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

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA NTP ISO/IEC 27001:2014 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE CHAMACA, CHUMBIVILCAS, CUSCO

PRESENTADO POR:

AUTOR:

BR. ALCIDES LAROTA CUITO

PARA OPTAR AL TÍTULO PROFESIONAL DE INGENIERO INFORMÁTICO Y DE SISTEMAS

ASESOR:

MGT. JULIO CESAR CARBAJAL LUNA

CUSCO – PERÚ

2024

INFORME DE ORIGINALIDAD

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

El que suscribe, **Asesor** del trabajo deinvestigación/tesis titulada: PROPUESTA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA NTP ISO/IEC 27001:2014 PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE CHAMACA, CHUMBIVILCAS, CUSCO

presentado por: ALCIDES LAROTA CUITO con DNI Nro.: 46621444 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 2 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 7 **%.**

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, 04 de FEBRERO de 2024

.....

Firma

Post firma JULIO CESAR CARBAJAL LUNA

Nro. de DNI 23903765

ORCID del Asesor 0000-0003-2629-250X

Se adjunta:

1. Reporte generado por el Sistema Antiplagio.
2. Enlace del Reporte Generado por el Sistema Antiplagio: **oid:** 27259:324033639

turnitin **Identificación de reporte de similitud**: oid:27259:324033639

NOMBRE DEL TRABAJO
Propuesta de un sistema de gestión de s eguridad de la información basado en la norma NTP ISO_IEC 270

AUTOR
Alcides Larota Cuito

RECUENTO DE PALABRAS
32461 Words

RECUENTO DE CARACTERES
187999 Characters

RECUENTO DE PÁGINAS
175 Pages

TAMAÑO DEL ARCHIVO
6.4MB

FECHA DE ENTREGA
Feb 4, 2024 9:06 PM GMT-5

FECHA DEL INFORME
Feb 4, 2024 9:09 PM GMT-5

7% de similitud general

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

- 6% Base de datos de Internet
- Base de datos de Crossref
- 3% Base de datos de trabajos entregados
- 0% Base de datos de publicaciones
- Base de datos de contenido publicado de Crossr

Excluir del Reporte de Similitud

- Material bibliográfico
- Material citado
- Bloques de texto excluidos manualmente
- Material citado
- Coincidencia baja (menos de 30 palabras)

Dedicatoria

El presente trabajo está dedicado a mi madre Genara Cuito Choqque y mi padre Cosme Larota Ilahuala a toda mi familia, a mis docentes de la Escuela profesional de Ing. Informática y de Sistemas y a Dios por haber sido mi apoyo en todo momento durante mi carrera universitaria y en el camino de mi vida. A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

Alcides Larota Cuito

Resumen

El propósito del presente proyecto es la protección de los activos de información de la Municipalidad Distrital de Chamaca, para lograr el desarrollo del proyecto se realizó un diagnóstico de seguridad de la información en los terminales tecnológicos y el personal que labora y maneja la información confidencial e importante de la Municipalidad distrital de Chamaca, que en la actualidad no cuenta con un sistema de gestión seguridad de información, con el cual se implementó normas estándares de seguridad de información para proteger los activos de información que eran manipulados de manera inadecuada por los trabajadores, para dar solución a esa problemática se desarrolló el siguiente trabajo de investigación. basados en las buenas prácticas de la norma técnica peruana NTP ISO/IEC 27001:2014. En el trayecto de este proyecto se realizó un diagnóstico de seguridad en las terminales tecnológicas y el personal que maneja la información utilizando la metodología del ciclo Deming (PDCA).

Se deja como propuesta los controles de seguridad de la información los cuales ayudan a fortalecer tres aspectos como son: “la confidencialidad, integridad, y la disponibilidad” de los activos de información de Software y Hardware”. Todo esto en las oficinas administrativas de la Municipalidad Distrital de Chamaca. Como es exigido por ley (RM N° 004-2016-PCM). y al oficio múltiple N° D000037-2020-PCM-SEGDI emitido a la Municipalidad Distrital de Chamaca en donde indica la obligatoriedad de la implementación de un Sistemas de Gestión de Seguridad de Información bajo los parámetros de la norma técnica peruana NTP ISO /IEC 27001:2014.

Palabras claves: Activos de información, Seguridad de la información, valoración de riesgos, proyecto de implementación, NTP Norma Técnica Peruana, ISO 27001, sistema de gestión de seguridad de la información SGSI.

