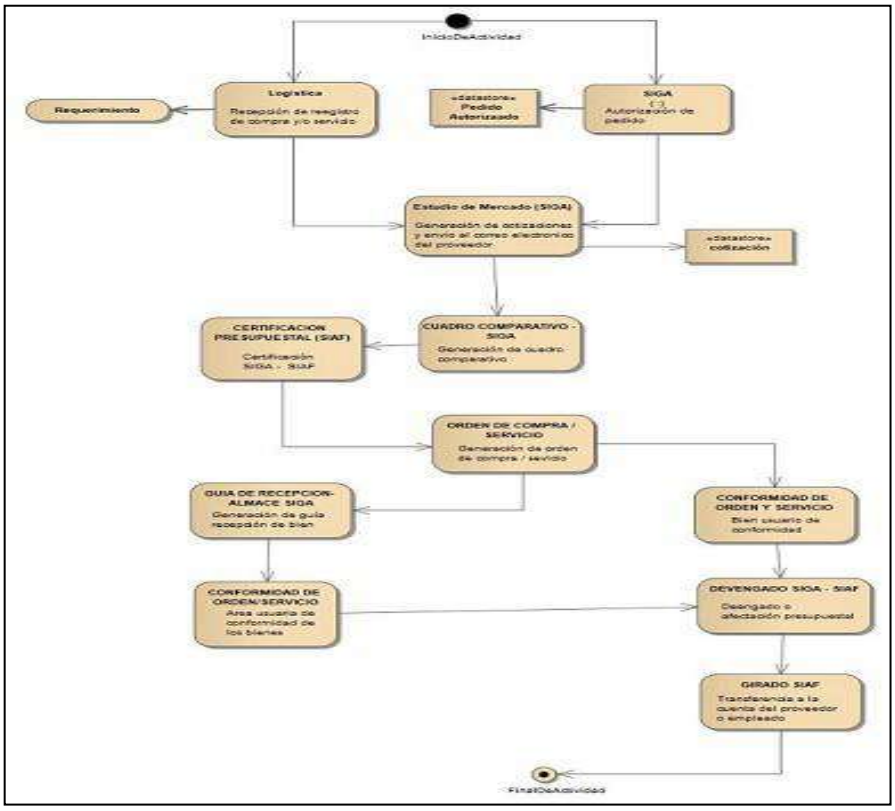


c. Gestión de documentos

- SIGA - SIAF

  El proceso de gestión documentaria dentro de los sistemas SIGA (Sistema Integrado de Gestión Administrativa) y SIAF (Sistema Integrado de Administración Financiera) implica la creación, registro y control de documentos administrativos y financieros en entidades gubernamentales. Esto abarca la generación de documentos, su clasificación, archivo y la gestión de flujos documentales para autorizaciones y trámites. Estos sistemas permiten un seguimiento eficiente de los procedimientos y la generación de reportes para una gestión transparente y eficaz de los recursos públicos.

Figura 10
Diagrama de procesos gestión *documentaría*



Para realizar el análisis de riesgos, es fundamental estandarizar los activos mediante siglas que los identifiquen claramente. En la Tabla 1 se detallan los tipos de activos que serán codificados de esta manera.

Tabla 1
Codificación de identificación de tipo de activo

Tipo de Activo Asignada	**Sigla**
Instalaciones	(L)
Personal	(P)
Equipos Informáticos	(HW)
Software y aplicaciones	(SW)
Servicios	(S)
Redes de comunicación	(RC)

***Fuente**: MAGERIT - catálogo de elementos.*

4) Fase 4: Definir un método de evaluación de riesgos

En este punto, es crucial entender el nivel de riesgo y las vulnerabilidades a las que están expuestos los distintos activos de información de la Municipalidad Distrital de Challhuahuacho. Utilizamos la norma ISO/IEC 27001:2013, que ofrece una lista detallada de amenazas y vulnerabilidades relacionadas con los activos de información considerados relevantes, como se muestra en la Tabla 2.

Tabla 2.:
Amenazas y vulnerabilidades que afecta a los activos

CODIGO	AMENAZAS POR SU ORIGEN	AMENZA	VULNERABILIDAD
N	NATURAL	• Fuego • Daños por agua • Humedad • Corte de servicio eléctrico	Falta de sistemas contra incendios Falta de protección contra el agua Problemas estructurales de mobiliarios del hogar donde se encuentra el activo Falta de control de temperatura
I	INDUSTRIAL	• Contaminación electromagnética • Avería de origen físico y lógico • Falla con el servicio de comunicaciones	Mal funcionamiento de la unidad de protección auxiliar No contar con generadores auxiliares Falta de mantenimiento periódico Falta de control en la manipulación de conexiones de red
E	PERSONA (CAUSA ACCIDENTAL)	• Errores de configuración • Expansión de software dañino • Mal uso de software • Destrucción de soporte de	Falta de conocimiento en el uso de aplicaciones, equipos y de sistemas Falta de uso de software de protección (antivirus) Desactualización de software, fallas en el mantenimiento de software Falta de control del manejo de dispositivos de

		almacenamiento de información	almacenamiento (HD, USB, DVD)
		• Uso no previsto de la información	Falta de control en la manipulación de la información.
		• Caída de servidor	Errores del administrador en la configuración, errores de secuencia Equipos obsoletos, poca capacidad de almacenamiento y procesamiento, errores de usuario
		• Caída del sistema	No se garantiza el uso de respaldos
		• Mala restauración de respaldos	Falta de control de actualizaciones de equipos poco o nulo
		• Fallas en el mantenimiento y actualización de equipos	Falta de uso de políticas de control Falta de mecanismo para el control de acceso a usuarios
E	PERSONA (CAUSA PROVOCADA)	• Indisponibilidad del personal	Falta de responsabilidad ausencia en el área de trabajo
		• Usurpación de identidad	Falta de control en la seguridad para permitir cambios de información en validación de usuarios
		• Indisponibilidad del personal	Cambios intencionados de contraseña
		• Abuso de privilegios de acceso	Falta de mecanismos para el control de almacenamiento
		• Difusión de la información	

	• Destrucción de la información • Modificación deliberada de la información • Robo • Cambio en los contenidos de software • Manipulación en los equipos de computo	y la protección de la información Falta de control de entrada y salida de información y recursos Falta de control en la manipulación de programas Falta de control en cambios y manipulación de los equipos de computo

Los riesgos identificados han sido evaluados según su nivel de criticidad y se han categorizado como altos y críticos. Siempre se consideran los principios básicos de seguridad de la información, tal como lo establece la norma ISO/IEC 27001:2013, como se muestra en la Tabla 3.

- Disponibilidad.
- Integridad.
- Confidencialidad.

Tabla 3
*Codificación de principios de **seguridad** según ISO/IEC 27001:2014*

Principios	**Sigla Asignada**
Disponibilidad	(D)
Integridad	(I)
Confidencialidad	(C)

***Fuente**: ISO/IEC 27001:2014.*

Principio de disponibilidad (D)

Con este principio se pretende garantizar que el escenario tenga un acceso oportuno por parte de los usuarios a los activos en el momento necesario *Tabla 4.*

Tabla 4*: Valoración de disponibilidad*

Disponibilidad		Descripción
1	**B (Bajo**	Si la información no está disponible no tiene efecto en la operación
2	**M (Medio)**	Si la información no esta disponible si tendría algo de efecto en las operaciones, pero se pueden usar alternativas para las operaciones.
3	**A (Alto)**	Si la información no esta disponible causará un efecto fatal en las operaciones

Fuente: MAGERIT - catálogo de elementos.

Principio de integridad (I)

Con este principio se busca instar a que el escenario contenga la información que el activo la procese, este completa y exacta Tabla 5.

Tabla 5
Valorización de integridad

Integridad		Clase Descripción
1 Usado para consultas	**B (Bajo)**	No Necesaria
2 Si el contenido fuera falso, se tendría problemas pero no afectara mucho las operaciones	**M (Medio)**	Necesaria
3 Si se pierde la integridad	**A (Alto)**	Importante tendrían efectos fatales

Fuente: MAGERIT - catálogo de elementos

Principio de confidencialidad(C)

Con este criterio se pretende asegurar si la información está disponible solo para los usuarios autorizados a su acceso Tabla 6.

Tabla 6
Valoración de confidencialidad

Confidencialidad		Clase	Descripción
Valor Cuantitativo	**Valor Cualitativo**		
1	B (bajo)	Pública	LA información se puede proporcionar a terceras personas
2	M (Medio)	Uso Interno	LA información se puede revelar no tendría gran efecto en las personas
3	A (Alto)	Secreto	La información sólo se puede proporcionar a usuarios específicos

- **Identificación de amenazas**

  Las amenazas pueden causar diversos daños a los activos y, en consecuencia, a la entidad u organización. Estas amenazas se pueden identificar según su origen, como se muestra en la Tabla 7.

  Tabla 7
  Codificación de identificación de tipo de amenaza

Tipo de amenaza	Sigla asignada
Ataque	(A)
Errores Humanos	(E)
Origen Industrial	(I)
Origen Natural	(N)

Fuente: MAGERIT - catálogo de elementos.

- **Análisis y evaluación de riesgos**

  Identificación de riesgos

  Se establecerán los tipos de amenazas y vulnerabilidades que afectan la seguridad informática de la Municipalidad Distrital de Challhuahuacho para su análisis y evaluación. En la Tabla 8 se

detallan el origen de las amenazas, el tipo de activo afectado y su impacto.

Tabla 8
Identificación de amenazas y vulnerabilidades

CLASIFICACIÓ DE ACTIVO	TIPO DE ACTIVO	ACTIVO	AMENZA	VULNERABILIDAD
ACTIVOS ESENCIALES	DATOS	Datos de tramite interno	Corte de servicio eléctrico Destrucción de información Modificación deliberada de información Difusión de información	Mal funcionamiento de la unidad de protección auxiliar, no contar con generadores auxiliares Falta de mecanismos para el control de almacenamiento y la protección de la información
		Multimedia (información de audio y video) USB	Degradación de soportes de almacenamiento de información Uso no previsto de información	Falta de mantenimiento periódico Falta de control en la manipulación
	INFORMACIÓN	Documentos	Destrucción de información Divulgación de la información Degradación de soportes de almacenamiento Condiciones inadecuadas de temperatura humedad	Falta de mecanismos para el control de almacenamiento y la protección de la información Falta de mantenimiento periódica Falta de control de temperatura
		Información pública	Difusión de información Abuso de privilegios de acceso	Falta de mecanismos para el control de almacenamiento y la protección de la información

APLICAIONES INFORMATICAAS	SERVICIO	Información clasificada	Difusión de información Modificación deliberada de la información	Falta de control en la seguridad para permitir cambios de información en validación de usuarios, cambios de contraseña Falta de mecanismos para el control de almacenamiento y la protección de la información
		Internet	Corte de servicio eléctrico	Mal funcionamiento de la unidad de protección auxiliar, no contar con generadores auxiliares
		Correo electrónico	Avería de origen físico o lógico Fallo del servicio de comunicaciones Usurpación de identidad Interrupción de otros servicios y suministros esenciales	Falta de mantenimiento periódico Falta de control en la manipulación de conexiones de red Falta de mecanismos para el control de acceso de usuarios
	SOFTWARE	Sistema operativo	Abuso de privilegios de acceso Acceso no autorizado Errores del administrador Vulnerabilidad de los programas	Falta de control en la seguridad para permitir cambios de información en validación de usuarios, cambios intensionales de contraseña
		SIGA	Fugas de información Caída del sistema por agotamiento de recursos	Falta de mecanismos para el control de acceso de usuarios Falta de conocimiento en el uso de aplicaciones equipos y de sistemas
		SIAF	Errores del administrador Vulnerabilidad de software	Falta de mantenimiento periódico
		MsOficce	Manipulación de la configuración Errores de mantenimiento o actualización	Falta de mecanismos para el control de almacenamiento de la protección de la información
		Antivirus	Errores de configuración Errores de mantenimiento, actualización	Errores del administrador, errores de configuración, errores de secuencia
		Sistema Tramite Documentario	Suplantación de identidad de usuario Divulgación de la información	Equipos obsoletos, poca capacidad de almacenamiento y procesamiento, errores de los usuarios

EQUIPOS INFORMATICOS	HARDWARE	Página web	Manipulación de la configuración Manipulación de software Caída de sistema Vulnerabilidad de software	Falta de conocimiento en el uso de las aplicaciones, equipos y de sistemas Desactualización de software fallas en el mantenimiento del software Falta de uso de software de protección antivirus
		Sistema de respaldo de información	Manipulación de la configuración Errores de configuración Mala gestión	Falta do control en la manipulación de programas Falta de conocimiento en el uso de aplicaciones equipos y de sistemas
		Impresora institucional	Avería de origen físico o lógico Errores de usuario	Falta de mantenimiento periódico
		Servidor	Fenómenos climáticos Corte de suministro eléctrico Fallos del servicio de comunicaciones. Errores de mantenimiento o actualización de software	Problemas estructurales de mobiliario del lugar donde se encuentra el activo Falta de control en la manipulación de conexiones de red Falta de control en la manipulación de programas
		Equipo de computo	Fenómeno climático Avería de origen físico o lógico Falla de mantenimiento o actualización de equipos de hardware Manipulación de configuración Robo Corte de servicio eléctrico	Falta de control de manipulación de programas Falta de control de entrada y de salida de información y recursos Mal funcionamiento de la unidad de protección auxiliar con contar con generadores auxiliares

COMUNICACIONES	**REDES DE COMUNICACION**	Red Local	Fallo de servicios de comunicaciones Interrupción de suministros esenciales Caída del sistema por agotamiento de recursos	Falta de control de la manipulación de conexione de red. Mal funcionamiento de la unidad de protección auxiliar no contar con generadores auxiliares
		Red Privada Virtual	Interrupción de otros servicios y suministros esenciales Fallo de servicios de comunicaciones	Errores del administrador, errores d configuración, errores de secuencia Equipos obsoletos, poca capacidad de almacenamiento y procesamiento errores de los usuarios
		ADSL	Fallo de servicios de comunicaciones Errores de configuraciones	Problemas estructurales de mobiliarios del lugar donde se encuentra el activo
		Red Inalámbrica	Errores de configuraciones Errores de mantenimientos Errores de actualización de equipos o hardware	Falta de control en la manipulación de red Falta de control en la manipulación de programas Falta de control de actualización de equipos poco o nulo Desactualización de software fallas en el mantenimiento del software
PERSONAL	**PERONAL**	Alcaldía	Indisponibilidad del personal Abuso de Privilegios de acceso	Falta de responsabilidad, ausencia en el área de trabajo
		Gerencia General	Suplantación de identidad de usuario Indisponibilidad del personal Abuso de Privilegios de acceso Suplantación de identidad de usuario	Falta de control en la seguridad para permitir cambios de información en validación de usuario, cambios intencionados de contraseña Falta de responsabilidad, ausencia en el área de trabajo
		Gerencia de Secretaría General	Abuso de Privilegios de acceso Suplantación de identidad de usuario	Falta de control en la seguridad para permitir cambios de información

		Indisponibilidad del personal	en validación de usuario, cambios intencionados de contraseña
	Gerencia de Administración	Abuso de Privilegios de acceso	
		Suplantación de identidad de usuario	
		Indisponibilidad del personal	Falta de responsabilidad, ausencia en el área de trabajo
	Gerencia de Administración tributaria	Abuso de Privilegios de acceso	
		Suplantación de identidad de usuario	Falta de control en la seguridad para permitir cambios de información
		Indisponibilidad del personal	en validación de usuario, cambios intencionados de contraseña
	Gerencia de Desarrollo Social y Económico	Abuso de Privilegios de acceso	Falta de responsabilidad, ausencia en el área de trabajo
		Suplantación de identidad de usuario	
		Indisponibilidad del personal	Falta de control en la seguridad para permitir cambios de información en validación de usuario, cambios intencionados de contraseña
	Gerencia de Medio Ambiente	Abuso de Privilegios de acceso	Falta de responsabilidad, ausencia en el área de trabajo
		Suplantación de identidad de usuario	Falta de control en la seguridad para permitir cambios de información en validación de usuario, cambios intencionados de contraseña
		Indisponibilidad del personal	Falta de responsabilidad, ausencia en el área de trabajo
	Gerencia de infra estructura y desarrollo territorial	Abuso de Privilegios de acceso	Falta de control en la seguridad para permitir cambios de información en validación de usuario, cambios intencionados de contraseña
		Suplantación de identidad de usuario	
		Indisponibilidad del personal	Falta de responsabilidad, ausencia en el área de trabajo
	Gerencia de Planeamiento y Presupuesto	Abuso de Privilegios de acceso	Falta de control en la seguridad para permitir cambios de información en validación de usuario, cambios intencionados de contraseña
		Suplantación de identidad de usuario	
	Gerencia de asesoría jurídica	Indisponibilidad del personal	Falta de responsabilidad, ausencia en el área de trabajo Falta de control en la seguridad para permitir cambios de información

	Abuso de Privilegios de acceso Suplantación de identidad de usuario Indisponibilidad del personal	en validación de usuario, cambios intencionados de contraseña Falta de responsabilidad, ausencia en el área de trabajo
Área de Estadística	Abuso de Privilegios de acceso Suplantación de identidad de usuario Indisponibilidad del personal	Falta de control en la seguridad para permitir cambios de información en validación de usuario, cambios intencionados de contraseña
Área de Informática	Abuso de Privilegios de acceso Suplantación de identidad de usuario	

- **Análisis de riesgos**

  A través del análisis de riesgos, se busca identificar los diferentes riesgos y las causas que pueden provocar situaciones críticas para los activos frente a las amenazas y vulnerabilidades. La valoración de estos activos se realizará considerando los principios mencionados en la norma ISO 27001-2014. Estos principios serán evaluados según los fundamentos de la metodología MAGERIT. La valoración puede ser cualitativa o cuantitativa, y se asignará la puntuación que se considere conveniente.

- **Evaluación de riesgos**

  Llevaremos a cabo la evaluación de los diferentes riesgos, considerando las medidas y tomando como referencia los criterios que maneja la metodología MAGERIT, como se muestra en las Tablas 9, 10, y 11. Esta metodología nos ayudará a valorar las ocurrencias de las amenazas y las vulnerabilidades, permitiendo obtener el nivel total de riesgo.

Tabla 9

Criterios para valorar que ocurra la amenaza

Nivel		Descripción
1	B (Bajo)	Fenómeno que rara vez ocurre
2	M(Moderado)	Probable que pueda ocurrir
3	A(Alto)	Existe gran probabilidad

***Fuente**: MAGERIT* catálogo de elementos

Tabla 10

Criterios para valorar vulnerabilidad

Nivel		Descripción
1	B (Bajo)	Existen controles suficientes
2	M(Moderado)	Se presentan algunos controles
3	A(Alto)	No se tienen controles y/o no

***Fuente**: MAGERIT - catálogo de elementos*

Tabla 11

Criterios para valorar riesgos

Nivel		Descripción
1	Insignificante B (Bajo)	Impacto muy bajo - no necesita ninguna acción
2	Menor B(Bajo)	Efectos menores - no es necesario acciones
3	Poco significativo M(Moderado)	Algún efecto negativo no es necesario acciones
4-6	Significativo M(Moderado)	Efecto negativo, riegos considerado aceptable
7-8	Importante A (Alto)	Tendrían efectos negativos serios
9	Mayor A(Alto)	Los efectos negativos serian mayores se deben reducir necesariamente

.

***Fuente:** MAGERIT- catálogo de elementos*

Luego de tener las diferentes tablas de valoración, procederemos a aplicarlas en la evaluación de los distintos activos identificados en la Municipalidad de Challhuahuacho. Esto nos permitirá determinar el nivel de riesgo asociado a cada activo y establecer las medidas necesarias para su protección.

- **Valoración de amenazas y vulnerabilidades**

  En este paso se medirá el efecto adverso vinculado a los diferentes activos de la Municipalidad de Challhuahuacho en caso de que se materialice un riesgo. Existe la posibilidad de que este impacto sea identificado como crítico. En tal caso, realizaremos la sumatoria de las vulnerabilidades para obtener un promedio y así determinar el impacto total.

Valoración del riesgo

En este momento, se realizará la multiplicación entre el valor del activo y los valores de la amenaza y la vulnerabilidad. De esta manera, obtendremos el nivel de riesgo correspondiente a la amenaza en los activos, como se muestra en el ejemplo de la Figura 11

Figura 11
Dominios y controles

5) **Fase 5: Preparar un inventario de los activos de información**

En esta fase se presentan los activos identificados en la Municipalidad de Challhuahuacho. Además, se realizará la valoración de estos activos, identificando los procesos más críticos. Para ello, se tomará en cuenta la clasificación según los diferentes tipos de activos, como se muestra en la Tabla 12.