Abstract

The purpose of this project is the protection of the information assets of the District Municipality of Chamaca, to achieve the development of the project, an information security diagnosis was made in the technological terminals and the personnel who work and manage confidential and of the District Municipality of Chamaca, which currently does not have an information security management system, with which standard information security regulations were implemented to protect information assets which were handled inappropriately by workers In order to solve this problem, the following research work was developed. based on the good practices of the Peruvian technical standard NTP ISO/IEC 27001:2014. In the course of this project, a security diagnosis was made in the technological terminals and the personnel that handles the information using the Deming cycle methodology (PDCA).

Information security controls were implemented which help to strengthen three aspects such as: "confidentiality, integrity, and availability" of Software and Hardware information assets. All this in the administrative offices of the District Municipality of Chamaca. As required by law (RM N° 004-2016-PCM). and to the multiple letter N° D000037-2020-PCM-SEGDI issued to the District Municipality of Chamaca where it indicates the obligatory nature of the implementation of an Information Security Management Systems under the parameters of the Peruvian technical standard NTP ISO / IEC 27001 :2014.

Keywords: Information assets, Information security, risk assessment, implementation project, NTP Peruvian Technical Standard, ISO 27001, ISMS information security management system.

ÍNDICE GENERAL

Índice de Anexos

Índice de figuras

Índice de tablas

Capítulo I

Aspectos Generales

CAPÍTULO I.

1 ASPECTOS GENERALES

1.1 PLANTEAMIENTO Y FORMULACIÓN DEL PROBLEMA

1.1.1 Descripción del problema

En el primer trimestre del 2020 en la Municipalidad Distrital de Chamaca tuvo una considerable perdida de información que ocasionaron grandes problemas con los documentos pertenecientes a las oficinas administrativas de la Municipalidad los que provocaron la mala manipulación de esos documentos por parte de usuarios, trayendo consigo sanciones administrativas a los trabajadores.

Se notó también que los equipos de cómputo con los que contaba la Municipalidad Distrital de Chamaca estaban con software sin licencia que eran instalados por trabajadores de la oficina de informática y algunos trabajadores que laboran en la Municipalidad, también no tienen instalado software de antivirus con licencia para detectar y eliminar amenazas de software malicioso.

Al momento de ejecución en la Municipalidad Distrital de Chamaca no contaban con los controles estándares de seguridad, medidas o procedimientos de seguridad necesarios para proteger sus activos de información tales como documentos, hardware, software, dispositivos físicos, personas, imagen, reputación y servicios que estaban expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes para proteger los activos de información más importantes que estaban almacenadas en los terminales tecnológicos como computadoras, laptops y celulares de la Municipalidad Distrital de Chamaca.

Esta Municipalidad Distrital de Chamaca, se encuentra estructurada de la siguiente manera: la oficina de logística conformado por el área de control institucional, abastecimiento y almacén cuya función principal realizar el control cotizaciones y requerimientos de los bienes o servicios los cuales sean necesarios para los usuarios de la Municipalidad Distrital de Chamaca según la normativa del Sistema abastecimiento.

Seguidamente se encuentra el área de Asesoría Jurídica, la cual se encarga de emitir opinión y asesorar acerca de asuntos de orden jurídico de competencia de la Municipalidad, también está el área de Presupuesto comprende las previsiones de ingresos y gastos que la Municipalidad tiene para un periodo anual, que les permite ejecutar obras de desarrollo local y brindar diversos servicios públicos, para garantizar los mayores beneficios sociales a la población como también el área de Contabilidad en la oficina quien se encargar de elaborar los registros y la información de las operaciones contables (balances, estados financieros, informes, reportes y otros), controlando y manteniéndolo actualizado, como también está la oficina de Tesorería quien se encarga de controlar la emisión, el endoso y el giro de cheques en representación de la Municipalidad, así como letras, pagarés, fianzas y cualquier otro que sea necesario para la gestión económica y financiera de la Municipalidad, se encuentra también la oficina de informática que es el órgano encargado de mantener un adecuado nivel de integración tecnológica de la municipalidad, así como de administrar, desarrollar y mantener tanto los recursos como los sistemas informáticos en la Municipalidad Distrital de Chamaca.