Tabla 12

Activos identificados en la Municipalidad Distrital de Challhuahuacho

CLASIFICACIÓN DE ACTIVO	TIPO DE ACTIVO	CODIGO	ACTIVO
ACTIVOS ESENCIAL	DATOS INFORMACIÓN SERVICIOS	**S**	Dato de trámite interno Multimedia UB Documentos Información Clasificada Internet Correo Electrónico Sistema Operativo SIGA SIAF
APLICACIONES INFORMATICAS	SOFTWARE	**SW**	MicroSoft Office Antivirus Sistema Trámite Documentario Página We Sistema de Respaldo de Información
EQUIPOS INFORMATICOS	HARDWARE	**HW**	Impresora Institucional Servidor Equipos de Computo Laptops Scaner Modem Switch
COMUNICACIONES	REDES DE COMUNICACIONES	**RC**	Red Local Internet Red Privada Virtual Red Telefónica ADSL Red Inalámbrica
EQUIPAMIENTO AUXILIAR	EQUIPAMIENTO	**I**	Sistema de almacenamiento ininterrumpida Fuentes de alimentación Cableado
PERSONAL	PERSONAL	**P**	Alcaldía Gerencia General Gerencia de secretaria general Gerencia de administración

			Gerencia de administración tributaria Gerencia de desarrollo social y económico Gerencia de medio ambiente Gerencia de infra estructura Gerencia de Planeamiento y presupuesto Gerencia de asesoría jurídica Área de estadística Área de informática

Una vez identificados los activos de la Municipalidad de Challhuahuacho, se calculará el promedio de los valores de cada activo, considerando su disponibilidad, integridad y confidencialidad. Este cálculo se realizará utilizando los valores asignados para cada uno, como se muestra en las Tablas 4, 5 y 6. Si el promedio obtenido es igual o mayor a 3, se procederá con un análisis de riesgos para aplicar un tratamiento y proponer controles. Estos activos son los que deben ser protegidos.

La valoración de los diferentes activos, considerando cada principio mencionado, se realizará según lo que se muestra a continuación en la tabla 13.

Tabla 13

Evaluación de activos

CODIGO	ACTIVO	CRITERIO DE VALORACION			
		C	D	I	VALOR FINAL
S-1	Datos de trámite interno	2	3	1	**2**
S-2	Multimedia (información en audio y video)	0	2	1	**1**
S-3	USB	3	2	2	**2**
S-4	Documentos	3	3	2	**3**
S-5	Información Pública	2	2	2	**2**
S-6	Información Clasificada	2	3	2	**2**
S-7	Internet	3	3	3	**3**
S-8	Correo electrónico	3	2	3	**3**
I-1	Sistema de almacenamiento ininterrumpida	2	2	1	**2**
I-2	Fuentes de alimentación	1	1	1	**1**
I-3	Cableado	1	2	1	**1**
P-1	Alcaldía	2	3	3	**2**
P-2	Gerencia General	2	2	2	**2**
P-3	Gerencia de Administración	2	3	3	**2**

P-4	Gerencia de Administración Tributaria	2	2	3	**2**
P-5	Gerencia de Desarrollo	2	2	2	**2**
P-6	Gerencia de medio ambiente	2	3	2	**2**
P-7	Gerencia de infraestructura	2	3	2	**2**
P-8	Gerencia de planeamiento	2	3	2	**2**
P-9	Gerencia de asesoría jurídica	2	2	2	**2**
P-10	Área de estadística	2	3	2	**2**
P-11	Área de informática	2	2	2	**2**
P-12	Usuarios externos	2	3	2	**2**
P-13	Proveedores	1	3	2	**2**
P14	Sistema Operativo	2	3	3	**2**
SW-1	SIGA	2	3	3	**2**
SW-2	SIAF	2	2	3	**3**
SW-3	MicroSoft office	3	2	2	**3**
SW-4	Antivirus	3	3	2	**2**
SW-5	Sistema de trámite documentario	3	3	2	**2**
SW-6	Página web	1	2	1	**1**
SW-7	Sistema de respaldo de información	3	3	3	**3**
HW-1	Impresora institucional	3	1	2	**2**
HW-2	Servidor	2	3	3	**3**
HW-3	Equipo de computo	3	3	3	**3**
HW-4	Laptops	3	3	2	**3**
HW-5	Scaner	2	2	2	**2**
HW-6	Modem	3	3	2	**3**
HW-7	Switch	2	2	2	**2**

II Etapa 2: Hacer

En esta fase, responderemos a los diversos riesgos identificados. Se establecerán políticas que incluirán controles y herramientas de capacitación (ISO, 2014).

1) Fase 6: Gestionar los riesgos y crear un plan de tratamiento de riesgos

Una vez valorado los activos se identificarán cuáles son las amenazas y riesgos a los que se expone cada activo, como se muestra en la siguiente tabla 14.

Tabla 14

Evaluación de los activos identificados en la Municipalidad Distrital de Challhuahuacho

CODIGO RIESGO	CODIGO ACTIVO	ACTIVO	ORIGEN DE AMENAZA	AMENAZA	VALOR DE AMENAZA	POSIBILIDAD OCURRENCIA AMENZA	VULNERABILIDD	VALOR VULNERABILIDAD	VALOR ACTIVO RIEGO ANTE VULNERABILIDAD	TOTAL RIESGO	NIVEL RIESGO
R1	**S**	INTERNET	A	Exposición a phishing	**2**	**3**	Falta de monitoreo de recurso para procesar información	**3**	**2**	**6**	**SIGNIFICATIVO**
R2			A	Exposición a riesgos con virus	**3**		Falta de monitoreo de recursos para procesar información	**2**			
R3			A	La configuración de contraseña se encuentra expuesta	**2**		No se finaliza la acción por el usuario	**2**			
R4			I	Corte de servicio eléctrico	**3**		La arquitectura de red es insegura	**3**			
R5			E	Conexión de terceros a la red	3						
R6	**S**	CORREO ELECTRÓNICO	E	Manipulación de acceso	2	3	Gestión pobre de contraseñas	2	3	7	**IMPORTANTE**
R7			A	Se encontraron mensajes SPAM con contenido malicioso	3		Parámetros configurados incorrectamente	2			
R8			A	Se encontró mensajes con contenido PISHING	3			3			
R9			A	Se encontró correos con presencia de falsas notificaciones	2						
R10	**SW**	SIGA	E	Mal funcionamiento de software	3	2	Errores de mantenimiento y actualización de software	2	2	4	**SIGNIFICATIVO**
R11			E	Errores de administrador	2		Falta de documentación	1			
R12			I	Caída del sistema por agotamiento de recursos	1		Falta de respaldos	3			
R13			E	Abuso de privilegios de acceso	2		Errores de distribución de acceso	2			
R14			A	Acceso no autorizado	2		No se finaliza sesión por el usuario	1			

R15			E	Errores de administrador	2		Errores de mantenimiento y actualización de software	2			SIGNIFICATIVO
R16	**SW**	SIAF	I	Caída del sistema por agotamiento de recursos	1	2	Falta de documentación	1	2	4	
R17			E	Abuso de privilegios de acceso	2		Falta de documentación	2			
R18			E	Acceso no autorizado	2		Falta de respaldos	2			
R19			E	Falta de instalación de antivirus	3		Falta de mantenimiento lógico	2			**SIGNIFICATIVO**
R20			I	Incompatibilidad de software	1		Defectos de software	2			
R21	**SW**	ANTIVIRUS	E	Falta de actualización de antivirus	2	2	Falta de monitoreo de recursos para procesar información	2	3	6	
R22			E	Falta de activación y autenticación de antivirus	3		Mantenimiento lógico insuficiente	2			
R23			I	Software funciona mal	3		Erro de mantenimiento y actualización de software	2			**SIGNIFICATIVO**
R24	**SW**	SISTEMA DE TRAMITE DOCUMENTARIO	E	Errores de administrador	2	2	Parametrar configuración incorrectamente	1	2	4	
R25			I	Caída del sistema por agotamiento	1		Falta de respaldos	2			
R26			E	Acceso no autorizado	2		Error en la distribución de acceso	2			
R27			E	Alteración accidental de la información	3		Parametrar configuración incorrectamente	3			**MAYOR**
R28	**SW**	SISTEMA DE RESPALDO DE INFORMACIÓN	E	Error en la creación de respaldo	3	3	Fallos en los procesos de crear respaldos	3	3	3	
R29			E	No existen respaldos	3		No se tienen políticas de respaldos	3			
R30			M	Exceso de temperatura y humedad	2		Susceptible a polvo y suciedad	3			
R31			E	Inexistencia de equipos para mantener temperatura ideal	3		Mantenimiento de equipo insuficiente	2			**SIGNIFICATIVO**
R32			E	No se tiene un control adecuado en el mantenimiento de equipo	2		Falta de pruebas suficientes del software	1			
R33	**HW**	SERVIDOR	E	No se actualiza el software de manera continua	3	3	Falta de protección del equipo	2	2	6	
R34			E	No se tiene un control en los cambios de información, propenso hacker	3		Gestión pobre de contraseña	3			
R35			I	Vulnerable a software dañino	3		Mantenimiento insuficiente	2			

R36			I	Vulnerable a software dañino	3		Gestión pobre de contraseñas	2			
R37			I	Propenso a averías físicas y lógicas	3		Mantenimiento insuficiente	2			SIGNIFICATIVO
R38		EQUIPOS DE COMPUTOS	M	Propenso a cortes de servicio eléctrico	3	2	Susceptible a variación de la tensión	3	2	5	
R39			E	Poco mantenimiento actualización del hardware	3		Mantenimiento insuficiente	2			
R40			I	Destrucción de equipo	2		Falta de reemplazo periódico	3			
R41			E	Uso no autorizado del equipo	1		Abuso de derechos	2			
R42				Uso no autorizado del equipo	3		Abuso de derechos	2			
R43			E	Propenso a averías de origen lógico	2		Mantenimiento insuficiente	3			
R44			I	Propenso a averías de origen físico	3		Susceptible a variación de la tensión	3			SIGNIFICATIVO
R45	**HW**	MODEM	M	Corte de servicio eléctrico	2	3	Parámetros configurados incorrectamente	1	2	5	
R46			I	Propenso a fallas de servicio de comunicación	3		Falta de conocimiento	2			
R47			E	Errores por parte del usuario	2			2			
R48			E	Error de uso	3		Parámetros configurados	2			
R49			E	Mal funcionamiento	2		incorrectamente	2			
R50			I	Destrucción de equipo	2			2			

En este análisis, se obtuvieron resultados que muestran riesgos clasificados como significativos, mayores e importantes. Por lo tanto, se deben determinar las acciones relacionadas con cada tipo de riesgo para su adecuada gestión y mitigación.:

- ✓ Evitar: donde se aplicarán medidas de protección.
- ✓ Reducir: donde se debe de evitar que suceda un evento que dé lugar a la presencia de un riesgo.
- ✓ Transferir: trasladar las responsabilidades de riesgo.
- ✓ Aceptar: la responsabilidad de los riesgos identificados.

- **Controles**

  Se adoptarán controles específicos acordes a los riesgos identificados, lo cual es crucial para proteger los activos utilizados en la gestión de datos e información. Los resultados obtenidos de la valoración de riesgos servirán como guía para la implementación de estos controles. En la Municipalidad de Challhuahuacho, los controles implementados se centraron en los procesos tecnológicos y en las políticas de seguridad de telecomunicaciones. Estos controles incluyen medidas relacionadas con los activos, la mejora e implementación de una cultura de seguridad, así como el establecimiento de sanciones detalladas en el reglamento interno en caso de incumplimiento.

  Se implementarán diversos procedimientos de seguridad operativa que incluirán la preparación de mecanismos, herramientas y actividades para garantizar de manera adecuada las operaciones en los diferentes sistemas de procesamiento. Además, se establecerán

controles para evitar la ejecución de códigos maliciosos, generar copias de seguridad, prevenir accesos no autorizados y supervisar la instalación de software.

Los controles propuestos por la ISO/IEC 27001:2013 están agrupados en 18 dominios de seguridad, como se muestra en la figura 12. Los controles que tendremos en cuenta se encuentran en las cláusulas correspondientes a políticas de seguridad de la información (cláusula 5 en adelante), detalladas en la tabla 15.

Figura 12
Dominios y controles

Tabla 15

Tabla de dominios

	DOMINIO	CONTROL
A-5	Políticas de seguridad de información	Plan de seguridad de información que sea metódico, definido de forma detallada para iniciar acciones de seguridad
A-6	Organización de la seguridad de la información	Asignar responsabilidades para mantener la seguridad de la información mantener contacto con autoridades de la organización, considerar acuerdos de confidencialidad
A-7	Seguridad de recursos humanos	Antes de emplear a una persona se deben de investigar antecedentes, al ser contratado, responsabilidades de gestión de capacitación en seguridad de información al concluir contrato, asegurarse de la entrega de los diferentes recursos usados y asignados
A-8	Gestión de activos	Contar con un inventario de activos definir responsabilidades de los activos identificados, clasificar la información y prever de un nivel apropiado de seguridad considerando lo importante para la organización, uno de los activos de manera aceptable para prevenir borrados divulgación o destrucción de la información
A-9	Control de accesos	Controlar accesos a sistemas y aplicaciones, tener restricciones de accesos a la información procedimientos que sean seguros para iniciar sesión, gestionar las contraseñas de los usuarios como responsabilidad del usuario es el uso de la información que sea confidencial para autenticación
A-10	Criptografía	Usar controles criptográficos adecuados para protección confidencialidad, integridad, y autenticidad de la información tiene gran importancia considerar controles criptográficos dentro de las políticas de seguridad de la organización
A-11	Seguridad física y ambiental	Considerar áreas de seguridad físicas y perimetrales. Protección contra amenazas externas y de entorno Ubicación y protección de equipos, elementos de soporte de equipos, seguridad en cableados, realizar mantenimiento de equipos de seguridad en estos equipos tanto en su redistribución como en su reutilización, tener seguridad para evitar el borrado de información o de software
A-12	Seguridad en operaciones	Protección en contra de cualquier código malicioso aplicando controles necesarios, implementar copias de seguridad de la información mantener un registro de eventos para poder poner en uso herramientas que ayuden a

		identificar eventos críticos, capacitar al personal para actuar de manera correcta ante la presencia de un virus que puedan llevar a cabo procedimientos de recuperación
A-13	Seguridad de las comunicaciones	Gestionar la seguridad en las redes, controles de res, aplicar los mecanismos necesarios de seguridad que se encuentren relacionados a servicios de red
A-14	Adquisición desarrollo y mantenimiento de sistemas	Establecer los requisitos de seguridad de sistemas de información, establecer políticas de desarrollo seguro de software, mantener la seguridad del software de sistemas de aplicaciones e informaciones, se debe de garantizar que cuando se presenten propuestas de cambio en los sistemas se revisen verificando que se presenten propuestas de cambio en los sistemas, revisen verificando que no se comprometa la información
A-15	Relación con proveedores	Seguridad de la información con respecto a proveedores que ayudará en la protección de activos de terceros, garantizar que los controles de seguridad en la prestación de servicios de proveedores
A-16	Gestión de incidencias de la seguridad de la información	Se debe de garantiza que se apliquen enfoques que sean consistentes y eficaces para poder gestionar los incidentes que se presenten en la seguridad de la información en la organización de establecerán responsabilidades para manejar eventos en su seguridad de la información efectivamente es necesario que se apliquen procesos de mejora continua como respuesta a la monitorización evaluación y gestionar los incidentes ocurridos en a seguridad de la información
A-18	Conformidad	La privacidad de los datos que son personales debe de estar asegurados como es requerida en la legislación y regulación donde dea aplicable

6) Fase 7: Establecer políticas y procedimientos para controlar los riesgos

En esta fase se delimitar las diferentes medidas de control de acuerdo a los riesgos identificados, teniendo en consideración su importancia y valoración.

- **Políticas generales**
  - ✓ Para acceder a los diferentes sistemas de gestión documental, es necesario que el usuario cuente con una clave de acceso, cuya administración recae en el responsable del sistema.
  - ✓ Los usuarios tendrán acceso únicamente a los equipos de cómputo que estén autorizados.
  - ✓ Las claves asignadas a los diferentes usuarios deberán ser actualizadas cada 4 meses, permitiendo al usuario cambiar la contraseña en cualquier momento.
  - ✓ Las aplicaciones utilizadas por los usuarios deben clasificarse en públicas y privadas.
  - ✓ Si la contraseña no se modifica dentro del plazo establecido, deberá ser eliminada, exceptuando casos relacionados con enfermedades o maternidad.
  - ✓ No se permitirá el ingreso de personas ajenas y no autorizadas al área y/o departamento de sistemas.
  - ✓ Los documentos pertenecientes al software de la Municipalidad Distrital de Challhuahuacho, como manuales y tutoriales, estarán bajo el resguardo del responsable del área de sistemas.
  - ✓ El área de recursos humanos deberá comunicar al área de sistemas.
  - ✓ El área de recursos humanos deberá comunicar el retiro de los empleados para que sean eliminados de la base de datos.
  - ✓ En conjunto con los usuarios relacionados con la base de datos, se realizará una limpieza de los discos duros (HDD).

- ✓ Cada usuario es responsable del cuidado y protección de los equipos de cómputo.
- ✓ La información en los discos duros es responsabilidad del usuario, quien debe crear respaldos siguiendo los estándares establecidos.
- ✓ El personal responsable del área de sistemas tendrá la obligación de comunicar cualquier anormalidad, así como problemas eléctricos, para su reparación o mantenimiento correspondiente.
- ✓ Todos los equipos de cómputo deben tener activada una clave de inicio y un protector de pantalla.
- ✓ Se requiere autorización para ingresar o retirar hardware y/o software propiedad de la Municipalidad Distrital de Challhuahuacho.
- ✓ Los softwares instalados deberán contar con licencias originales.

- **Políticas de seguridad a nivel físico**
  - ✓ Solo se podrá ingresar al área de sistemas con autorización.
  - ✓ Se debe notificar al personal de seguridad laboral en caso de incidentes relacionados con incendios, accidentes eléctricos o situaciones de fuerza mayor.
  - ✓ Se prohíbe el consumo de alimentos y bebidas cerca de los equipos de cómputo.
  - ✓ Los extintores de incendios deben recibir mantenimiento periódico y estar ubicados en las diferentes áreas de la Municipalidad Distrital de Challhuahuacho.

- ✓ Se deben contar con equipos que respalden el abastecimiento de energía, como los UPS, que aseguran el apagado sistemático y regulado.
- ✓ Es recomendable que los equipos de hardware estén asegurados por una compañía de seguros.
- ✓ Se recomienda que el área de sistemas cuente con vigilancia permanente.
- ✓ El responsable del área de sistemas debe estar presente durante el mantenimiento de los equipos de cómputo.
- ✓ Mantener un control de las condiciones ambientales, verificando que no afecten el funcionamiento de las instalaciones, la información y los equipos de respaldo.

- **Políticas de seguridad a nivel lógico**
  - ✓ Los incidentes ocurridos con los activos informáticos que provocan dificultades en el buen desempeño del área de informática deben registrarse en una base de datos de incidentes.
  - ✓ La instalación y mantenimiento del sistema operativo solo podrán ser realizados por el responsable del área de sistemas.
  - ✓ La instalación y mantenimiento de los sistemas de gestión documental (SIGA, SIAF) solo podrán ser realizados por el responsable del área de sistemas.
  - ✓ La instalación y actualización de la base de datos estarán a cargo del responsable del área de sistemas.
  - ✓ La responsabilidad de mantener la estructura lógica y la seguridad de la red recae en el responsable del área de sistemas.

- ✓ El responsable de otorgar las claves de usuario y crear los usuarios será el área de sistemas.
- ✓ Se otorgarán claves de acceso de software solo a los usuarios encargados de manejar dicho software.
- ✓ Se deben implementar medios contra ataques maliciosos provenientes de hackers o programas dañinos.
- ✓ Para apoyar la protección de la red, se deben implementar equipos de firewall.

- **Políticas de seguridad a nivel de sistemas**
  - ✓ Los softwares y las aplicaciones en las que se deben ingresar datos deben tener la opción de ser validados previamente.
  - ✓ Los softwares donde se modifican, ingresan y eliminan datos deben considerar la generación de registros de verificación, que ayuden a auditar los datos, como fecha, hora y otros.
  - ✓ De acuerdo al diseño de los diferentes sistemas, se deben considerar roles para los usuarios según la actividad que cumplen, agrupándolos de acuerdo a la clase y/o tipo.
  - ✓ En caso de que ocurra una falla del sistema, se debe considerar la recuperación automática de la información.
  - ✓ Las normas del área de sistemas deben ser consideradas en el diseño y desarrollo de los sistemas.
  - ✓ Se deben planificar reuniones periódicas con los usuarios de los diferentes software y aplicaciones para asegurar el buen uso y desempeño de los mismos.

- ✓ La ejecución de sistemas que contengan datos privados debe realizarse a nivel de usuario y/o en un equipo específico.
- ✓ Si se cuenta con sistemas diseñados para la empresa, se debe entregar la documentación del diseño lógico y el código al responsable del área de sistemas. La documentación incluye: manual técnico del sistema, manual de usuario y manual de operador.
- ✓ Al recibir un sistema que ha sido diseñado para la organización, se debe firmar un acta de entrega y recibido como garantía de propiedad del autor.

- **Políticas de respaldos y recuperación de información**
  - ✓ De acuerdo a la importancia del respaldo, se debe establecer tiempos entre respaldos.
  - ✓ Para los respaldos se usarán diferentes dispositivos de almacenamiento para la base de datos, aplicaciones, usuarios, archivos documentales y archivos del sistema operativo.
  - ✓ Los respaldos se deben mantener en lugares seguros.
  - ✓ Los respaldos de archivos estarán disponibles en línea por dos años; posteriormente, serán resguardados en servidores.
- **Políticas relacionadas a los equipos de computación**
  - ✓ Todos los equipos de informática que cuenten con configuración deben considerar la infraestructura de la red de la organización, siguiendo los diferentes estándares y la instalación del área de sistemas.

- ✓ Se debe crear una base de datos coordinada con las áreas de administración y sistemas, que incluya todos los equipos que tiene la organización.
- ✓ El área de sistemas es responsable de todas las operaciones relacionadas con los equipos informáticos, así como de su asignación y rotación.
- ✓ La seguridad física del equipo será responsabilidad del usuario.

- **Políticas de mantenimiento de equipos**
  - ✓ El área de sistemas tiene la responsabilidad de realizar y controlar las actividades de mantenimiento preventivo y correctivo de los diferentes equipos informáticos, para garantizar la seguridad de los equipos.
  - ✓ Se debe considerar el contrato de organizaciones externas a la institución como complemento para el mantenimiento de los equipos informáticos que hayan cumplido con su tiempo de vida útil.
  - ✓ La autorización para llevar a cabo el mantenimiento de los equipos de cómputo no alcanza a los usuarios.
  - ✓ Se debe mantener actualizado el plan de mantenimiento preventivo para los equipos, para estar al tanto de las necesidades que se presenten.
  - ✓ Los equipos informáticos de la organización deben actualizarse de manera periódica para mantener su conservación y funcionamiento adecuado.

- **Políticas de accesos remotos**
  - ✓ El área de sistemas tiene la responsabilidad de dar autorizaciones a terceras personas para que puedan usar los recursos informáticos de la red.
  - ✓ Se deben cumplir los lineamientos dispuestos por el área de sistemas para tener accesos remotos.
- **Políticas de control de virus, uso de software**
  - ✓ El software que se use debe tener licencias adquiridas por la organización.
  - ✓ El área de sistemas debe garantizar que el antivirus instalado en los equipos de cómputo funcione correctamente y que las actualizaciones estén disponibles.
  - ✓ Se debe configurar el antivirus para que escanee el dispositivo de almacenamiento al ser conectado al equipo de cómputo.

7) **Fase 8: Asignar recursos y capacitar al personal.**

En esta fase del proyecto, se llevaron a cabo diversas pruebas del sistema de gestión de seguridad informática propuesto para confirmar que el diseño planteado es el correcto. Para implementar este diseño, se sugiere documentar de manera detallada cada uno de los controles, lo que permitirá determinar los recursos necesarios, ya sean técnicos o económicos. Además, se deben considerar los planes de capacitación para garantizar un desarrollo óptimo del proyecto.

Es indispensable garantizar una comunicación efectiva entre las partes involucradas, como el departamento de sistemas, la alcaldía y las diferentes áreas de la municipalidad. Esto permitirá que trabajen en equipo para

comprender el proceso de mantenimiento de buenas prácticas en seguridad de la información y colaboren en la resolución de posibles incidentes que afecten a los activos de información e informática.

Se propone la conformación de un comité de seguridad informática que esté presidido por el encargado del área de sistemas e incluya a un representante de las diferentes áreas que forman parte del diseño del sistema de gestión de seguridad de la Municipalidad Distrital de Challhuahuacho. Se deben asignar responsabilidades y elaborar cronogramas donde se considere la implementación de las diferentes políticas propuestas.

- **Implementación de un programa de sensibilización y capacitación**

  Las capacitaciones son de gran importancia, ya que garantizan que las diferentes áreas y usuarios involucrados en la implementación del sistema de gestión de seguridad comprendan las políticas de seguridad que deben cumplir en el ejercicio de sus funciones. Esto es crucial porque, en caso de incidentes, la falta de conocimiento sobre los procesos no debería ser una causa significativa. La aplicación de estas capacitaciones permitirá llevar a cabo las siguientes acciones:

  - ✓ Reducción de incidentes debido al poco o nulo conocimiento del proceso.
  - ✓ Evitación de resistencias a la implementación de sistemas de gestión de seguridad informática.
  - ✓ Capacitación integral del personal, tanto práctica como teórica.
  - ✓ Facilitación en la implementación del diseño del sistema de gestión de seguridad de la información.

Las áreas involucradas tienen la obligación de responder a incidentes de seguridad informática y colaborar activamente para mitigar riesgos y mejorar procesos relacionados directamente con la seguridad informática.

- **Implementación de un programa de gestión de incidentes**

  La elaboración de documentación de los incidentes relacionados con la seguridad de los diferentes activos de información en la Municipalidad Distrital de Challhuahuacho es fundamental. Esto ayuda a mitigar los incidentes que ocurran y reduce las probabilidades de que se repitan. Se deben llevar a cabo monitoreos de los incidentes para asegurar el cumplimiento de las políticas de seguridad. Es necesario crear un manual de procesos que proponga y establezca las acciones a seguir para enfrentar los incidentes que puedan surgir. En este sentido, se deben considerar los siguientes aspectos:

  - ✓ Formas de reportar el incidente.
  - ✓ Plan de contingencia.
  - ✓ Acciones correctivas.
  - ✓ Priorización de los incidentes y áreas afectadas.
  - ✓ Recolección de evidencias.
  - ✓ Comunicación con los usuarios afectados en el menor tiempo posible.
  - ✓ Presentación de informes mensuales o trimestrales.
  - ✓ Elaboración de estadísticas sobre los incidentes ocurridos.
  - ✓ Programación de auditorías internas para el sistema de gestión de seguridad informática, verificando el cumplimiento de las políticas

de seguridad y el alcance de los indicadores propuestos para mitigar riesgos.

III Etapa 3: Revisión

Los procesos dentro de una organización deben evaluarse de forma continua. Este proceso de revisión permite ajustar las propuestas del diseño de gestión de seguridad informática según la situación real de la organización. A pesar de haber realizado análisis previos, las propuestas para aplicar políticas y controles pueden quedar desfasadas o resultar demasiado estrictas, lo que podría causar inconvenientes en la armonía organizacional y generar costos adicionales.

Es fundamental que estas revisiones se lleven a cabo conforme a la norma ISO 27001:2013, aplicada para la implementación del sistema de gestión de seguridad informática. Estas revisiones deben realizarse periódicamente y deben ser responsabilidad del área de sistemas. En caso necesario, se puede considerar la contratación de una empresa externa certificada para llevar a cabo la revisión

8) Fase 9: Supervisar la implementación del sistema de gestión de seguridad informática

- **Monitoreo**

  El propósito del monitoreo es identificar las anomalías relacionadas con las políticas y su cumplimiento en los procesos reales de la Municipalidad Distrital de Challhuahuacho. Este monitoreo debe ser responsabilidad del área de sistemas y llevarse a cabo de acuerdo a los controles aplicados a cada activo de la entidad. Se ejecutará conforme a un plan de monitoreo que contribuirá a la prevención oportuna de

amenazas que puedan surgir por el incumplimiento de las políticas de seguridad propuestas

Tabla 16
Cronograma de monitoreo

CODIGO	CONTROL	SEMANA				RESPONSABLE
		1	2	3	4	
A-6	Acuerdos de confidencialidad y secreto	X	X	X	X	Áreas sistemas -área recursos humanos
	Asignación de responsabilidades para la seguridad de la información	X				Área de Sistema
	Investigar antecedentes del empleado	X				Áreas sistemas -área recursos humanos
A-7	Capacitación en seguridad de información	X		X		Área de Sistema
	Responsabilidades de gestión			X		Área de Sistema
	Inventario de activos				X	Alcaldía
A-8	Definir responsables de los activos	X				Área de Sistema
	Etiquetado y manipulado de información				X	Área de Sistema
	Uso aceptable de activos				X	Área de Sistema
A-9	Restricción del acceso a la información	X				Área de Sistema
	Políticas del control de accesos		X			Área de Sistema
	Gestión de los derechos de acceso asignados				X	Área de Sistema
A-10	Gestión de controles criptográficos				X	Área de Sistema
A-11	Protección contra las amenazas externas y ambientales	X				Área de Sistema
	Mantenimiento de los equipos			X		Área de Sistema
	Gestión de cambios			X		Área de Sistema
A-12	Controles contra el código malicioso		X	X	X	Área de Sistema
	Gestión de las vulnerabilidades técnicas	X	X	X		Área de Sistema
	Copias de seguridad de la información			X		Área de Sistema
	Restricciones en las instalaciones de software				X	Área de Sistema
A-13	Controles de red		X		X	Área de Sistema
	Políticas y procedimientos de intercambio de información			X	X	Área de Sistema
	Mecanismos de seguridad asociados a servicios de red			X		Área de Sistema
	Restricciones a los cambios en los paquetes de software			X		Área de Sistema
					X	Área de Sistema
A-14	Procedimientos de control de cambios en los sistemas			X		Área de Sistema
	Pruebas de aceptación				X	Área de Sistema

	Uso de principios de ingeniería de protección de sistemas	X				Área de Sistema
A-16	Notificaciones de los eventos de seguridad de la información	X	X	X	X	Áreas sistemas -área recursos humanos

- **Métricas**

  El área de sistemas, en coordinación con la oficina de Alcaldía, debe establecer indicadores que permitan evaluar y asignar valores al cumplimiento de los controles establecidos según las políticas de seguridad informática. Mediante el plan de indicadores y su verificación, se podrá determinar si el control asignado satisface adecuadamente las necesidades de seguridad de los activos informáticos, o si podría ser excesivo. En caso de ser insuficiente, se deberá replantear el control, ya que podría representar una amenaza oculta que podría convertirse en un incidente negativo y afectar gravemente a los activos de la Municipalidad Distrital de Challhuahuacho.

9) Fase 10: Prepararse para la auditoria de certificación

- **Auditorías internas y externas**

  Las opiniones sobre los procesos proporcionadas por el personal interno son valiosas; sin embargo, es importante complementar estas opiniones con evaluaciones de terceros. Por esta razón, es necesario implementar auditorías internas y externas en intervalos planificados, conforme a las recomendaciones de la norma ISO 27001 y considerando la norma ISO 27002. El objetivo de estos procesos de auditoría es verificar:

  ✓ La implementación de los requisitos, legislaciones y reglamentaciones relacionadas con las políticas de seguridad.

- ✓ La disponibilidad de los requisitos necesarios para la ejecución de las políticas de seguridad de la información en la Municipalidad Distrital de Challhuahuacho.
- ✓ La correcta implementación de los controles y su adecuación a las necesidades de seguridad de los activos de información y activos informáticos.
- ✓ La verificación de cada control y su ejecución para reducir el nivel de riesgos según las amenazas identificadas para los activos.

- **Revisión**

  Las revisiones deben realizarse de forma periódica y programada, siendo responsabilidad del área de sistemas plantear estos controles y asegurar su cumplimiento. Es necesario seguir los siguientes procesos para llevar a cabo una revisión completa:

  - ✓ Evaluar la efectividad del sistema de gestión de seguridad informática en la mitigación del riesgo.
  - ✓ Valorar y analizar los recursos económicos, humanos y tecnológicos disponibles.
  - ✓ -Considerar los diferentes riesgos residuales para establecer procedimientos que ayuden a mitigar el impacto de las amenazas.
  - ✓ -Renovar los planes de seguridad conforme a las últimas actualizaciones propuestas por la norma ISO, para estar preparados frente a amenazas futuras.

Tabla 17

Programación de evaluación del sistema de gestión de seguridad informática

PROCESO	MESES												RESPONSABLES
	1	2	3	4	5	6	7	8	9	10	11	12	
Valorar la efectividad de sistema de gestión de seguridad informática en mitigar riesgos	X				X			X			X		Alcaldía – área de sistemas
Analizar valorar los recursos humanos, tecnológicos y económicos	X					X					X		Área de recursos humanos Área de sistemas
Considerar los riesgos que son residuales establecer procedimientos que ayuden a mitigar planes de seguridad		X					X					X	Alcaldía – área de sistemas
Resolver planes de seguridad considerando las actualizaciones de la ISO para dar respuesta a futuras amenazas				X							X		Alcaldía – área de sistemas

IV Etapa 4: Actuar

10) Fase 11: Realizar auditorías periódicas de reevaluación

De acuerdo a las situaciones presentadas, se tomaron las medidas necesarias detalladas en la Etapa III, considerando los resultados de los controles, métricas, monitoreo, revisión y la implementación del sistema de gestión de seguridad informática en la Municipalidad Distrital de Challhuahuacho. Es fundamental analizar las políticas que requieren refuerzo para abordar los incidentes ocurridos, replantearlas si es necesario, o considerar sanciones para garantizar una mayor mitigación de riesgos en los activos.

En esta etapa, es crucial plantear acciones de mantenimiento y mejoras para el sistema de gestión de seguridad informática. Esto permitirá mitigar considerablemente las posibilidades de materialización del riesgo. Verificar el funcionamiento de los activos asegurará que los procesos cumplan cabalmente con las políticas de seguridad informática propuestas para la

Municipalidad Distrital de Challhuahuacho, garantizando así un servicio de calidad y alto nivel de seguridad informática en todas las áreas municipales (ISO, 2014).

Esta etapa debe incluir los siguientes aspectos:

- ✓ No debe haber conformidades respecto a la aplicación de las políticas del sistema de gestión de seguridad informática.
- ✓ Se deben establecer acciones correctivas según sea necesario.
- ✓ Analizar los informes de auditoría y corregir los fallos identificados.
- ✓ Considerar las sugerencias del personal del área administrativa.
- ✓ Obtener recursos para optimizar el sistema de gestión de seguridad informática.
- ✓ Monitorear las implementaciones de cambios y modificaciones al sistema de gestión de seguridad informática.
- ✓ Comunicar al área de sistemas de la Municipalidad Distrital de Challhuahuacho cualquier cambio o modificación realizada en el sistema de gestión de seguridad informática.

Para el mantenimiento del sistema de gestión de seguridad informática, se utilizará un formato de registro de control del proceso de mantenimiento, Anexo 03.

- **Plan de continuidad del negocio de la Municipalidad Distrital de Challhuahuacho**

El ciclo DEMING o PDCA (Planear, Hacer, Verificar y Actuar) vuelve a iniciar con el Plan de Continuidad. En este plan se analizarán los procedimientos que deben desarrollarse en caso de que las amenazas se

materialicen, después de la implementación del sistema de gestión de seguridad informática en la Municipalidad Distrital de Challhuahuacho.

El objetivo de este plan es garantizar el funcionamiento normal de los diferentes procesos de información dentro de la Municipalidad, incluso si la amenaza se materializa. Para que este plan de continuidad funcione, es crucial analizar dos situaciones principales:

- ✓ Identificar los activos críticos para el funcionamiento de la organización.
- ✓ Determinar el tiempo necesario para recuperar los activos informáticos afectados por la materialización de la amenaza.

En el diseño del sistema de gestión de seguridad informática, se propone elaborar un plan de continuidad del negocio para responder a posibles fallas en las políticas implementadas y en los controles de seguridad. Esto subraya la necesidad de prepararse para casos donde las amenazas se materialicen, convirtiéndose en un plan de contingencia ejecutado por el área de sistemas de la Municipalidad. Este plan asegura soluciones inmediatas para minimizar los impactos de las amenazas.

Una vez que se evidencie la materialización de una amenaza, se activará el plan de continuidad, convirtiéndose en una herramienta esencial para ejecutar procesos y salvaguardar aspectos críticos.

3.1.1. Elaboración del plan de seguridad informática

El plan de seguridad es el conjunto de decisiones que ayudarán a definir las acciones futuras y los medios que se utilizarán para conseguirlas. Esta premisa debe tenerse en cuenta al elaborar los planes de seguridad informática, los cuales también servirán como insumo para cualquier sistema de información.

Después de identificar los diferentes riesgos, amenazas y vulnerabilidades, se han determinado actividades clave que se aplicarán en la Municipalidad Distrital de Challhuahuacho. Estas actividades permitirán que las medidas de seguridad se alineen con las existentes para garantizar la reducción de los riesgos y amenazas identificados.

El plan de seguridad informática se realizará considerando los riesgos previamente identificados, los cuales se detallan en la Tabla 18

Tabla 18
Riesgos y amenazas identificados

ACTIVO	AMENAZA	VALOR DE AMENAZA	VULNERABILIDD	VALOR VULNERAB	NIVEL RIESGO
INTERNET	Exposición a phishing	**2**	Falta de monitoreo de recurso para procesar información	**3**	**SIGNIFICATIVO**
	Exposición a riesgos con virus	**3**	Falta de monitoreo de recursos para procesar información	**2**	
	La configuración de contraseña se encuentra expuesta	**2**	No se finaliza la acción por el usuario	**2**	
	Corte de servicio eléctrico	**3**	La arquitectura de red es insegura	**3**	
	Conexión de terceros a la red	3			
CORREO ELECTRÓNICO	Manipulación de acceso	2	Gestión pobre de contraseñas	2	**IMPORTANTE**
	Se encontraron mensajes SPAM con contenido malicioso	3	Parámetros configurados incorrectamente	2	
	Se encontró mensajes con contenido PISHING	3		3	
	Se encontró correos con presencia de falsas notificaciones	2			
SIGA	Mal funcionamiento de software	3	Errores de mantenimiento y actualización de software	2	SIGNIFICATIVO
	Errores de administrador	2	Falta de documentación	1	
	Caída del sistema por agotamiento de recursos	1	Falta de respaldos	3	
	Abuso de privilegios de acceso	2	Errores de distribución de acceso	2	
	Acceso no autorizado	2	No se finaliza sesión por el usuario	1	
SIAF	Errores de administrador	2	Errores de mantenimiento y actualización de software	2	SIGNIFICATIVO
	Caída del sistema por agotamiento de recursos	1	Falta de documentación	1	
	Abuso de privilegios de acceso	2	Falta de documentación	2	
	Acceso no autorizado	2	Falta de respaldos	2	
ANTIVIRUS	Falta de instalación de antivirus	3	Falta de mantenimiento lógico	2	**SIGNIFICATIVO**
	Incompatibilidad de software	1	Defectos de software	2	
	Falta de actualización de antivirus	2	Falta de monitoreo de recursos para procesar información	2	

SISTEMA DE TRAMITE DOCUMENTARIO	Falta de activación y autenticación de antivirus	3	Mantenimiento lógico insuficiente	2	SIGNIFICATIVO
	Software funciona mal	3	Erro de mantenimiento y actualización de software	2	
	Errores de administrador	2	Parametrar configuración incorrectamente	1	
	Caída del sistema por agotamiento	1	Falta de respaldos	2	
	Acceso no autorizado	2	Error en la distribución de acceso	2	
SISTEMA DE RESPALDO DE INFORMACIÓN	Alteración accidental de la información	3	Parametrar configuración incorrectamente	3	MAYOR
	Error en la creación de respaldo	3	Fallos en los procesos de crear respaldos	3	
	No existen respaldos	3	No se tienen políticas de respaldos	3	
SERVIDOR	Exceso de temperatura y humedad	2	Susceptible a polvo y suciedad	3	SIGNIFICATIVO
	Inexistencia de equipos para mantener temperatura ideal	3	Mantenimiento de equipo insuficiente	2	
	No se tiene un control adecuado en el mantenimiento de equipo	2	Falta de pruebas suficientes del software	1	
	No se actualiza el software de manera continua	3	Falta de protección del equipo	2	
	No se tiene un control en los cambios de información, propenso hacker	3	Gestión pobre de contraseña	3	
	Vulnerable a software dañino	3	Mantenimiento insuficiente	2	

Los planes que deben aplicarse para tratar estos riesgos son los siguientes:

1. Gestión de vulnerabilidades técnicas.
2. Gestión de respuesta a incidentes de seguridad informática.
3. Concientización sobre seguridad de la información.
4. Establecimiento de políticas de control de acceso basadas en requisitos de negocio.
5. Control de cambios sobre los sistemas.
6. Política de uso aceptable de los activos.
7. Clasificación e la información.

Las tareas que deben desarrollarse para cada actividad son:

1. Gestión de vulnerabilidades técnicas

a. Objetivo

Prevenir que exista un aprovechamiento de vulnerabilidades técnicas.

b. El riesgo que se va a tratar

Las deficiencias detectadas evidencian la presencia de vulnerabilidades técnicas debido a fallas en la detección o en la propuesta de soluciones en el sistema de información.

c. Responsable

Área de sistemas y administración.

d. Actividades

- Definir y establecer responsabilidades relacionadas con la gestión de vulnerabilidades técnicas, considerando posibles roles:
  - ✓ Responsable de realizar el análisis de vulnerabilidades en los activos identificados.
  - ✓ Responsable de aplicar la remediación sobre las vulnerabilidades técnicas identificadas.
  - ✓ Responsable de realizar el seguimiento de la remediación.
- Definir los recursos a utilizar para la identificación de vulnerabilidades técnicas:
  - ✓ Realización de escaneos periódicos en las vulnerabilidades identificadas, utilizando herramientas automatizadas.
- Tomar acciones ante las vulnerabilidades identificadas:
  - ✓ Al detectar una vulnerabilidad potencial, el personal de la Municipalidad Distrital de Challhuahuacho debe estar capacitado para identificar los riesgos asociados y proponer soluciones.
  - ✓ Aplicación de controles necesarios frente a incidentes de seguridad de la información.

- ✓ Suspensión de servicios relacionados con la vulnerabilidad identificada.
- ✓ Implementación de controles de acceso, como firewalls.

2. Gestión de respuesta a incidentes de seguridad informática

a. Objetivo

Actuar de manera eficaz ante la ocurrencia de incidentes de seguridad informática.

e. Riesgos tratados

- La presencia de deficiencias en la detección o planteamiento de soluciones para estas deficiencias puede llevar a la explotación de vulnerabilidades técnicas.
- Posible afectación en la integridad y disponibilidad del sistema debido a la manipulación de la configuración.

f. Responsable:

Área de Sistemas.

g. Actividades:

- Definir responsables para gestionar los incidentes y asegurar la comunicación dentro de la Municipalidad Distrital de Challhuahuacho sobre la presencia de incidentes mediante los siguientes procedimientos:
  - ✓ Planificar y preparar respuestas ante incidentes.
  - ✓ Procedimientos para el seguimiento, detección, análisis y reporte de eventos de seguridad.
  - ✓ Registrar los incidentes que ocurran.