1.1.2 Identificación del problema

En la actualidad la Municipalidad Distrital de Chamaca no cuenta con los controles, medidas o procedimientos de seguridad necesarios para resguardar sus activos de información tales como documentos, software, dispositivos físicos, personas, imagen, reputación y servicios, están expuestos a altos niveles de riesgos, frente a las diversas amenazas físicas y lógicas existentes:

- Estructurales (Incendios, inundaciones, humedad, cortes de electricidad, agua, refrigeración, comunicaciones, etc.)
- Hardware (fallo total o parcial de Servidores, Estaciones PC, portátiles, etc.)
- Software (Errores en los SO, BD, software base, Web servers, aplicaciones, elementos de seguridad, etc.)
- Información (Bases de datos, ficheros manuales, procedimientos, planes de contingencia, etc.).
- Personal (Errores y ataques de personal interno, externo, funciones, perfiles, formación, etc.)

El presente trabajo de investigación se basa en una propuesta de un Sistema de Gestión de Seguridad de la Información para la protección de los activos de la información enfocadas en la aplicación de la NTP ISO/IEC 27001:2014 en la Municipalidad Distrital de Chamaca.

A continuación, se ve algunos de los problemas suscitados en la Municipalidad durante el desarrollo de las actividades laborares en la Municipalidad como se muestra en las fotografías.

Figura 1. ***Fotografía de una impresora en una mala ubicación en la oficina de la MDCH.***

Fuente: Elaboración propia

Figura 2. ***Manipulación inadecuada del cartucho de una impresora laser***

Fuente: Elaboración propia

Figura 3. ***Mantenimiento preventivo de impresora laser***

Fuente: Elaboración propia

1.2 Descripción de la entidad receptora de la propuesta del SGSI

1.2.1 Nombre o razón social

La Municipalidad Distrital de Chamaca ubicado en el departamento de Cusco, Provincia de Chumbivilcas y distrito de Chamaca.

1.2.2 Rubro

Administración pública en general.

1.2.3 Municipalidad Distrital de Chamaca

El distrito peruano de Chamaca es uno de los ocho distritos de la Provincia de Chumbivilcas, ubicada en el Departamento de Cusco, bajo la administración el Gobierno regional del Cuzco. El Papa Juan XXIII segregó de la Arquidiócesis del Cusco, las Provincias civiles de Canchis, Canas, Espinar y Chumbivilcas y con ellas creó la Prelatura de Sicuani, haciéndola sufragánea del Cusco, mediante la Constitución Apostólica

Dirección: Calle Concepción s/n Chamaca Chumbivilcas-Cusco

- **HISTORIA:**

El distrito fue creado mediante Ley del 2 de enero de 1855, dado en el gobierno del presidente Ramón Castilla.

- **COMUNIDADES CAMPESINAS:**

Cuenta con 10 comunidades: Cconchaccollo, Sihuincha, Tintaya, Tincurca, Ccacho Limamayo, Cangalle, Quellomarca, Ingata, Añahuichi y Uchucarco