- ✓ Valorar eventos de seguridad y vulnerabilidades para tomar decisiones.
- ✓ Responder a los incidentes y mantener comunicación con el personal municipal.
- ✓ Abordar las debilidades de seguridad que causaron el incidente.

- Registro de todos los incidentes de seguridad.

3. Concientización sobre seguridad de la información.

a. Objetivo

Crear cultura de seguridad de la información y seguridad informática en la Municipalidad Distrital de Challhuahuacho.

b. Riesgo a tratar

Existe la posibilidad de que la confidencialidad e integridad se encuentren afectados al presentarse una posible suplantación de usuario.

c. Responsable

Área de sistemas.

d. Actividades

- Promover reuniones de sensibilización dentro de la Municipalidad Distrital de Challhuahuacho. Se recomienda crear un equipo de seguridad para llevar a cabo la sensibilización.
  - ✓ Captar la atención de los trabajadores de la Municipalidad para asegurar la receptividad (fase de expectativa).
  - ✓ Organizar talleres de sensibilización con actividades personalizadas.
  - ✓ Realizar evaluaciones posteriores a los talleres de concientización.

- ✓ Diseñar folletos con temas relacionados con la seguridad informática y de la información, los cuales deben ser publicados en la página web de la institución.
- ✓ Realizar inducciones sobre seguridad de la información y seguridad informática para el personal nuevo.

4. políticas de control de acceso

a. objetivo

Controlar los derechos de acceso de usuarios a los diferentes recursos de la Municipalidad Distrital de Challhuahuacho.

b. Riesgo a tratar

- La posibilidad de que la disponibilidad e integridad de la información se vean afectadas por la falta de control en los privilegios.
- La posibilidad de suplantación de usuarios debido a la falta de protección de contraseñas.

c. Responsable

Área de sistemas.

d. Actividades

- Definir políticas para el control de acceso de usuarios:
  - ✓ Verificar los permisos de usuario necesarios para el uso de los diferentes software y servicios disponibles en la Municipalidad Distrital de Challhuahuacho.
  - ✓ Asignar identificaciones únicas a cada usuario.
  - ✓ Asegurar que los proveedores de servicios no otorguen accesos hasta que el usuario esté debidamente autorizado.

- ✓ Revisar, retirar o bloquear cuentas de usuario redundantes, garantizando que cada cuenta sea única.
- ✓ Asignar privilegios de manera apropiada para la ejecución de funciones específicas.
- ✓ Mantener una matriz de roles y perfiles para cada sistema de información, aplicaciones y recursos de red.
- ✓ Realizar revisiones periódicas de los cambios en las cuentas con privilegios.

- En cuanto a las contraseñas de usuarios:
  - ✓ Los administradores de sistemas son responsables de cambiar las contraseñas que fueron predefinidas por los proveedores después de la instalación del software.
  - ✓ No permitir que los sistemas inicien más de una sesión con el mismo usuario.
  - ✓ Promover buenas prácticas como cerrar la sesión y bloquear los equipos como medidas de seguridad al salir del puesto.
  - ✓ Configurar los sistemas de información y equipos de cómputo para que las sesiones se desconecten automáticamente después de un período determinado de inactividad.

5. control de cambios sobre los sistemas

a. Riesgo a tratar

- Riesgo en la disponibilidad e integridad del sistema debido a manipulación en la configuración:
- Riesgo en la disponibilidad de servicios informáticos debido a errores en actualizaciones y mantenimiento:

b. Objetivo

Implementar controles en la asignación de los derechos de acceso del usuario para los diferentes recursos de la Municipalidad Distrital de Challhuahuacho.

c. Responsable

Área de sistemas

d. Actividades

- Establecer procedimientos formales de control de cambios para gestionar cambios significativos, documentando cada paso y considerando evaluaciones de riesgos, análisis de impacto y especificación de controles de seguridad:
  - ✓ Identificar y clasificar los componentes afectados por los cambios planeados.
  - ✓ Evaluar y clasificar los tipos de cambios que se van a implementar en cada componente.
  - ✓ Realizar un análisis de riesgos para evaluar el impacto en la seguridad de los sistemas.
  - ✓ Establecer un proceso de aprobación formal para autorizar los cambios programados.
  - ✓ Comunicar de manera efectiva los cambios planificados a todas las áreas y personas relevantes dentro de la Municipalidad Distrital de Challhuahuacho.

6. política de uso aceptable de los activos

a. Objetivo

Identificar los activos que se tienen con su respectiva clasificación y los responsables asignados a estos.

b. Riesgo a Tratar

Posibilidad de que los equipos informáticos y/o archivos se encuentren afectados por mal uso de hardware y software.

c. Responsable

Área de sistemas.

d. Actividades

- Establecimiento de políticas de inventario de activos:Es fundamental implementar y mantener actualizado periódicamente un inventario de activos informáticos en la Municipalidad Distrital de Challhuahuacho, junto con una matriz de riesgos clasificados y etiquetados:
  - ✓ -El inventario debe incluir información relevante como el tipo de activo, ubicación, detalles de licencias y clasificación de seguridad.
  - ✓ Debe prepararse un inventario específico para software, aplicaciones y sistemas de información de la Municipalidad, detallando sus características generales.
  - ✓ Es esencial contar con un inventario separado para software de servidores y PCs, incluyendo sistemas operativos, programas, utilidades, controladores, software de oficina y su licenciamiento.

- ✓ Se debe mantener un inventario de activos físicos como equipos de cómputo, equipos de comunicaciones y medios removibles, especificando sus características técnicas.
- ✓ Además, se debe mantener un registro actualizado del personal de la Municipalidad Distrital de Challhuahuacho.

- Asignación de responsabilidades a través de la administración y el área de sistemas:
  - ✓ Es crucial asignar responsabilidades claras para el control del desarrollo, mantenimiento, procesamiento de servicios y seguridad de los activos identificados, asegurando la implementación adecuada de restricciones de acceso y controles necesarios.
- Cumplimiento de políticas por parte de los usuarios de activos: Todos los usuarios de activos en la Municipalidad Distrital de Challhuahuacho deben cumplir con las políticas establecidas y propuestas:
  - ✓ El personal responsable de manejar expedientes en la municipalidad debe entregarlos física y electrónicamente a través de sistemas de información, con validación del jefe inmediato.
  - ✓ Los activos físicos deben ser entregados con el proceso de descarga de responsabilidad correspondiente.
  - ✓ Se debe proporcionar documentación completa para el soporte, mantenimiento y actualización de equipos de cómputo,

aplicaciones, bases de datos, servidores y sistemas de información.

7. Establecer política de clasificación de la información

a. Objetivo

Proteger la información de la Municipalidad Distrital de Challhuahuacho de acuerdo al nivel de sensibilidad de la información y su importancia.

b. Riesgo a Tratar

La posibilidad de que la confidencialidad de la información este afectada.

c. Responsable

Área de sistemas.

d. Actividades

- La Municipalidad debe clasificar la información para identificar su nivel de criticidad, siguiendo la guía proporcionada por la Norma ISO/IEC 27001:2013.
- Los responsables deben garantizar la protección de la información reservada para evitar su divulgación sin autorización.
- Es fundamental que la información no se deje descuidada en ningún momento para asegurar su integridad y confidencialidad.

Capítulo 4

Análisis y discusión de resultados

4.1. Análisis de resultados respecto a los objetivos

Una vez desarrollado el plan de gestión de seguridad informática basado en la norma ISO/IEC 27001:2014 para mejorar el manejo de la información en el área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho, se obtuvieron los siguientes resultados:

1. **Objetivo general:**

   a. ***Diseñar e implementar un plan de gestión de seguridad informativa para mejorar la protección de información en el ´área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.***

      A partir de la información que se evidencia, luego de haber analizado el estado en el que se encuentra la seguridad de la información e identificado cuales son los riesgos a los que se encuentran expuestos los activos con los que cuenta la Municipalidad, se propuso el diseñó y la implementación de diferentes políticas de seguridad necesarias.

      Para garantizar la efectividad en el cumplimiento de las políticas establecidas, se diseñó un plan de gestión de seguridad en el que se determinan las diferentes acciones que se deben tomar y los responsables de hacer cumplir estas acciones. *(pág. 59).*

      Este plan de gestión de seguridad informática para mejorar la seguridad de la información se debe de revisar y actualizar

periódicamente, toman- do en cuenta las revisiones y monitoreo. tabla 3.16 que se sugiere en una de las faces que la norma ISO 27001:2014 sugiere que se cumplan para implementar gestiones de seguridad informática, de acuerdo a los crono- gramas establecidos el plan se encuentra en ejecución, figura 1.3 una vez cumplido el periodo de prueba realizara una encuesta para analizar el estado de seguridad en la que se encuentran los activos de información como los activos informáticos.

Se demuestra que se alcanzó a cumplir el objetivo propuesto al haber aplicado el formato de mantenimiento del sistema de seguridad de la información (Anexo 03) cumpliendo con las fases 9,10, 11 de las etapas 3 y etapa 4 del ciclo (PDCA).

2. Objetivos específicos:

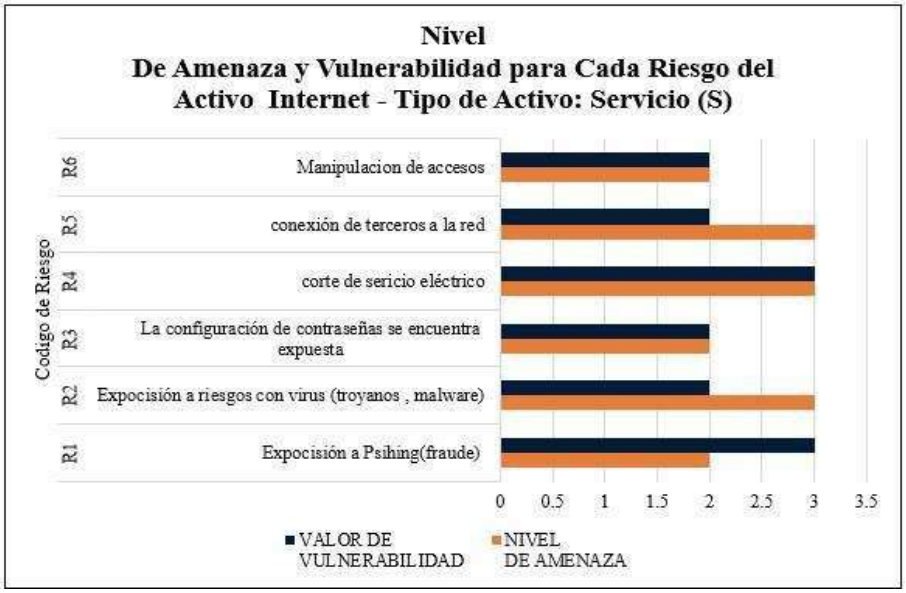
a. Analizar el estado actual de la seguridad de información a través del ´área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.

Se ha determinado que la seguridad de la información enfrenta riesgos significativos, tal como se detalla en la Tabla 14, donde se presentan valores continuos que oscilan entre significativo, importante y mayor. Estos resultados se refuerzan con la evaluación individual realizada para cada activo identificado, como se ilustra en los gráficos siguientes. Los valores en estos gráficos han sido calculados según la Tabla 14 (Evaluación de activos identificados en la Municipalidad Distrital de Challhuahuacho).

En la figura 13 se muestra que de acuerdo a los riesgos identificados se observa que el nivel de amenaza y teniendo en cuenta este nivel se puede identificar valores de vulnerabilidad en la que se encuentra el activo analizado en este caso el servicio *INTERNET*.

Figura 13

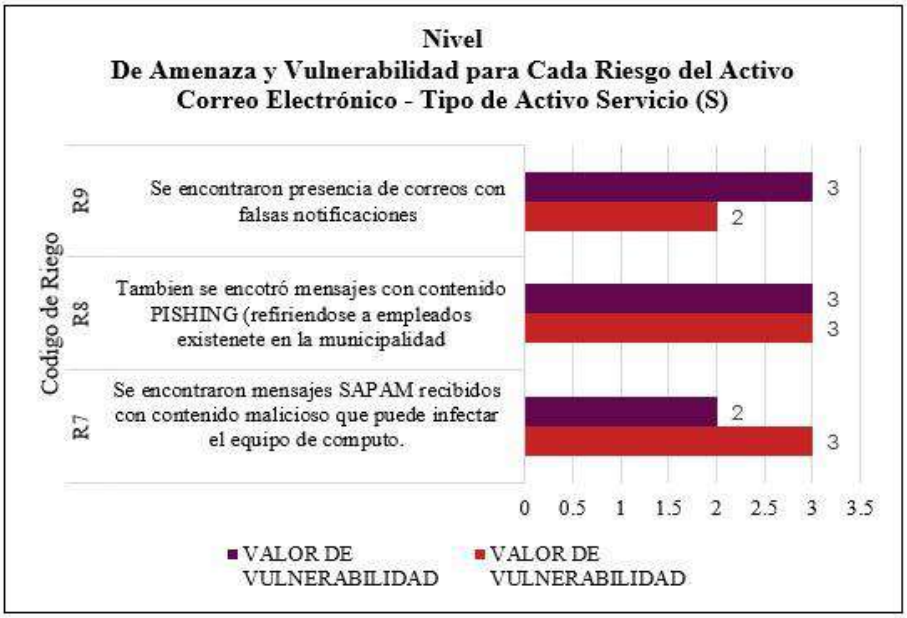
Nivel de amenaza y vulnerabilidad del activo internet



En la figura 14 se observa que de acuerdo a los riesgos identificados se muestran el nivel de amenaza y teniendo en cuenta este nivel se tienen los valores de vulnerabilidad en la que se encuentra el activo analizado, en este caso el servicio CORREO ELECTRÓNICO.

Figura 14

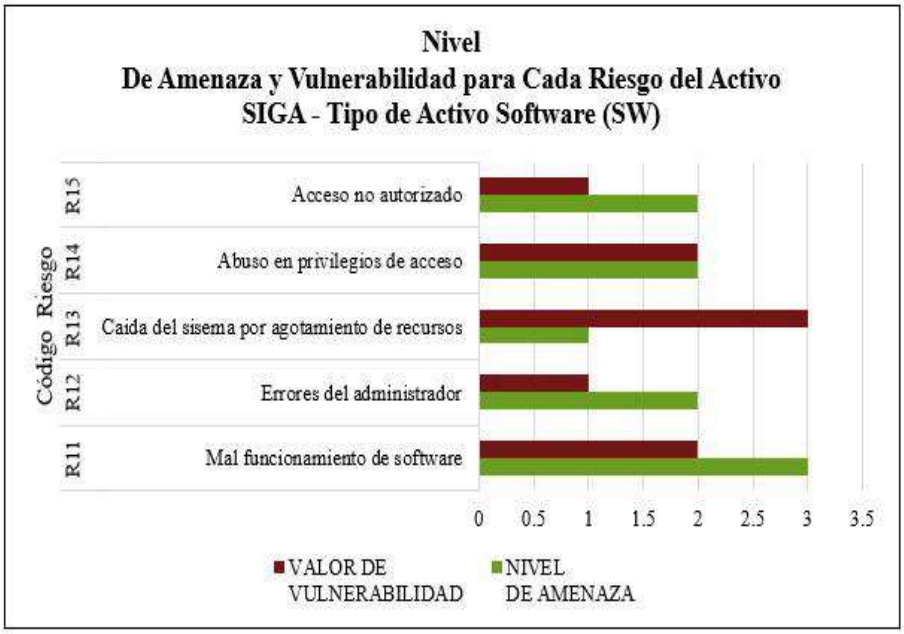
Nivel de amenaza y vulnerabilidad del activo correo electrónico



En la figura 15 se muestra que de acuerdo a los riesgos identificados se observa el nivel de amenaza y teniendo en cuenta este nivel se tienen los valores de vulnerabilidad en la que se encuentra el activo analizado, en este caso el software SIGA.

Figura 15

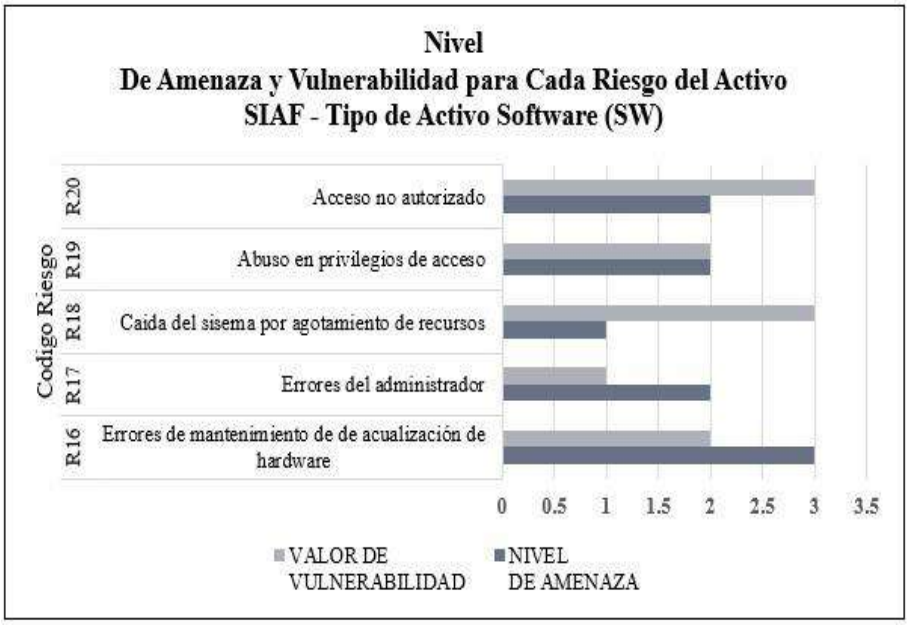
Nivel de amenaza y vulnerabilidad del activo SIGA



En la figura 16 se muestra que de acuerdo a los riesgos identificados se observa el nivel de amenaza y teniendo en cuenta este nivel se tienen los valores de vulnerabilidad en la que se encuentra el activo analizado, en este caso el software SIAF.

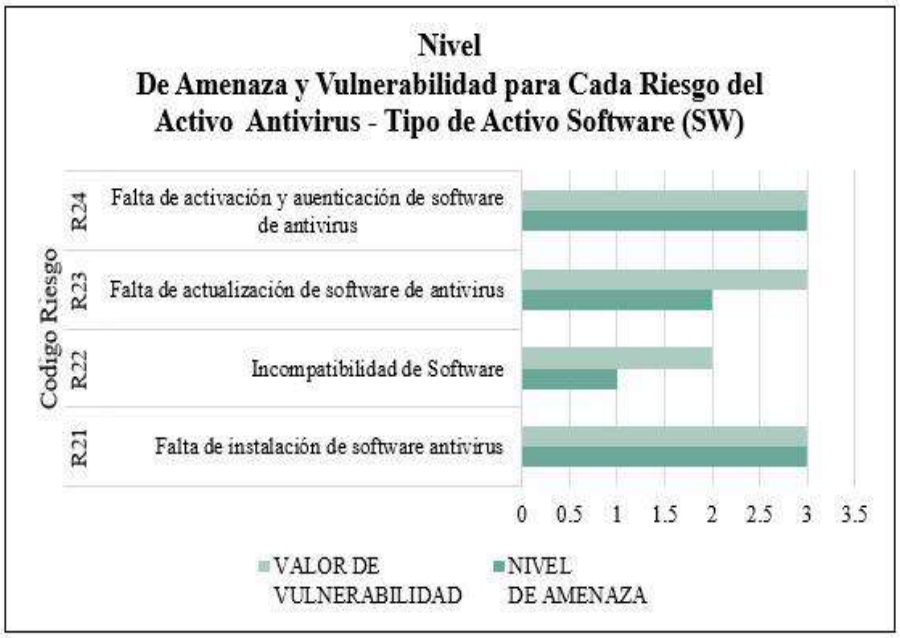
Figura 16

Nivel de amenaza y vulnerabilidad del activo SIAF



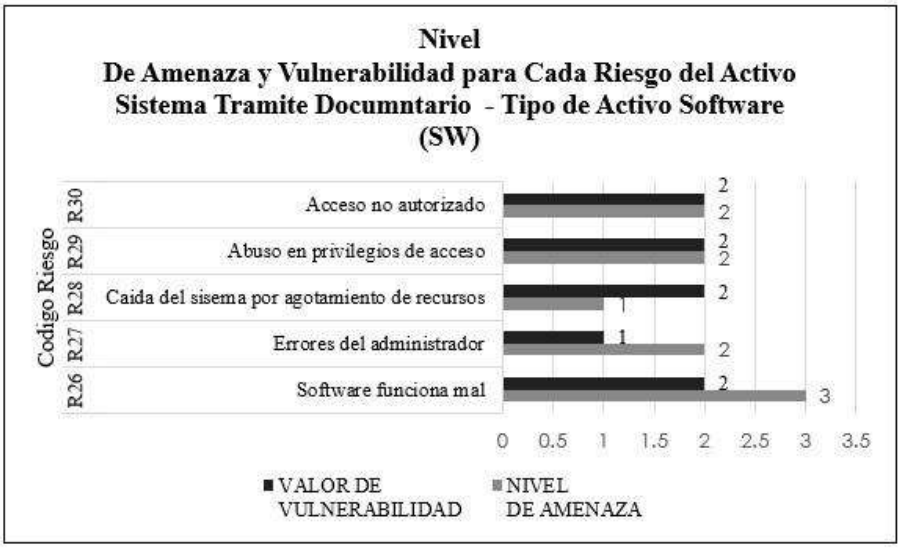
En la figura 17 se muestra que de acuerdo a los riesgos identificados se tiene el nivel de amenaza y teniendo en cuenta este nivel se puede observar los valores de vulnerabilidad en la que se encuentra el activo analizado, en este caso el software ANTIVIRUS.

Figura 17
Nivel de amenaza y vulnerabilidad del activo ANTIVIRUS



En la figura 18 se muestra que de acuerdo a los riesgos identificados se tiene el nivel de amenaza y teniendo en cuenta este nivel se puede observar los valores de vulnerabilidad en la que se encuentra el activo analizado en este caso el software SISTEMA DE TRAMITE DOCUMENTARIO.

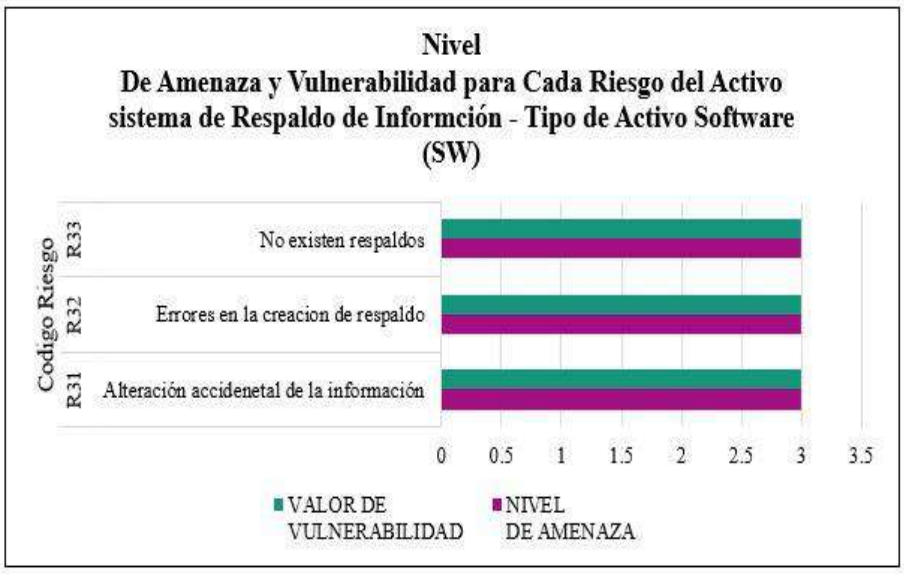
Figura 18
Nivel de amenaza y vulnerabilidad del activo tramite documentario



En la figura 19 se muestra que de acuerdo a los riesgos identificados se tiene el nivel de amenaza y teniendo en cuenta este nivel se puede observar los valores de vulnerabilidad en la que se encuentra el activo analizado en este caso el software RESPALDO DE INFORMACION

Figura 19

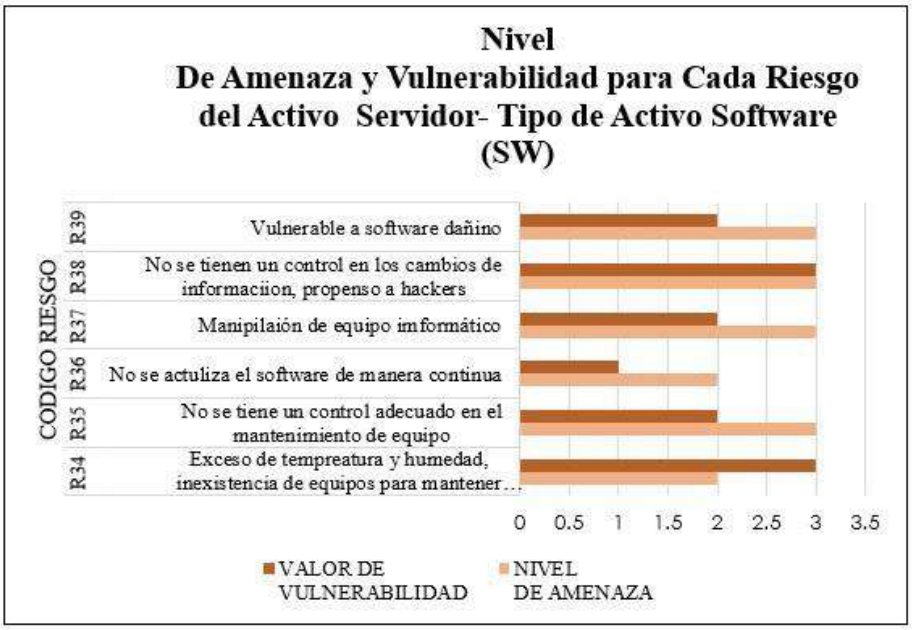
Nivel de amenaza y vulnerabilidad del activo respaldo de información



En la figura 20 se muestra que de acuerdo a los riesgos identificados se tiene el nivel de amenaza y teniendo en cuenta este nivel se puede observar los valores de vulnerabilidad en la que se encuentra el activo analizado en este caso el software DATA CENTER - SERVIDOR.

Figura 20

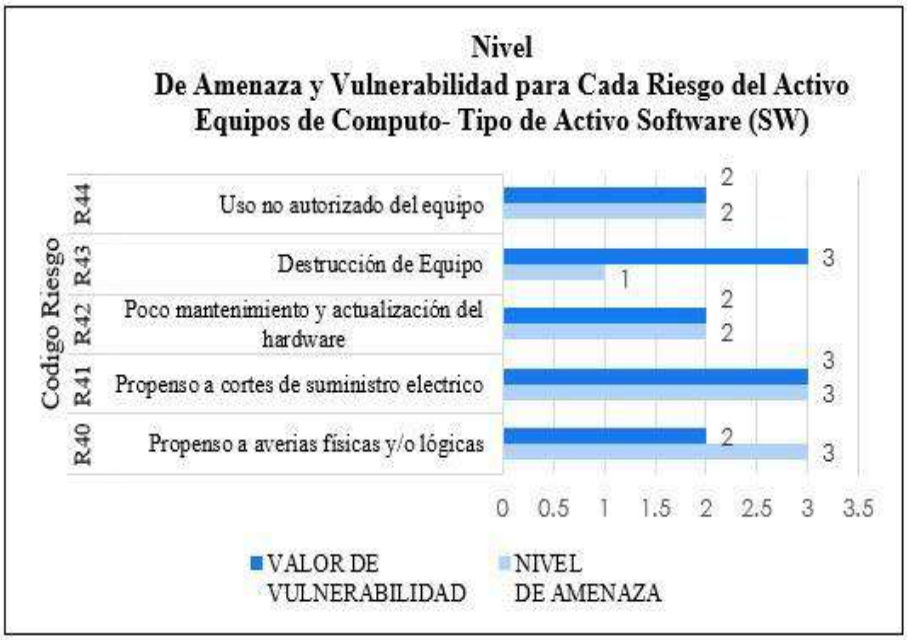
Nivel de amenaza y vulnerabilidad del activo data center – servidor



En la figura 21 se muestra que de acuerdo a los riesgos identificados se tiene el nivel de amenaza y teniendo en cuenta este nivel se puede observar los valores de vulnerabilidad en la que se encuentra el activo analizado en este caso el hardware EQUIPO DE COMPUTO.

Figura 21

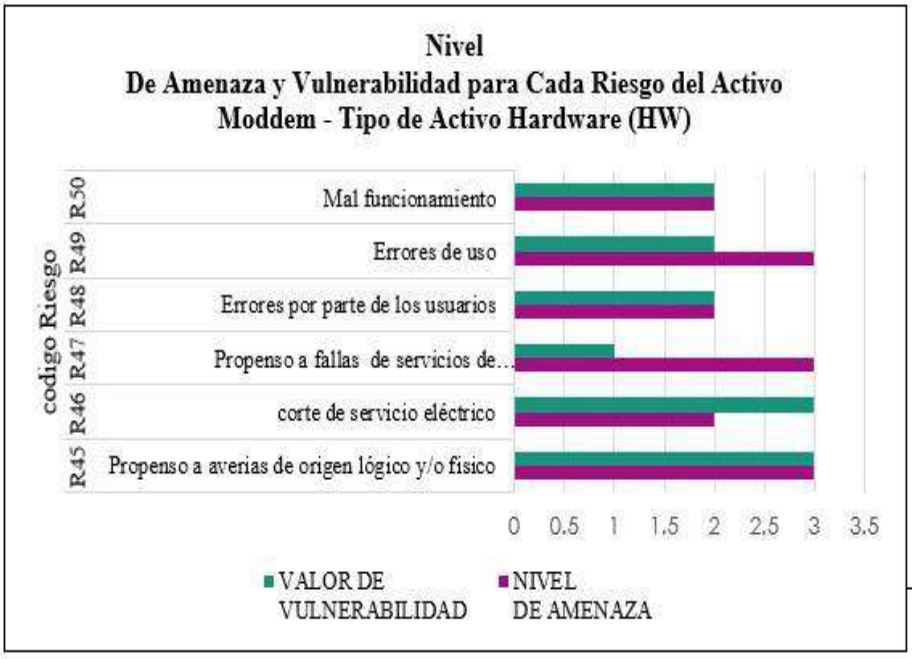
Nivel de amenaza y vulnerabilidad del activo equipos de computo



En la figura 22 se muestra que de acuerdo a los riesgos identificados se tiene el nivel de amenaza y teniendo en cuenta este nivel se puede observar los valores de vulnerabilidad en la que se encuentra el activo analizado en este caso el hardware MODEM.

Figura 22

Nivel de amenaza y vulnerabilidad del activo modem

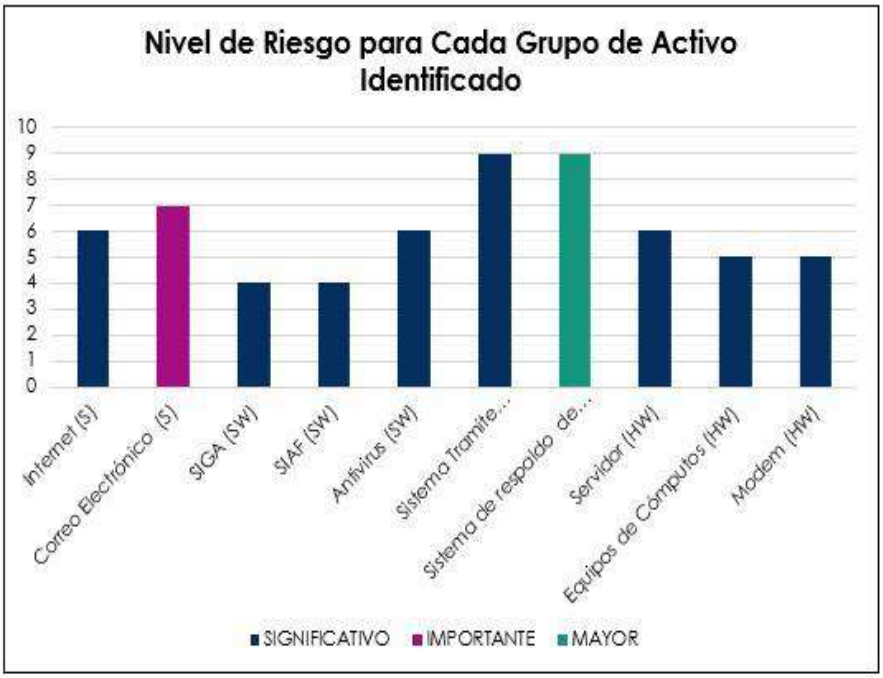


b. Identificar los riesgos de la seguridad de información a través del área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.

Tras el análisis respectivo de los diferentes riesgos identificados, se ha determinado el nivel de riesgo para cada activo, como se muestra en la Figura 23 Aunque la figura indica que los activos con un mayor nivel de riesgo son el sistema de trámite documentario y el sistema de respaldo de la información, es crucial aplicar tratamientos para proteger la información en todos los activos. Esto se debe a que la evaluación se basa en los criterios de confidencialidad, integridad y

disponibilidad. Según los resultados de la evaluación, los activos que tienen un valor igual o mayor a 3 se consideran en riesgo.

Figura 23
Nivel de riesgo de los activos identificados en la Municipalidad de Challhuahuacho



c. Diseñar políticas de seguridad informática para la protección de información a través del área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.

El diseño de las políticas para la seguridad de la información se llevó a cabo después de la identificación de amenazas y vulnerabilidades. Estas políticas están directamente relacionadas con los activos identificados dentro de la Municipalidad y siguen las especificaciones sugeridas por la norma ISO/IEC 27001:2013 para la implementación de la seguridad de la información y la seguridad informática. Para evaluar la aplicación de estas políticas, se realizó una entrevista al personal que trabaja en la Municipalidad Distrital de Challhuahuacho,

como se detalla en el Anexo 01. Los resultados obtenidos reflejan el nivel de cumplimiento de cada una de las políticas propuestas en la norma ISO/IEC 27001:2013.

La entrevista realizada se centra en los accesos a los equipos de cómputo, verificando si los usuarios cumplen con la responsabilidad de cuidar los diferentes equipos de la Municipalidad Distrital de Challhuahuacho. Además, se investiga si existen informes sobre anomalías eléctricas reportadas por el área de sistemas, y si el personal de la Municipalidad está obligado a presentar autorizaciones al sacar o ingresar hardware o software. Todo lo mencionado está en consonancia con las políticas de seguridad de la información y seguridad informática establecidas por la norma ISO/IEC 27001:2013.

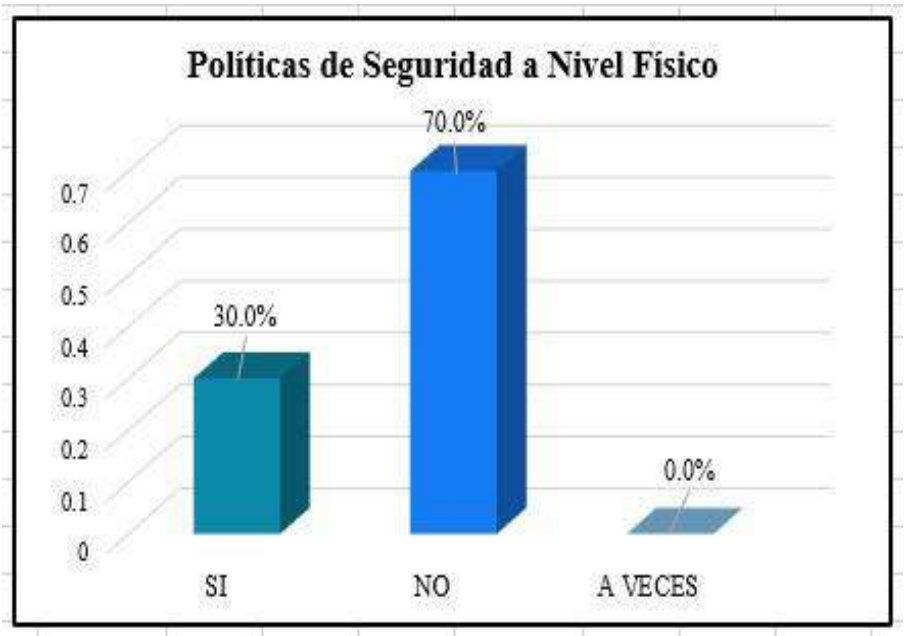
Según se muestra en la figura 24, un 35% indica que sí se cumplen con las políticas relacionadas con la seguridad, mientras que un 65% menciona que no existen políticas generales de seguridad.

Figura 24
Existencia de políticas de generales de seguridad

Los resultados presentados en la figura 25 evalúan la existencia de normativas para evitar el consumo de alimentos cerca de los equipos de computación. Además, se verifica la disponibilidad de respaldos para el suministro eléctrico en caso de problemas eléctricos, y se considera la presencia del responsable del área de sistemas durante el mantenimiento de los equipos. Todos estos aspectos están alineados con las Políticas de Seguridad a Nivel Físico establecidas.

Según los resultados, el 30% indica que se cumplen con políticas de seguridad a nivel físico, mientras que el 70% menciona que no existen políticas de seguridad establecidas en ese ámbito.

Figura 25
Existencia de políticas de seguridad a nivel físico

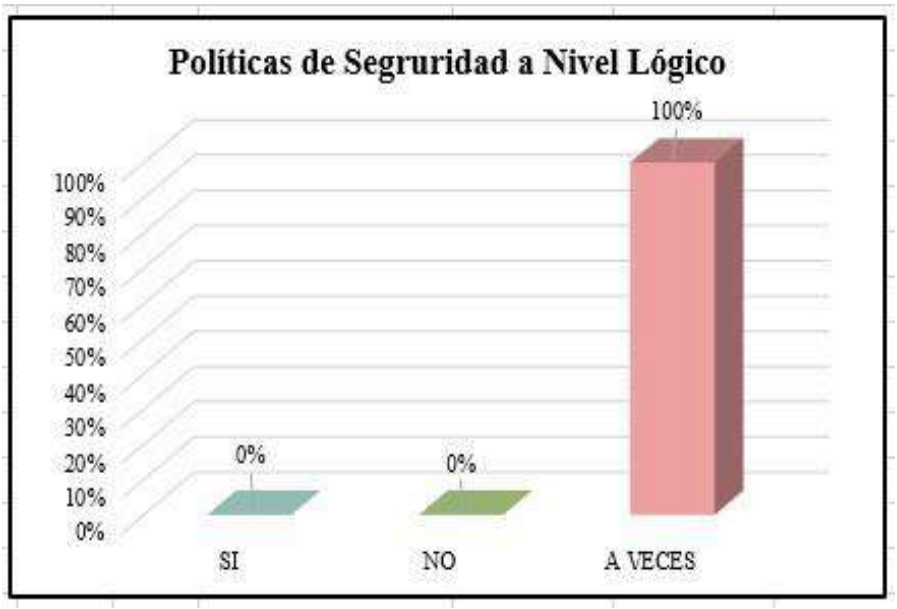


Los resultados que se presentan en la figura 26 consideran si la persona responsable de la instalación y mantenimiento del sistema operativo es el encargado del área de sistemas, así como la

gestión de software documental como el SIAF y el SIGA. También se evalúa el mantenimiento de la red.

Estos aspectos están enmarcados dentro de las políticas de seguridad a nivel lógico. Según los resultados, se observa que el 100% menciona que a veces se cumplen estas políticas.

Figura 26
Existencia de políticas de seguridad a nivel lógico

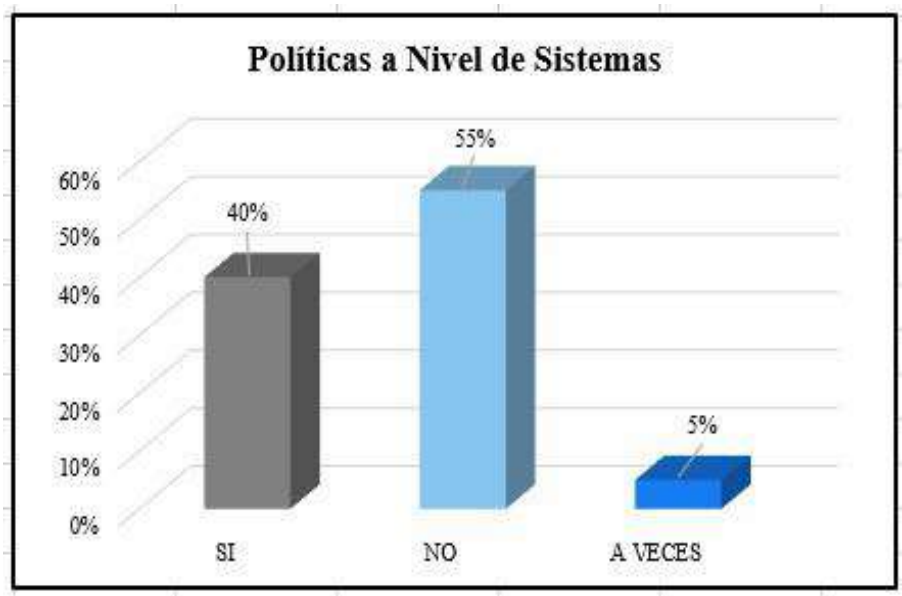


Los resultados presentados en la figura 27 están relacionados con la seguridad de los softwares utilizados para el ingreso y eliminación de datos. Estos programas deben contar con opciones de validación, considerar la recuperación automática de datos y asegurar que el responsable organice reuniones periódicas con los usuarios para garantizar su correcto uso.

Estos aspectos están enmarcados dentro de las Políticas de Seguridad a Nivel de Sistemas. Según los resultados, se observa que un 40% indica que se cumplen con las políticas relacionadas con la seguridad

a nivel de sistemas, un 55% menciona que no existen estas políticas y un 5% menciona que a veces se aplican.