- **POBLACIÓN TOTAL (INEI 2017):**

Total: 7698 habitantes, densidad: 11.42 habitantes/ km²

1.2.4 Ubicación Geográfica

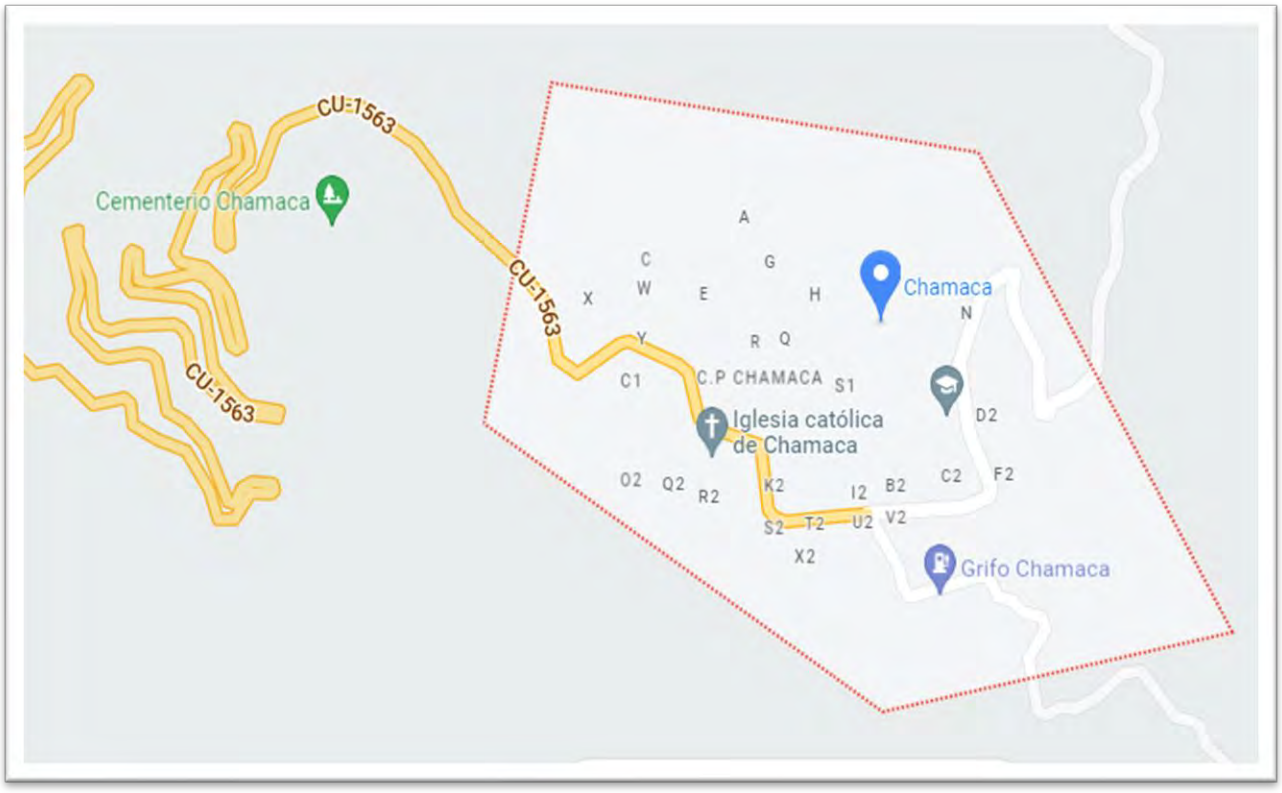
GEOGRAFÍA:

Está ubicado en 3 739 msnm.