Figura 27
Existencia de políticas de seguridad a nivel de sistemas

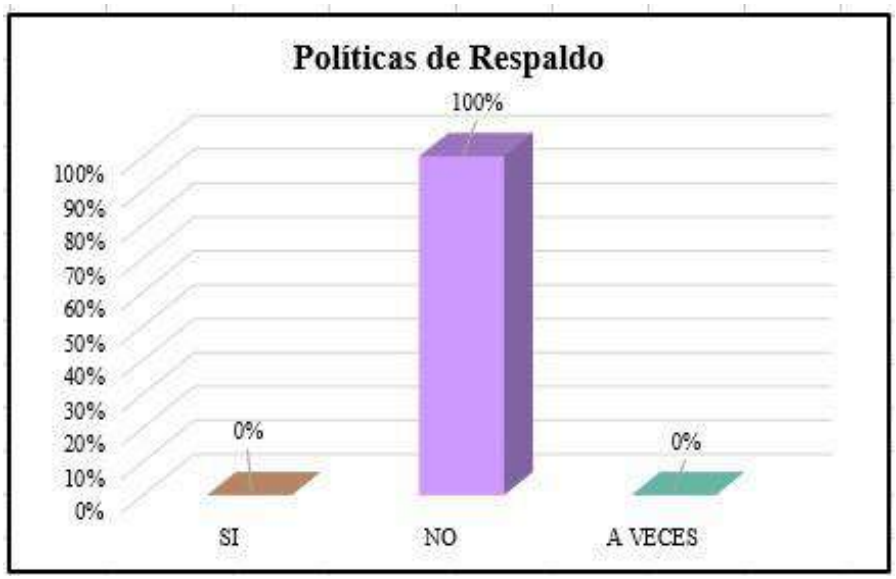


Los resultados presentados en la figura 28 muestran si se considera la programación de creación de respaldos en periodos definidos y si se cuentan con dispositivos de almacenamiento dedicados exclusivamente para esta tarea. Estos aspectos están enmarcados dentro de las Políticas de Respaldos y Recuperación

Según los resultados, el 100% indica que no existen políticas que aseguren la creación de respaldos de información.

Figura 28

Existencia de políticas de respaldo y recuperación de la información

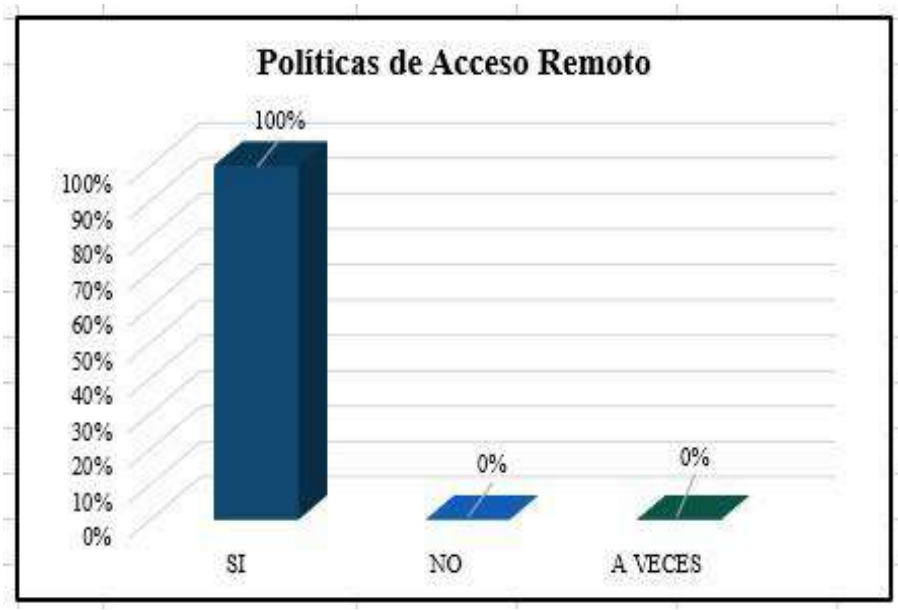


Los resultados presentados en la figura 29 se relacionan con el cumplimiento de los estándares necesarios para la configuración de los equipos de cómputo conectados en red en la Municipalidad Distrital de Challhuahuacho. Esto incluye verificar si los equipos están registrados en una base de datos, si los mantenimientos preventivos y correctivos son realizados adecuadamente por el área de sistemas, si se actualizan oportunamente y si se restringen los accesos a la red para evitar el ingreso de terceras personas.

Estos aspectos están enmarcados dentro de las Políticas de Seguridad de Equipos de Cómputo. Según los resultados, un 35% menciona que se cumplen con estas políticas, un 50% indica que no se tienen políticas establecidas para los equipos de cómputo, y un 15% menciona que a veces se aplican estas políticas. En el gráfico 30 se observa que el 100% indica que sí se cuentan con políticas de seguridad relacionadas con accesos remotos.

Figura 29
Existencia de políticas de seguridad para equipos de computo

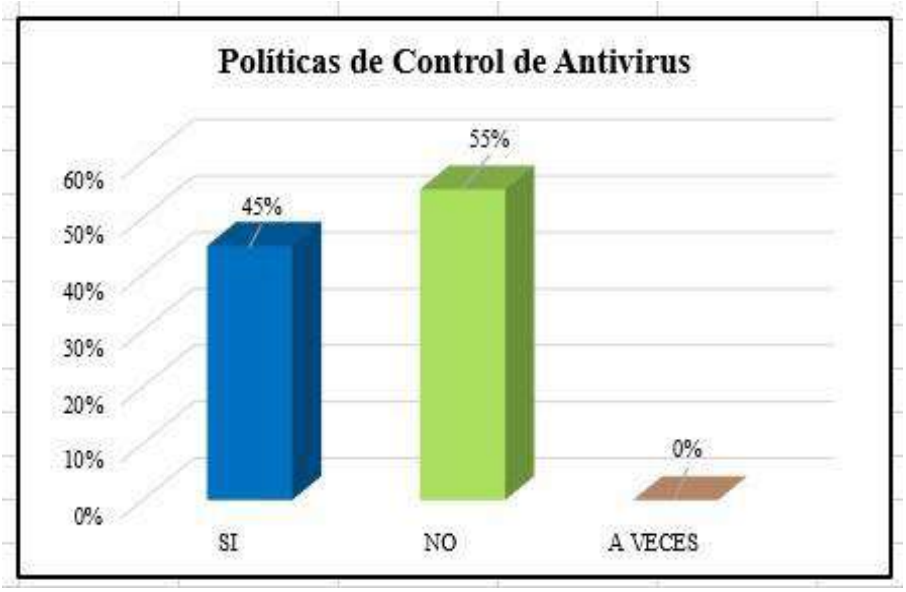
Figura 30
Existencia de políticas de acceso remoto.



Los resultados presentados en la figura 31 están relacionados con las licencias de software, verificando si son originales o no, así como si los programas antivirus están actualizados y activados.

Estos aspectos están enmarcados dentro de las Políticas de Control de Virus y Software. Según los resultados, un 40% menciona que se cumplen con estas políticas, un 55% indica que no se tienen políticas establecidas para el control de virus y software, y un 5% menciona que a veces se aplican estas políticas.

Figura 31
Existencia de políticas de control de antivirus y software



Entiendo, parece que la figura 32 indica que no se tienen implementadas políticas en la municipalidad según los resultados de la encuesta realizada.

Figura 32
Implementación de políticas de seguridad informática

Para diseñar las políticas de seguridad de la información basadas en los datos obtenidos y los resultados del análisis de amenazas y riesgos, aquí tienes una propuesta estructurada:

a. Políticas generales
b. Políticas de seguridad a nivel físico
c. Políticas de seguridad a nivel lógico
d. Políticas de seguridad a nivel de sistemas
e. Políticas de Respaldo y recuperación de información
f. Políticas relacionadas a nivel de equipos de cómputo
g. Políticas de mantenimiento de equipos
h. Políticas de acceso remoto
i. Políticas de control de virus, uso de software

Estas políticas deben ser adaptadas específicamente a las necesidades y contexto de la Municipalidad Distrital de Challhuahuacho, siguiendo los lineamientos de la norma ISO/IEC 27001:2013 y

ajustándose a los riesgos y amenazas identificados durante el análisis previo.

d. Implementar políticas de seguridad informática para la protección de información a través del ´área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho

Es excelente ver que se han implementado las políticas de seguridad de acuerdo al diseño propuesto y siguiendo las fases recomendadas por la norma ISO/IEC 27001:2013. Aquí se resumen los pasos clave que se llevaron a cabo:

Se han identificado los activos informáticos y de información dentro de la Municipalidad, valorándolos en términos de integridad, disponibilidad y confidencialidad.

Se realizó un análisis detallado para identificar las amenazas y vulnerabilidades asociadas a cada activo. Esto permitió determinar el nivel de riesgo en el que se encuentran, como se detalla en la tabla 15.

Se han implementado las políticas diseñadas para abordar los riesgos identificados. Esto incluye establecer roles y responsabilidades claras para mitigar los riesgos según lo indicado en la tabla 9.

Se ha llevado a cabo una campaña de sensibilización entre los usuarios de la municipalidad, destacando la importancia de cumplir con las políticas de seguridad establecidas. Esto es crucial para que todos comprendan su rol en la protección de datos, información y activos informáticos.

Este enfoque estructurado no solo fortalece la seguridad de la información dentro de la Municipalidad Distrital de Challhuahuacho,

sino que también promueve una cultura de seguridad entre los empleados. Continuar con la monitorización y el ajuste periódico de estas políticas asegurará que la seguridad de la información siga siendo efectiva y adaptada a los cambios en el entorno operativo y las amenazas emergentes.

Discusión de resultados respecto a los antecedentes

El proyecto que estás desarrollando en la Municipalidad Distrital de Challhuahuacho refleja una implementación importante y estructurada de un plan de gestión de seguridad informática basado en la norma ISO/IEC 27001:2013.

- Análisis de estado de seguridad: Similar a otros estudios como el realizado por Guarnizo Arias, Prieto Sarmiento en Agility S.A., tu proyecto también ha identificado los riesgos existentes mediante un análisis detallado de amenazas y vulnerabilidades. Esto es crucial para definir las políticas y controles necesarios que minimicen estos riesgos.
- Metodología aplicada el ciclo DEMING, similar al utilizado en proyectos como el de Alfaro Lana y Vargas León en la Procuraduría General de la Nación. Esta metodología proporciona un marco estructurado para evaluar y analizar amenazas, así como para implementar políticas de seguridad basadas en los resultados obtenidos.
- La aplicación de la norma ISO/IEC 27001:2013 en tu proyecto sigue las mejores prácticas reconocidas internacionalmente para la gestión de la seguridad de la información. Esto se alinea con otros proyectos como el presentado por Merino Rosas en Ransa Comercial S.A., donde también se implementaron políticas basadas.
- Como menciona Remoilina Becerra, el desarrollo de políticas de seguridad cubre una amplia gama de aspectos cruciales para proteger la información y prevenir problemas relacionados, como fugas de información o uso indebido de datos. Esto subraya la importancia de implementar un plan de gestión de seguridad informática en todas las organizaciones.

Conclusiones

1. Se llevó a cabo el diseño e implementación de un plan de gestión de seguridad informática, demostrando su importancia esencial para proteger los activos informáticos expuestos a diversas amenazas. Este plan no solo establece políticas de seguridad, sino que también asigna responsabilidades claras para garantizar su cumplimiento. Delegar estas responsabilidades es fundamental para asegurar que las medidas de seguridad se apliquen de manera efectiva en toda la organización y se minimicen los riesgos cibernéticos.
2. El análisis del estado de la información en el sistema de gestión informática, mediante la aplicación de la metodología del ciclo DEMING, reveló que los activos identificados en la Municipalidad Distrital de Challhuahuacho están en riesgo. Se logró la implementación de políticas y controles de riesgos para mantener la seguridad de la información. La evaluación se realizó siguiendo las pautas establecidas por la norma ISO/IEC 27001:2013, lo que permitió identificar los problemas existentes en la gestión de la información.
3. Se logró identificar las amenazas, vulnerabilidades y el nivel de riesgo al que están expuestos los activos informáticos y de información. Además, se propusieron las mejoras necesarias para garantizar la seguridad de la información.
4. Se implementaron políticas de seguridad de la información en la Municipalidad que establecen lineamientos y responsabilidades para los trabajadores, mejorando la confidencialidad, integridad y disponibilidad de la información. El proyecto resalta la necesidad de un plan de gestión de seguridad informática siguiendo la norma ISO/IEC 27001:2013.

Recomendaciones

1. Es fundamental que todos los empleados de la Municipalidad Distrital de Challhuahuacho cumplan con las políticas de seguridad informática, ya que esto permitirá evaluar y prevenir los riesgos de manera oportuna.
2. Es importante establecer procesos de actualización del inventario de activos informáticos, con evaluaciones regulares para prevenir posibles daños. Estos procesos deben incluir información detallada sobre el estado actual de cada activo.
3. Se deben realizar revisiones periódicas de las amenazas registradas y los riesgos identificados, considerando los cambios tecnológicos y la implementación de nuevos proyectos. El objetivo es establecer controles permanentes y mantener actualizado el plan de gestión de seguridad informática vigente.
4. Es crucial llevar a cabo mantenimientos periódicos de las políticas de seguridad implementadas, dado que el entorno organizacional evoluciona constantemente debido a los avances tecnológicos

Bibliografía

Alfaro Vina, I. A., & Vargas Lón, E. (2021). *DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN MISIONAL DE LA PROCURADURÍA GENERAL DE LA NACIÓN*. Bogota.

Arana Fernandez, J. (2019). *SEGURIDAD EN AS TECNOLOGIAS DE LA INFORMACION*. Moquegua Peru.

Bojaca Garavito, E. A. (2021). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001- 27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SANFRANCISCO DE GACHETÁ.* Cundinamarca.

Borrero Ochoa, P. (2019). *IDENTIFICACIÓN DE ACTIVOS DE INFORMACIÓN, RIESGOS Y CONTROLES ASOCIADOS PARA LA EMPRESA ESTRATEGIAS EMPRESARIALES DE COLOMBIA BAJO LA NORMA ISO 27001 E ISO 31000.* Colombia.

Castillo Pineda, L. (2019). *EL MODELO DEMING COMO ESTRATEGIA COMPETITIVA PARA REALZAR EL POTENCIAL ADMINISTRATIVO.* Colombia.

Fukusaki Infantas, S., & Cruz Diaz, M. A. (2018). *DISEÑO E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA CLÍNICA MEDCAM PERÚ.* Lima Peru.

Guarnizo Arias, J. f., & Prieto Sarmiento, E. J. (2018). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA AGILITY S.A.S.* Bogota.

Guevara, M. (2018). *CONCEPTS BÁSICOS DE GESTIÓN DE RIESGOS.* El Salvador.

Hernandez Sampieri, R., Fernadez Collado, C., & Baptista Lucio, P. (2018). *Metodología de la Investigación.* Mexico.

Irurita Alzueta, J., & Villanueva Roldan, P. M. (2019). *SISTEMAS DE GESTIÓN DE LA CALIDAD.* Navarra - España.

Medina Iriarte, J. (2020). *"ESTANDARES PARA LA SEGURIDAD DE INFORMACIÓN CON TECNOLOGIAS DE INFORMACIÓN.* Chile.

Merino Rosas, e. A. (2021). *IMPLEMENTACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA CON LA NORMA ISO/IEC 27001 EN LA EMPRESA RANSA COMERCIAL S.A - PIURA; 2021*. Piura Perú.

Muñoz Hernandez, H. (2019). *RIESGOS INFORMÁTICOS Y ALTERNATIVAS PARA LA SEGURIDAD INFORMÁTICA EN SISTEMAS CONTABLES EN COLOMBIA.* Colombia.

Murillo, W. (2008). *La investigación científica.*

Norma Española, N. (2017). *Tecnología de la Información Técnicas de seguridad Código de prácticas para los controles de seguridad de la información (ISO/IEC 27002:2013 incluyendo Cor 1:2014 y Cor 2:2015).* España: UNE.

Noticias, B. (7 de Julio de 2024). *Ude Cataluña*. Obtenido de https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber

Reaño Rivera, J. (2022). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTION DE CALIDAD EN LA ISO 9001:2015 EN UN rESTAURANTE.* Lima Peru.

Remolina Becerra, L. C. (2019). *DISEÑO DE UN MODELO DE SEGURIDAD INFORMÁTICA A UNA EMPRESA EN SU SISTEMA DE MONITOREO DEL ÁREA DE TECNOLOGÍA.* Colombia.

Route. (25 de julio de 2022). *simpliroute*. Obtenido de https://simpliroute.com/es/blog/ciclo-de-deming

Vargas Cordero, Z. R. (2019). *LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA.* Costa Rica: Educacion.

Villo Guerrero, P. L. (2021). *MODELO DE GESTIÓN DE RIESGOS PARA SEGURIDAD INFORMATICA BAJO ISO/IEC27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA-2021*. Pimentel Paru.

yala Ñiquen, E. E. (2019). *TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.* España.

ANEXO

Anexo 01

- **Encuesta**

Encuesta dirigida al personal de trabajo de la Municipalidad Distrital de Challhuahhuacho para identificar la presencia de políticas de seguridad informática

a) **En cuanto a políticas generales de seguridad de la información**

1 ¿ Se tienen implementados controles relacionados a los accesos de equipos de cómputo y diferentes sistemas que maneja la Municipalidad Distrital de Challhuahuacho?

a Si

b No

c Algunas veces

2 ¿ Los usuarios asumen responsabilidades sobre el cuidado y protección de los equipos de cómputo?

a Si

b No

c Algunas veces

3 ¿ El personal en el área de sistemas cumple con informar cualquier anormalidad en los equipos de computo y/o problemas eléctricos?

a Si

b No

c Algunas veces

4 ¿Se exigen autorizaciones al personal que labora en la Municipalidad Distrital de Challhuahuacho, pueda sacar o ingresar hardware y/o software?

a Si

b No

c Algunas veces

b **En cuanto a las políticas de seguridad a nivel físico**

5 ¿ Existen normas que prohíben el consumo de alimentos donde se encuentren los equipos de computo?

a Si

b No

c Algunas veces

6 ¿ Se cuenta con respaldos de abastecimiento de energía en la Municipalidad Distrital de Challhuahuacho?

a Si

b No

c Algunas veces

7 Cuando se realizan los mantenimientos a los equipos de computo el responsable del área de sistemas ¿se encuentra presente?

a Si

b No

c Algunas veces

- **En cuanto a políticas de seguridad de nivel lógico**

8 ¿ El responsable del área de sistemas es el encargado de instalar y realizar el mantenimiento del sistema operativo?

a Si

b No

c Algunas veces

9 ¿ El responsable del área de sistemas es el encargado de instalar y realizar el mantenimiento del software de gestión documentaría (SIGA, SIAF)?

a Si

b No

c Algunas veces

10 ¿ El responsable del área de sistemas es el encargado de mantener la seguridad de la red.?

a Si

b No

c Algunas veces

11 ¿ El responsable del área de sistemas es el encargado de otorgar las claves de usuario y contraseñas.?

a Si

b No

c Algunas veces

- **En cuanto a las políticas a nivel de sistemas**

12 ¿ Los softwares que se usan para ingreso de datos y eliminación de datos tienen la opción de validación?

a Si

b No

c Algunas veces

13 ¿ Se tiene en consideración la recuperación de datos de forma automática?

a Si

b No

c Algunas veces

14 ¿Se tienen reuniones periódicas entre el área de sistemas y los usuarios que manejan los software que se tienen en la Municipalidad Distrital de Challhuahuacho, que asegure el buen uso del software?

a Si

b No

c Algunas veces

- **En cuanto a políticas de respaldos y recuperación de información**

15 ¿ Se tienen programados periodos específicos para la creación de respaldos?

a Si

b No

c Algunas veces

16 ¿ Se tienen dispositivos de almacenamiento dedicados solo para la creación de respaldos de información?

a Si

b No

c Algunas veces

- **En cuanto a las políticas a los equipos de computo**

17 ¿ Los equipos de computo que se encuentren configurados en red cumplen con los estándares correspondiente para su instalación?

a Si

b No

c Algunas veces

18 ¿ Se cuenta con una base de datos donde se encuentran registrados todos los equipos con las que cuenta la Municipalidad Distrital de Challhuahuacho ?

a Si

b No

c Algunas veces

19 ¿ El área de sistemas lleva acabo el mantenimiento tanto correctivo como preventivo de los equipos de cómputo con las que cuenta la Municipalidad Distrital de Challhuahuacho

a Si

b No

c Algunas veces

20 ¿ Los equipos de cómputo son actualizados periódicamente para ser reemplazados en caso de que estén desfasados?

a Si

b No

c Algunas veces

- **En cuanto a las políticas de accesos remotos**

21 ¿ El acceso de terceras personas al servicio de red se encuentra restringido?

a Si

b No

c Algunas veces

- **En cuanto apolíticas de control de virus y uso de software**

22 ¿ Los softwares que se usan en la Municipalidad Distrital de Challhuahuacho cuentan con licencias originales?

a Si

b No

c Algunas veces

23 ¿ Los antivirus instalados en los equipos de cómputo están activados y actualizados?

a Si

b No

c Algunas veces

Anexo 02

- **Acta de Constitución con la Municipalidad Distrital de Challhuahuacho**

Acta de Constitución del Proyecto

Diseño e Implementación del Plan de Gestión de Seguridad Informática en el Área Funcional de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho

Fecha: *[17/04/2023]*

.

18 de abril del 2023

CARTA N° 003-2023-OTISI/MDCH/ALR

SEÑOR:
LUIS IVAN CRUZ PUMA
Alcalde de la municipalidad de Distrito de Challhuahuacho

ASUNTO: Solicito firma de autorización para la implementación de mi proyecto de Tesis

Mediante el presente documento, me es grato dirigirme a su despacho, para saludarle muy fraternalmente y a la vez, presentarle mi proyecto de tesis titulado **"Diseño e Implementación del Plan de Gestión de Seguridad Informática en el Área Funcional de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho".** Para lo cual solicito firma de autorización en el Acta de Constitución de proyecto adjunto en el presente, para implementar el proyecto de tesis en mención.

El proyecto se desarrollará en la municipalidad Distrital de Challhuahuacho el plan de gestión de seguridad informática permitirá la protección a la información sensible que incluye información sobre los empleados, usuarios y personal directivo, información de valor, datos financieros, registros legales y datos personales, resguardar la información de SIGA y SIAF tener a disponibilidad en tiempo real los recursos de los sistemas informáticos que administra la municipalidad, con lo que se obtendrá los siguientes beneficios.