Distrito de Chamaca tiene 674.19km² de área total de superficie terrestre

M4XX+237, Chamaca 08461

Figura 4. Mapa de ubicación del Distrito de Chamaca, Chumbivilcas, Cusco



Fuente: Elaboración propia

Figura 5. Ubicación de la Municipalidad Distrital de Chamaca

Fuente: Elaboración propia

1.2.5 Misión

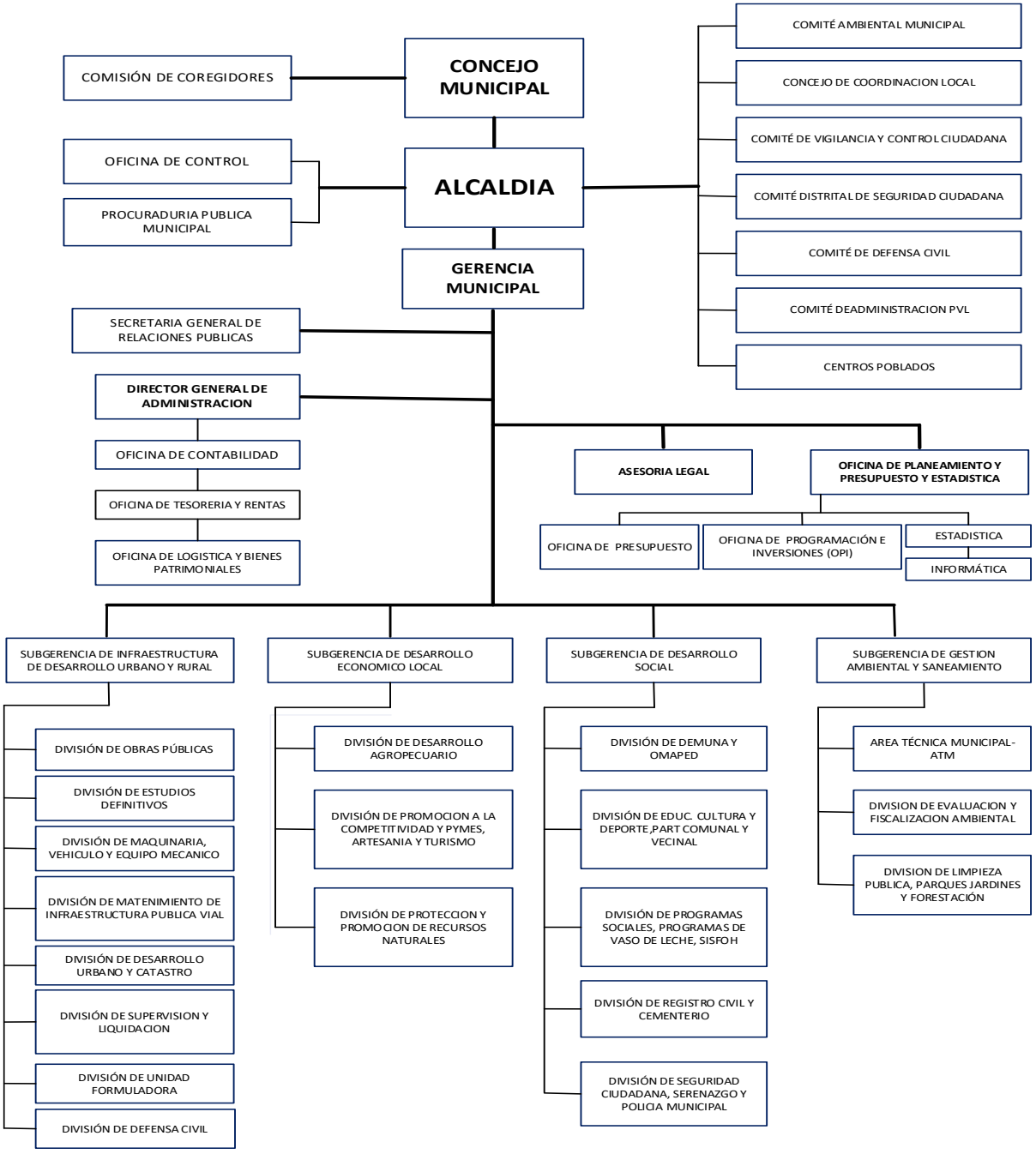
Brindar servicios de calidad con eficiencia y eficacia manteniendo una gestión transparente y responsable que garantice el manejo óptimo de los recursos públicos, promoviendo así el bienestar y desarrollo integral y sostenible de su población de manera participativa e inclusiva.

1.2.6 Visión

Constituirnos como la municipalidad líder en la región y ser reconocidos por la mejora constante en nuestra labor proactiva y eficiente ofrecida por nuestros trabajadores altamente calificados a favor del bienestar de nuestra población.

1.2.7 Organigrama

Figura 6. Organigrama de la Municipalidad Distrital de Chamaca



Fuente: Elaboración Propia

1.2.8 Objetivos estratégicos de la MDCH.

1) Desarrollar una economía competitiva de transformación productiva y agropecuaria.
2) Generar oportunidad de desarrollo local sostenible.
3) Formular el plan de acondicionamiento territorial y el plan de desarrollo urbano.
4) Conservación y aprovechamiento de los recursos naturales y la biodiversidad.
5) Fortalecer el sistema de impacto ambiental respecto a la minería
6) Promover el desarrollo de capacidades humanas y bienestar de las personas.
7) Brindar los servicios básicos de calidad, mejorar el ambiente y la calidad de vida de las personas.
8) Modernizar la administración municipal y mejorar la calidad de los servicios.

1.3 Formulación del problema.

1.3.1 Problema general

¿Existe riesgo de pérdida de activos de información en la Municipalidad Distrital de Chamaca?

1.3.2 Problemas específicos

- ¿Cuál es el alcance de las políticas del Sistema de Gestión de la seguridad de la información para la Municipalidad Distrital de Chamaca?
- ¿Qué metodología se usará para la gestión de los riesgos de los activos de información en la Municipalidad Distrital de Chamaca?
- ¿Cómo evaluar los controles y mecanismos de seguridad de información en la Municipalidad Distrital de Chamaca?

1.4 Objetivos de la investigación

1.4.1 Objetivo general

Desarrollar una propuesta de un Sistema de Gestión de Seguridad de la Información basado en la norma técnica peruana NTP ISO/IEC 27001:2014, para proteger los activos de información de la Municipalidad Distrital de Chamaca, Chumbivilcas, Cusco.