- Confidencialidad de la Información.
- Integridad de la Información.
- Disponibilidad de la Información.

Se adjunta:

- Acta de Constitución de Proyecto de Tesis
- Plan de Tesis

Es todo cuanto tengo que informar a Ud., aprovecho la oportunidad para expresar mi estima personal.

SECRETARIA GENERAL
Exp.: 1027 N° de folios: 36
Hora: 2:39
Firma
Fecha: 14/04/2023

ANIBAL LIMA RAMOS
DNI: 73737128

Acta de Constitución del Proyecto

Empresa / Organización	Municipalidad Distrital de Challhuahuacho
Proyecto	Diseño e implementación del plan de gestión de seguridad informática en la Municipalidad Distrital de Challhuahuacho
Fecha de preparación	17 de abril 2023

JUSTIFICACIÓN DEL PROYECTO

La información manejada en las diferentes áreas de la Municipalidad Distrital de Challhuahuacho, está expuesta por lo que se hace vulnerable a diferentes amenazas entre ellas la intrusión no permitida a la información sobre todo por personal interno pudiendo tener acceso datos y ser manipulados, por lo que se presenta la necesidad de considerar alternativas de solución a este problema, entre ellas establecer sistemas de gestión de seguridad de la información.

Un sistema de gestión de seguridad de la información (SGSI) va a permitir a la Municipalidad que tenga una estructura en su organización, con roles y responsabilidades en conjunto, con políticas coherentes a los objetivos de seguridad en los diferentes niveles de la institución, el diseño de gestión de seguridad se basara en la norma ISO/IEC 27001:2014, ya que nos proporciona medios necesarios para obtener la seguridad necesaria de la información que ayude a la viabilidad en la dirección y logro de objetivos de la diferentes áreas de la Municipalidad.

V°B° JEFE DE LA UNIDAD DE RECURSOS HUMANOS

DETALLES DEL PROYECTO

El proyecto se desarrollará en la Municipalidad Distrital de Challhuahuacho, este plan de gestión de seguridad informática permitirá la protección a la información sensible que incluye información sobre los empleados, usuarios y personal directivo, información de valor, datos financieros, registros legales y datos personales.

Para ello se llevaron a cabo la recopilación de datos con las personas interesadas en la implementación del plan de gestión de seguridad informática, con lo que obtendremos los siguientes beneficios.

- ✓ Confidencialidad de la información.
- ✓ Integridad de la información.
- ✓ Disponibilidad de la información.

Con todo esto se busca que se logre tomar acciones para mejorar la protección de la información que se considere sensible

Miembros del equipo:

Patrocinador	: Alcalde de la Municipalidad Distrital de Challhuahuacho
Líder del Proyecto	: Lima Ramos, Aníbal
El proyecto iniciara el 17 de abril del 2023 hasta el 16 de junio, con una duración de dos meses	

ALCANCE PRELIMINAR

El alcance que tiene este proyecto es la de implementar un plan de gestión de seguridad informática que mejorará la protección de información en el área funcional de tecnologías de la información de la Municipalidad Distrital de Challhuahuacho.

Se aplicarán las siguientes acciones:

- Identificar el estado de la Seguridad de información de la Municipalidad Distrital de Challhuahuacho.
- Determinar el estado de la Protección de datos del sistema de gestión de seguridad informática de la Municipalidad Distrital de Challhuahuacho.
- Definir las políticas de seguridad de acuerdo a las normas de los sistemas de gestión de seguridad Informática que se requieren en el área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho.

EXCLUSIONES DEL PROYECTO

- Se cuenta con una línea de tiempo de tres meses para la implementación del Plan de Gestión de Seguridad Informática
- El tiempo de entrega será de acuerdo al cronograma establecido cumpliendo las fechas que han sido determinadas.

FINALIDAD DEL PROYECTO

Implementar un plan de gestión de seguridad informática que mejorará la protección de información en el área funcional de tecnologías de la información de la Municipalidad Distrital de Challhuahuacho. En el tiempo planeado de 2 meses, cumpliendo en un 100% la implementación de las diferentes políticas de seguridad para resguardar la información, por lo que es necesario tener a disponibilidad los recursos y poder alcanzar los objetivos de que fueron definidos en el caso de negocio.

OBJETIVO DEL PROYECTO		
CONCEPTO	**OBJETIVOS**	**CRITERIOS DE ÉXITO**
ALCANCE	Cumplir con Implementar un plan de gestión de seguridad informática en su totalidad, cumpliendo con lo establecido en un 100%	Que se consiga mantener la seguridad en la información
TIEMPO	Que el proyecto concluya en un tiempo de tres meses, tiempo establecido de acuerdo al cronograma propuesto	Terminar el proyecto en el tiempo planificado

FACTORES CRÍTICOS DE ÉXITO
No obtener la información correspondiente en el momento adecuado
No estar de acuerdo en los alcances propuestos por parte del interesado.
La falta de coordinación para las reuniones de trabajo con la parte interesada

RESTRICCIONES DEL PROYECTO
DE TIEMPO:
El proyecto no debe de tener una duración de más de 02 (dos) meses
DE PERSONAL:
Para la implementación del sistema se considerará un horario laboral, que será de lunes a viernes de 8 am. a 1 pm. y de 3 a 6 pm. Se excluyen los días que no son laborales que se designan por ley

SUPUESTOS DEL PROYECTO
✓ La gestión del proyecto será realizada en la Municipalidad Distrital de Challhuahuacho, desde el área funcional de tecnologías de la información.
✓ La Municipalidad Distrital de Challhuahuacho deberá tener participación en la revisión de los diferentes entregables a medida que se vayan realizando.
✓ Existe una buena comunicación verbal y escrita con los interesados.
✓ Se cuenta con personal eficiente y con experiencia para llevar a cabo las tareas designadas para el desarrollo del proyecto.
✓ Se va a obtener la información necesaria y apropiada, para la gestión de todas las partes del proyecto.
✓ Al ser aprobado los entregables, las personas responsables estarán sujetos a cumplir con los plazos que ya fueron definidos.
✓ Se llevarán a cabo capacitaciones para aplicar las diferentes políticas de seguridad establecidas, acorde al cronograma establecido

ORGANIZACIÓN O GRUPOS ORGANIZACIONALES QUE INTERVIENEN EN EL PROYECTO	
Organización	***Rol que Desempeña***
Lima Ramos, Aníbal (LRA)	Proveer el servicio de implementación de un plan de gestión de seguridad informática
Municipalidad Distrital de Challhuahuacho	Demandante del servicio de implementación del plan de gestión de seguridad informática

DEFINICIÓN DE REQUISITOS DEL PROYECTO		
Stakeholder (Interesado)	***Necesidades Expectativas, deseos***	***Rol de requerimiento del proyecto***
Lima Ramos, Aníbal (LRA)	Implementar un plan de gestión de seguridad informática	• Identificar el estado de la Seguridad de información dentro de la Municipalidad Distrital de Challhuahuacho. • Llevar a cabo la planificación dentro del tiempo requerido. • Organizar y cumplir con las actividades fijadas para las fechas establecidas
Municipalidad Distrital de Challhuahuacho.	Contar con un plan de gestión de seguridad informática, para preservar la información	• Los entregables deben tener un inicio y realizar la entrega en tiempos establecidos. • Los entregables cumplirán con las diferentes especificaciones técnicas y características de calidad de acuerdo a los estándares manejados por la institución. • Los entregables cumplirán con las diferentes especificaciones técnicas y características de calidad de acuerdo a los estándares manejados por la ISO/IEC 27001:2014 • Se hace la entrega de responsabilidad de la implementación del plan de gestión de seguridad informática a un profesional responsable y conocedor de este rubro

	El proyecto hará uso de los estándares que ya están definido por la ISO/IEC 27001:2014	Se respetarán los estándares y normativas vigentes

PRINCIPALES ENTREGABLES
a) Identificación y definición de objetivos, alcances, identificación de riesgos y métodos de tratamiento de riesgos e inventario de activos
b) Plan de tratamiento de riesgos, políticas y procedimientos para el control de riesgos
c) Plan de monitoreo y auditorías internas preventivas periódicas
d) Informes de resultados obtenidos luego de a implementación del plan de gestión de seguridad informática
e) Informe de resultados de auditorias

SOLUCIÓN DE CONFLICTOS
Las especificaciones del proyecto serán revisadas por el interventor, quien realizara los comentarios y observaciones que sean necesarios, se llevarán a cabo reuniones con ambas partes para poder llegar a acuerdos, que serán plasmadas de manera escrita. Se realizarán revisiones necesarias para poder llegar al compendio final, que se considera como documento de cumplimiento obligatorio

SPONSOR QUE AUTORIZA EL PROYECTO			
NOMBRE	INSTITUCION	CARGO	FECHA
Alcalde	Municipalidad Distrital de Challhuahuacho	Alcalde de la Municipalidad Distrital de Challhuahuacho	17/04/2023

V°B°
JEFE DE LA UNIDAD DE RECURSOS HUMANOS

MUNICIPALIDAD DISTRITAL DE CHALLHUAHUACHO
COTABAMBAS - APURIMAC
Abg. Miriam Alicioneth Quispe Huamani
JEFE DE LA OFICINA DE RECURSOS HUMANOS

PLAN DE SEGURIDAD DE LA INFORMACIÓN

2022

MUNICIPALIDAD DISTRITAL DE CHALLHUAHUACHO

INTRODUCCIÓN

La gestión y almacenamiento de la información supone que se aseguren los medios de almacenamiento de la misma, así como que se establezcan los controles necesarios para acceder a ella. En lo que respecta a la seguridad de la información ésta debe ser gestionada de manera eficiente para asegurar su integridad, confidencialidad y disponibilidad, y de esto se encarga un Sistema de Gestión de Seguridad de la Información.

La seguridad de la información es crucial para las organizaciones, siendo la gestión de la seguridad de la información (SGSI) un proceso clave para enfrentar amenazas y gestionar riesgos de manera efectiva. En el caso de la Municipalidad Distrital de Challhuahuacho, las diversas áreas interconectadas por una red de comunicaciones manejan información digital para ofrecer servicios oportunos a los usuarios. Sin embargo, se enfrentan a problemas significativos como la pérdida y alteración de información debido a vulnerabilidades en el acceso a través de la red, debido a la falta de protocolos adecuados para establecer accesos restringidos. El problema central identificado es la falta de seguridad informática en el área de tecnologías de la información de la Municipalidad, lo cual compromete la protección e integridad de los datos. El objetivo general propuesto es diseñar e implementar un plan de gestión de seguridad informática para mejorar esta situación. Se adopta el ciclo Deming (PDCA: Planificar, Hacer, Verificar, Actuar) como metodología para el desarrollo del proyecto, asegurando un enfoque sistemático y cíclico para implementar un sistema de gestión de seguridad informática efectivo. El resultado obtenido incluye el diseño detallado del plan de gestión de seguridad informática, que define acciones concretas para mejorar la protección de la información. Este plan se implementará con revisiones y actualizaciones periódicas para garantizar su eficacia continua. En conclusión, se destaca la importancia crucial de contar con un plan de gestión de seguridad informática para proteger los activos informáticos de la Municipalidad ante Palabras Clave. Gestión de seguridad informática, normas de seguridad informática diversas amenazas.

En el marco de estas atribuciones, la Municipalidad Distrital de Challhuahuahco implementa el presente Plan de Seguridad de la Información el cual describe las actividades planificadas en lo que va del año y que están orientadas a iniciar el seguimiento del Sistema de Gestión de Seguridad de la Información, con miras a proteger la confidencialidad, integridad y disponibilidad de la información que administra la Municipalidad.

1. BASE LEGAL

1.1. Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
1.2. Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
1.3. Decreto de Urgencia N° 006-2020, que crea el Sistema Nacional de Transformación Digital.
1.4. Decreto de Urgencia N° 007-2020, se aprueba el Marco de Confianza Digital y se dispone medidas para su fortalecimiento.
1.5. Decreto de Urgencia Nº 021-2020, que establece el Modelo de Ejecución de Inversiones Públicas a través de Proyectos Especiales de Inversión Pública.
1.6. Decreto Supremo N° 011-2020-MINEDU, que crea el Proyecto Especial de Inversión Pública Escuelas Bicentenario.
1.7. Decreto Supremo N° 119-2020-EF, que aprueba el Reglamento de Proyectos Especiales de Inversión Pública
1.8. Resolución Ministerial N° 338-2020-MINEDU, que aprueba el "Manual de Operaciones del Proyecto Especial de Inversión Pública Escuelas Bicentenario".
1.9. Resolución Ministerial N° 004-2016-PCM que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO-IEC 27001:2014, Tecnología de la Información. Requisitos 2da Edición" en todas las entidades integrantes del Sistema Nacional de Informática.

2. OBJETIVO

Diseñar plan de gestión de seguridad informática para mejorar la protección de la información a través del área de Tecnologías de la Información de la Municipalidad Distrital de Challhuahuacho.

3. FINALIDAD

3.1. Planificar las acciones que conduzcan a la implementación del SGSI.
3.2. Iniciar acciones a fin de contar con normas, directivas, procedimientos en materia de seguridad.
3.3. Proteger la información de la Municipalidad Distrital de Challhuahuacho de las amenazas y peligros a la que se puede encontrar expuesta.
3.4. Proteger contra acceso o uso no autorizado los datos e información, los cuales podrían resultar en un daño sustancial a la institución.

4. ALCANCE

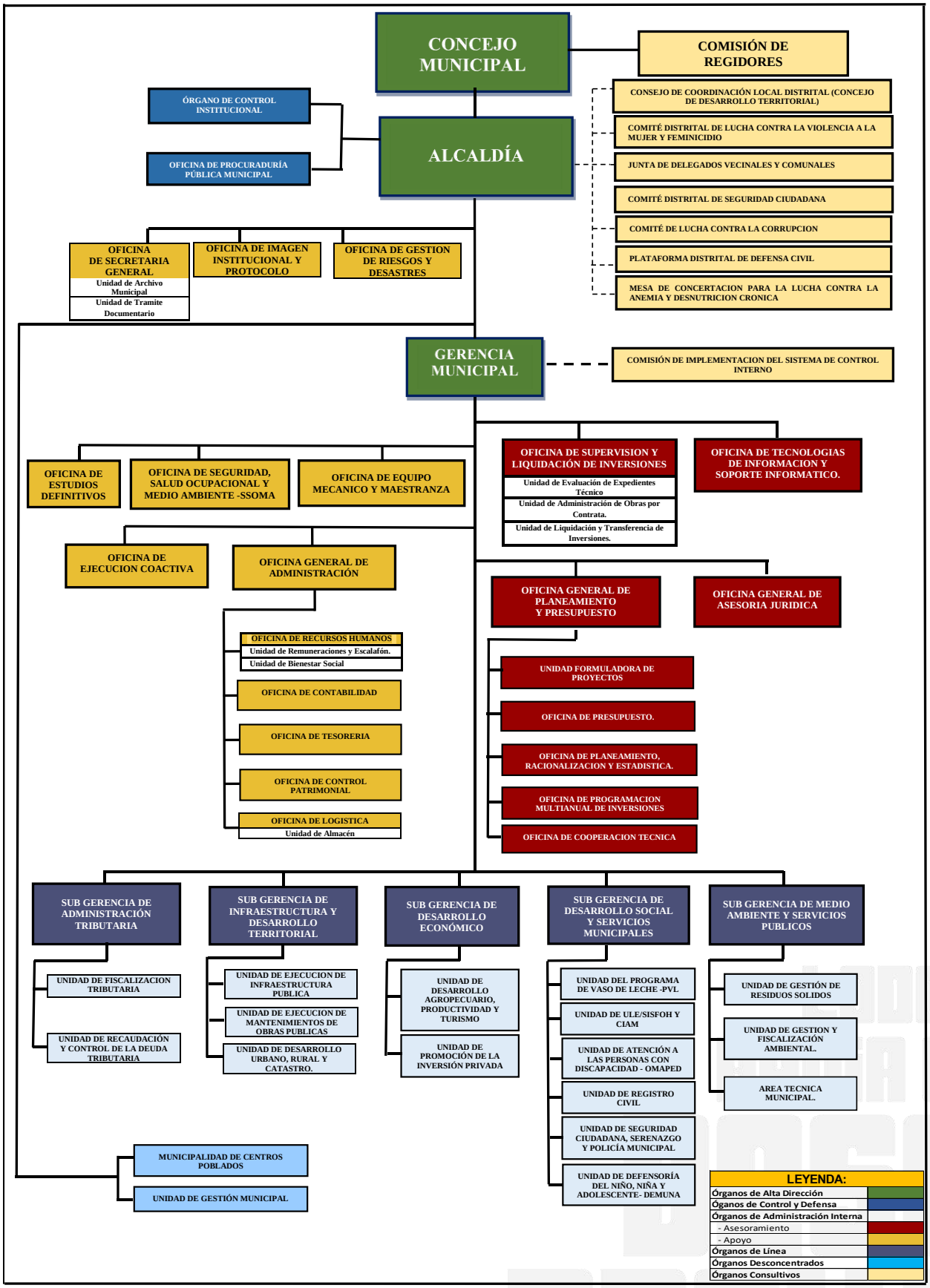
El presente plan de seguridad tiene alcances a toda información que independientemente de su formato y soporte; es adquirida, transmitida, procesada, almacenada y/o mantenida en la Municipalidad Distrital de Challhuahuacho.

5. ENTORNO DE LA MUNICIPALIDAD DISTRITAL DE CHALLHUAHUACHO

5.1. Organización

La Municipalidad se encuentra organizada funcionalmente de la siguiente forma:

II. ORGANIGRAMA ESTRUCTURAL DE LA MUNICIPALIDAD DISTRITAL DE CHALLHUAHUACHO SEGÚN ORDENANZA MUNICIPAL Nº 005-2021-MDCH/C-A



Para la gestión de los temas vinculados a la seguridad de la información se cuenta con:

- Oficina de Tecnologías de Información

5.2. Funciones

La Municipalidad Distrital de Challhuahuacho señala que la Oficina de Tecnologías de la Información es la unidad funcional de apoyo responsable del desarrollo, implementación y mantenimiento de Software; la implementación y mantenimiento de las redes y comunicaciones; así como gestionar los servicios de tecnologías de la información institucional; *asegurar el cumplimiento de los sistemas de gestión orientados a la Seguridad de la Información en el ámbito de la Municipalidad y formular los planes basados en buenas prácticas en gobierno y gestión de las tecnologías de la información*.

Asimismo, establece como una de sus funciones:

Coordinar y supervisar las actividades de seguridad de la información de la Municipalidad, así como la implementación y mantenimiento del sistema de gestión de la seguridad de la Información.

5.3. Infraestructura Tecnológica

La infraestructura tecnológica que administra la Municipalidad Distrital de Challhuahuacho está compuesta por:

- Servicio de Correo Electrónico en nube
- Servidores de los sistemas de información.

5.4. Sistemas de Información

La OTI se encarga del desarrollo, mantenimiento y soporte técnico funcional de los siguientes sistemas de información:

- Sistema de tramite documentario
- Página web institucional y portal de transparencia
- SIGA y SIAF (administración de cuentas)

6. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

6.1. OBJETIVOS EN MATERIA DE SEGURIDAD

OBJ.01	Establecer la seguridad estratégica dentro de la municipalidad formulando e implementando políticas, controles, procedimientos y otros componentes del Sistema de Gestión de Seguridad de la Información.
OBJ.02	Prevenir la materialización de riesgos de seguridad informática a través de la identificación inicial de vulnerabilidades sobre la infraestructura tecnológica, así como mediante la implementación de controles mitigantes de seguridad a fin de gestionar los riesgos dentro de niveles aceptables.
OBJ.03	Implementar políticas de seguridad informática para la protección de información a través del área funcional de tecnologías de la Municipalidad Distrital de Challhuahuacho

6.2. Seguridad Estratégica

La oficina de tecnologías de información tiene como responsabilidad la implementación del Sistema de Gestión de Seguridad de la Información – SGSI en la Municipalidad. Asimismo, la implementación de un SGSI es un imperativo en las entidades de la Administración Pública conforme lo señalado por el D.U. N° 007-2020. La seguridad estratégica se encarga de alinear el SGSI con los objetivos de la organización en materia de seguridad. Estos objetivos deben estar vinculados a:

- Brindar soluciones de seguridad de la información a los procesos de la institución, tomando en cuenta la cultura y la estructura de la organización, el gobierno de TI, y la infraestructura tecnológica de la Municipalidad Distrital de Challhuahuacho.
- Contar con una inversión en Seguridad de la Información que debe ser congruente con la estrategia y las operaciones de la Municipalidad, y con un perfil bien definido de amenaza, vulnerabilidad y riesgo.

6.3. Seguridad Táctica Operacional

Respecto a la seguridad táctica operacional se requiere proteger los componentes de infraestructura tecnológica y de comunicación que soportan la operación de la institución enfocándose principalmente en hardware y software, favoreciendo la utilización de las herramientas informáticas de manera apropiada. Se puede decir que el análisis de riesgos se orienta principalmente en identificar vulnerabilidades de hardware y/o software sobre la infraestructura, con el fin de mitigar y llevar el riesgo a un nivel aceptable a través de acciones preventivas y correctivas.

Como parte de seguridad informática se debe realizar:

- ❖ Identificación de vulnerabilidades de seguridad en la Infraestructura Tecnológica.
- ❖ Análisis de vulnerabilidades en entornos productivos y no productivos.

7. IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Un Sistema de Gestión de Seguridad de la Información – SGSI, es un conjunto de políticas de administración de la información. Es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Algunos de los beneficios de implementar un SGSI se listan a continuación:

- ❖ Preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos.
- ❖ Reducción de costos por el tratamiento oportuno de los riesgos de seguridad de la información, evitando su materialización.
- ❖ Permite gestionar los riesgos de seguridad de la información a través de un marco metodológico.
- ❖ Cumplimiento normativo.
- ❖ Permite prevenir incidentes de seguridad de la información.
- ❖ Fomenta una cultura de seguridad y mejora continua
- ❖ Proporciona confianza en la Institución.
- ❖ Liderazgo institucional.

a) Aspectos críticos en la implementación del SGSI

En la implementación y gestión de un SGSI, se deben considerar los siguientes aspectos:

- **Gestión de riesgos:**

  Se deben ejecutar medidas apropiadas para mitigar los riesgos y reducir el posible impacto que tendrían en los recursos de información. Gestionar los riesgos hacia un nivel aceptable requiere de:

  - ❖ Entendimiento colectivo del perfil de amenaza, vulnerabilidad y riesgo de la organización.
  - ❖ Entendimiento de la exposición al riesgo y las posibles consecuencias de la inestabilidad.
  - ❖ Conciencia de las prioridades de la gestión de riesgos con base en las posibles consecuencias.

❖ Suficiente mitigación de riesgos para obtener consecuencias aceptables de riesgo residual.
❖ Aceptación / transferencia del riesgo a partir de un entendimiento de las posibles consecuencias del riesgo residual.

- **Políticas, procedimientos y directrices:**
  La normatividad en seguridad está expresada en Políticas, Normas, procedimientos y directrices.

  Políticas generales:
  - ❖ Para acceder a los diferentes sistemas de gestión documental, es necesario que el usuario cuente con una clave de acceso, cuya administración recae en el responsable del sistema.
  - ❖ Los usuarios tendrán acceso únicamente a los equipos de cómputo que estén autorizados.
  - ❖ Las claves asignadas a los diferentes usuarios deberán ser actualizadas cada 4 meses, permitiendo al usuario cambiar la contraseña en cualquier momento.
  - ❖ Las aplicaciones utilizadas por los usuarios deben clasificarse en públicas y privadas.
  - ❖ Si la contraseña no se modifica dentro del plazo establecido, deberá ser eliminada, exceptuando casos relacionados con enfermedades o maternidad.
  - ❖ No se permitirá el ingreso de personas ajenas y no autorizadas al área y/o departamento de sistemas.
  - ❖ Los documentos pertenecientes al software de la Municipalidad Distrital de Challhuahuacho, como manuales y tutoriales, estarán bajo el resguardo del responsable del área de sistemas.
  - ❖ El área de recursos humanos deberá comunicar al área de sistemas.
  - ❖ El área de recursos humanos deberá comunicar el retiro de los empleados para que sean eliminados de la base de datos.
  - ❖ En conjunto con los usuarios relacionados con la base de datos, se realizará una limpieza de los discos duros (HDD).
  - ❖ Cada usuario es responsable del cuidado y protección de los equipos de cómputo.
  - ❖ La información en los discos duros es responsabilidad del usuario, quien debe crear respaldos siguiendo los estándares establecidos.
  - ❖ El personal responsable del área de sistemas tendrá la obligación de comunicar cualquier anormalidad, así como problemas eléctricos, para su reparación o mantenimiento correspondiente.
  - ❖ Todos los equipos de cómputo deben tener activada una clave de inicio y un protector de pantalla.

- ❖ Se requiere autorización para ingresar o retirar hardware y/o software propiedad de la Municipalidad Distrital de Challhuahuacho.
- ❖ Los softwares instalados deberán contar con licencias originales.

Políticas de seguridad a nivel físico:

- ❖ Solo se podrá ingresar al área de sistemas con autorización.
- ❖ Se debe notificar al personal de seguridad laboral en caso de incidentes relacionados con incendios, accidentes eléctricos o situaciones de fuerza mayor.
- ❖ Se prohíbe el consumo de alimentos y bebidas cerca de los equipos de cómputo.
- ❖ Los extintores de incendios deben recibir mantenimiento periódico y estar ubicados en las diferentes áreas de la Municipalidad Distrital de Challhuahuacho.
- ❖ Se deben contar con equipos que respalden el abastecimiento de energía, como los UPS, que aseguran el apagado sistemático y regulado.
- ❖ Es recomendable que los equipos de hardware estén asegurados por una compañía de seguros.
- ❖ Se recomienda que el área de sistemas cuente con vigilancia permanente.
- ❖ El responsable del área de sistemas debe estar presente durante el mantenimiento de los equipos de cómputo.
- ❖ Mantener un control de las condiciones ambientales, verificando que no afecten el funcionamiento de las instalaciones, la información y los equipos de respaldo.

Políticas a nivel lógico:

- ❖ Los incidentes ocurridos con los activos informáticos que provocan dificultades en el buen desempeño del área de informática deben registrarse en una base de datos de incidentes.
- ❖ La instalación y mantenimiento del sistema operativo solo podrán ser realizados por el responsable del área de sistemas. La instalación y mantenimiento de los sistemas de gestión documental (SIGA, SIAF) solo podrán ser realizados por el responsable del área de sistemas.
- ❖ La instalación y actualización de la base de datos estarán a cargo del responsable del área de sistemas.
- ❖ La responsabilidad de mantener la estructura lógica y la seguridad de la red recae en el responsable del área de sistemas.
- ❖ El responsable de otorgar las claves de usuario y crear los usuarios será el área de sistemas.

- Se otorgarán claves de acceso de software solo a los usuarios encargados de manejar dicho software.
- Se deben implementar medios contra ataques maliciosos provenientes de hackers o programas dañinos.
- Para apoyar la protección de la red, se deben implementar equipos de firewall.

Políticas a nivel de sistemas:

- Los softwares y las aplicaciones en las que se deben ingresar datos deben tener la opción de ser validados previamente.
- Los softwares donde se modifican, ingresan y eliminan datos deben considerar la generación de registros de verificación, que ayuden a auditar los datos, como fecha, hora y otros.
- De acuerdo al diseño de los diferentes sistemas, se deben considerar roles para los usuarios según la actividad que cumplen, agrupándolos de acuerdo a la clase y/o tipo.
- En caso de que ocurra una falla del sistema, se debe considerar la recuperación automática de la información.
- Las normas del área de sistemas deben ser consideradas en el diseño y desarrollo de los sistemas.
- Se deben planificar reuniones periódicas con los usuarios de los diferentes software y aplicaciones para asegurar el buen uso y desempeño de los mismos.
- La ejecución de sistemas que contengan datos privados debe realizarse a nivel de usuario y/o en un equipo específico.
- Si se cuenta con sistemas diseñados para la empresa, se debe entregar la documentación del diseño lógico y el código al responsable del área de sistemas. La documentación incluye: manual técnico del sistema, manual de usuario y manual de operador.
- Al recibir un sistema que ha sido diseñado para la organización, se debe firmar un acta de entrega y recibido como garantía de propiedad del autor.

Políticas de respaldo y recuperación de información:

- De acuerdo a la importancia del respaldo, se debe establecer tiempos entre respaldos.
- Para los respaldos se usarán diferentes dispositivos de almacenamiento para la base de datos, aplicaciones, usuarios, archivos documentales y archivos del sistema operativo.
- Los respaldos se deben mantener en lugares seguros.
- Los respaldos de archivos estarán disponibles en línea por dos años; posteriormente, serán resguardados en servidores.

Políticas relacionadas a los equipos de cómputo:

- Todos los equipos de informática que cuenten con configuración deben considerar la infraestructura de la red de la organización, siguiendo los diferentes estándares y la instalación del área de sistemas.
- Se debe crear una base de datos coordinada con las áreas de administración y sistemas, que incluya todos los equipos que tiene la organización.
- El área de sistemas es responsable de todas las operaciones relacionadas con los equipos informáticos, así como de su asignación y rotación
- La seguridad física del equipo será responsabilidad del usuario.

Políticas de mantenimiento de equipos:

- El área de sistemas tiene la responsabilidad de realizar y controlar las actividades de mantenimiento preventivo y correctivo de los diferentes equipos informáticos, para garantizar la seguridad de los equipos.
- Se debe considerar el contrato de organizaciones externas a la institución como complemento para el mantenimiento de los equipos informáticos que hayan cumplido con su tiempo de vida útil.
- La autorización para llevar a cabo el mantenimiento de los equipos de cómputo no alcanza a los usuarios.
- Se debe mantener actualizado el plan de mantenimiento preventivo para los equipos, para estar al tanto de las necesidades que se presenten
- Los equipos informáticos de la organización deben actualizarse de manera periódica para mantener su conservación y funcionamiento adecuado.

Políticas de acceso remoto:

- El área de sistemas tiene la responsabilidad de dar autorizaciones a terceras personas para que puedan usar los recursos informáticos de la red.
- Se deben cumplir los lineamientos dispuestos por el área de sistemas para tener accesos remotos.
-

Políticas de control de virus, uso de software:

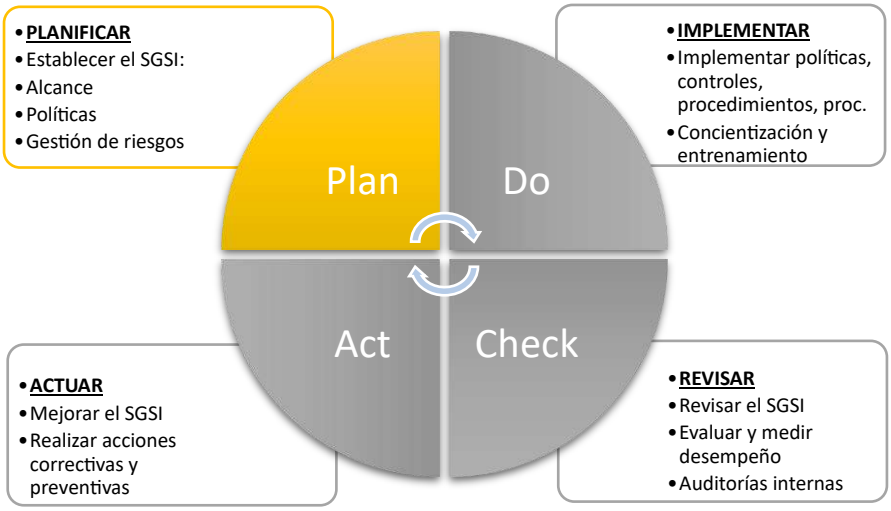
- El software que se use debe tener licencias adquiridas por la organización.
- El área de sistemas debe garantizar que el antivirus instalado en los equipos de cómputo funcione correctamente y que las actualizaciones estén disponibles.
- Se debe configurar el antivirus para que escanee el dispositivo de almacenamiento al ser conectado al equipo de cómputo.

• **Plan de director:**

El plan director del Sistema de Gestión de Seguridad de la Información es el conjunto de objetivos, proyectos y actividades como resultado de un análisis detallado de las necesidades de la organización en materia de seguridad de la información.

b) Ciclo Deming para el seguimiento de la implementación del SGSI

El seguimiento de la implementación del Sistema de Gestión de Seguridad de la Información se desarrolla siguiendo el ciclo de Deming



c) Matriz de actividades a desarrollar en cada fase del ciclo

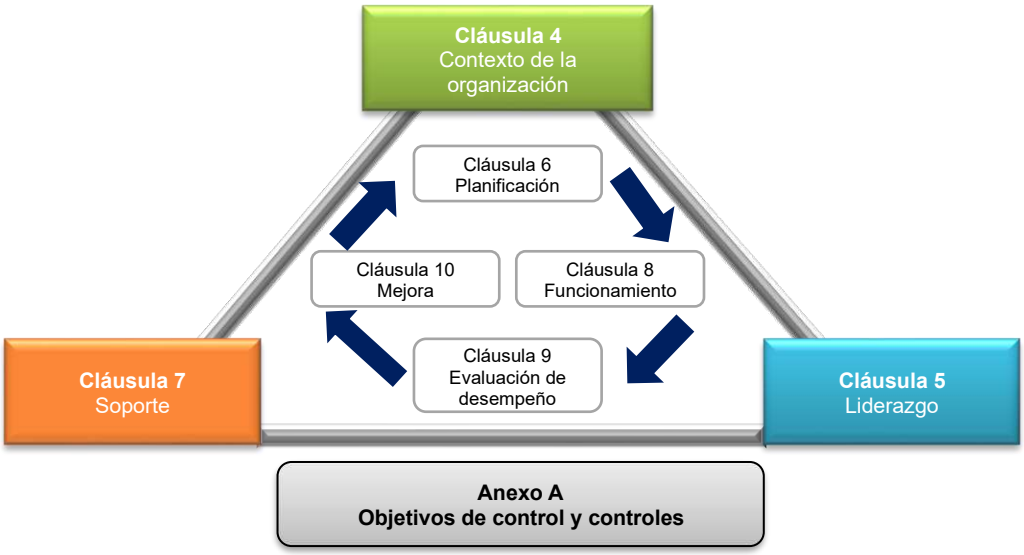
Cada fase puede involucrar el desarrollo de las siguientes actividades:

Planear (Plan)	Hacer (Do)	Revisar (Check)	Actuar (Act)
•Elaborar documento de contexto externo e interno • Elaborar matriz de requisitos de partes interesadas • Elaborar Directivas de Seguridad de la Información •Elaborar procedimientos (acciones correctivas, gestión de incidentes de seguridad de la información; entre otros). •Elaborar inventario y valoración de activos de información • Identificar, analizar y evaluar riesgos y oportunidades de seguridad de la información •Elaborar plan de tratamiento de riesgos y oportunidades de seguridad de la información •Elaborar Declaración de Aplicabilidad •Elaborar matriz de indicadores del Sistema de Gestión de Seguridad de la Información •Elaborar plan de comunicación •Elaborar plan de capacitación y concientización en seguridad de la información •Elaborar plan de monitoreo, medición, análisis y evaluación de resultados •Elaborar programa de auditoría •Elaborar Manual del SGSI.	•Gestionar y/o realizar la implementación de controles de seguridad de la información establecidos en el Plan de Tratamiento de Riesgos •Implementación de Directivas y procedimientos •Realizar capacitación y concientización en seguridad de la información •Gestionar los incidentes de seguridad de la información	•Revisar la conformidad de los requisitos de la NTP ISO/IEC 27001: 2014 y el cumplimiento y/o la implementación de los controles de seguridad de la información • Realizar Auditoría Interna •Realizar la revisión por la Dirección (Comité) •Realizar Auditoría Externa de Certificación	•Establecer e implementar Acciones Correctivas para las No Conformidades u observaciones como resultado de las revisiones, Auditoría Interna y Auditoría Externa de Certificación. •Establecer e implementar acciones de mejora continua en base a la recomendación es u observaciones como resultado de la revisión de la Dirección.

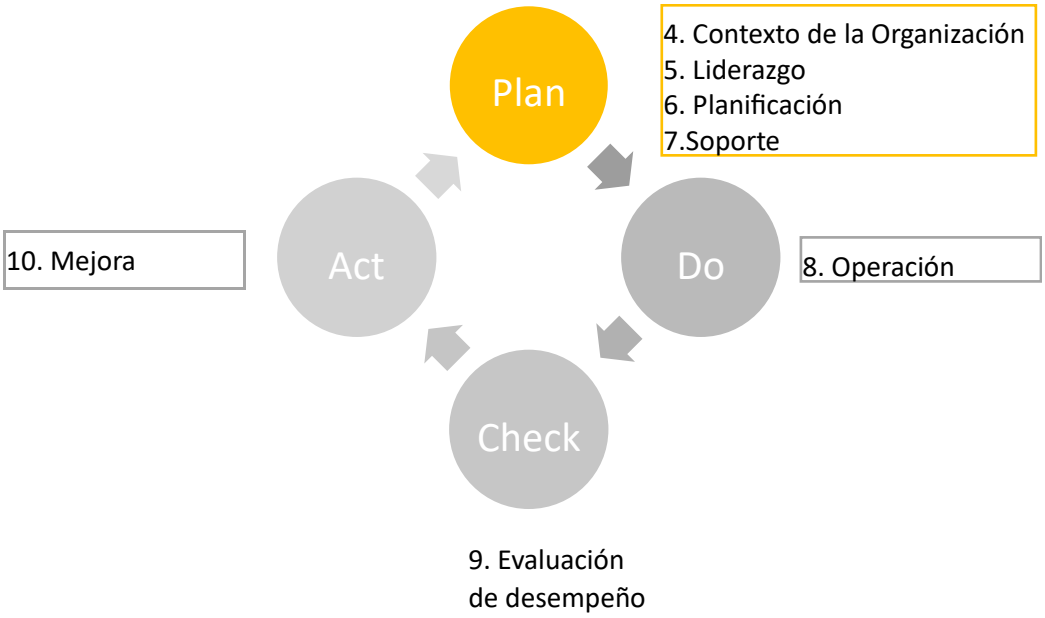
8. ALCANCE INICIAL PARA LA IMPLEMENTACIÓN DEL SGSI

El SGSI se implementa de acuerdo a la NTP ISO/IEC 27001:2014 la cual proporciona los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información.

La norma está estructurada en 10 cláusulas y un Anexo que especifica los objetivos de control y controles de seguridad.

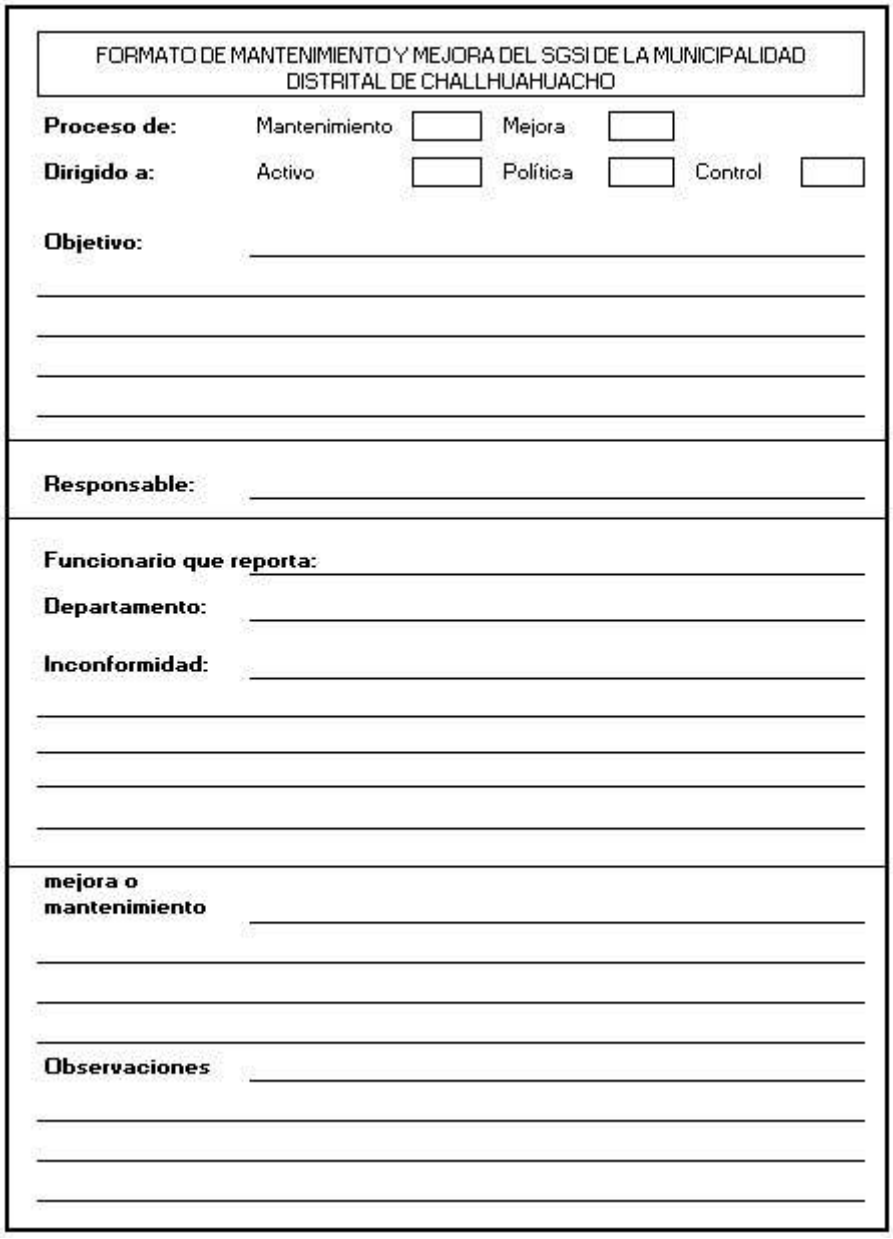


La implementación del SGSI iniciaría con la Fase "*Planificar*", desarrollando las cláusulas 4, 5, 6 y 7 de la NTP ISO/IEC 27001:2014.



Anexo 03

- **Formato para realizar el mantenimiento y mejora del sistema de gestión de seguridad informática (SGSI) de la Municipalidad Distrital de Challhuahuacho**



FORMATO DE MANTENIMIENTO Y MEJORA DEL SGSI DE LA MUNICIPALIDAD DISTRITAL DE CHALLHUAHUACHO

Proceso de: Mantenimiento ☐ Mejora ☐

Dirigido a: Activo ☐ Política ☐ Control ☐

Objetivo: _____

Responsable: _____

Funcionario que reporta: _____

Departamento: _____

Inconformidad: _____

mejora o mantenimiento _____

Observaciones _____

Figura 4.21: Implementación de Políticas de Seguridad Informática

Fuente: Elaboración Propia

.