1.4.2 Objetivos específicos

- Desarrollar alcances de políticas de seguridad de información, para proteger los activos de información bajo la NTP ISO/IEC 27001:2014 en la Municipalidad Distrital de Chamaca.
- Identificar los riesgos de seguridad de información de las principales terminales tecnológicas aplicando la fase de planificación de la metodología del ciclo Deming (PDCA).
- Establecer controles de seguridad de información con la NTP/ISO/IEC 27001:2014 en la Municipalidad Distrital de Chamaca.

1.5 Justificación

1.5.1 Conveniencia

La elaboración de esta propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Municipalidad Distrital de Chamaca es altamente conveniente por varias razones:

- **Protección de la información sensible:** La Municipalidad maneja una gran cantidad de información sensible, como datos personales de los ciudadanos, información financiera y registros legales.

- **Cumplimiento normativo:** La implementación de un SGSI puede ayudar a la municipalidad a cumplir con regulaciones y leyes relacionadas con la seguridad de la información.
- **Prevención de incidentes de seguridad:** Un SGSI establece medidas preventivas y correctivas para minimizar el riesgo de incidentes de seguridad, como ataques cibernéticos, pérdida de datos o mal uso de la información.
- La elaboración de una propuesta para implementar un SGSI en la Municipalidad puede ser crucial para garantizar la seguridad y protección de activos de información, cumplir con las regulaciones, fortalecer la confianza ciudadana y mejorar la eficiencia operativa.

1.5.2 Relevancia

La elaboración de una propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) en una Municipalidad Distrital de Chamaca es de gran relevancia por diversas razones, ya que aborda la necesidad de proteger los activos de información sensible y asegurar la continuidad operativa en un entorno Municipal. Aquí hay algunas razones específicas que destacan la relevancia de esta propuesta. Protección de Datos Sensibles

a) Cumplimiento Normativo

b) Confianza Ciudadana

c) Prevención de Riesgos

d) Garantía de Continuidad Operativa

e) Optimización de Recursos

f) Gestión de Incidentes

1.5.3 Implicancias practicas

1.5.4 Valor teórico

Al proponer un SGSI, es probable que adaptes y apliques marcos de referencia reconocidos, como ISO 27001. Este proceso de adaptación y contextualización puede ser un aporte valioso al mundo científico, mostrando cómo las mejores prácticas pueden implementarse en entornos específicos como el gubernamental.

La implementación de un SGSI implica desarrollar una cultura de seguridad en el entorno gubernamental. Investigar y proponer estrategias para fomentar esta cultura puede ser de interés científico, especialmente en el contexto del sector público.

El propósito del desarrollar esta propuesta de un sistema de gestión de seguridad de información, es la de reducir riesgos que afectan a los activos de información que se encuentran en las terminales tecnológicas que son administrados por los trabajadores y usuarios de la Municipalidad distrital de Chamaca bajo la norma técnica peruana ISO 27001:2014.

En el caso de una Municipalidad los activos de información más críticos serian: los servicios, información relativa a los productos, proveedores, personal, método de trabajo, organización, estrategias empresariales, información económica y financiera, etc.

La presente investigación busca mediante la aplicación de la ISO/IEC 27001:2014, elaborar una propuesta de un sistema gestión de seguridad de información que permita una buena gestión y salvaguardar la integridad, confidencialidad y disponibilidad de los activos de información en la Municipalidad Distrital de Chamaca.

1.6 Alcances y limitaciones.

1.6.1 Alcances

El alcance del plan de tesis estará limitado por el oficio múltiple Nro D00037-2020-PCM-SEGDI y las recomendaciones dadas a todas las municipalidades Distritales y Provinciales de parte de la secretaria del Gobierno Digital para la elaboración de un sistema Gestión de Seguridad de Información emitido el oficio a la Municipalidad Distrital de Chamaca de parte de la Presidencia del Consejo de Ministros – PCM.

Para el desarrollo de esta propuesta de sistema de gestión de seguridad de información está basada en el oficio múltiple emitido a la municipalidad que indica la “Vigilancia y Acompañamiento al Cumplimiento de la Implementación del Sistema de Gestión de Seguridad de la Información en el marco del Resolución Ministerial Nº 004-2016-PCM” , En virtud de ello, y con la urgencia que nos exige la emergencia nacional a causa de la pandemia del COVID19, la Secretaría de Gobierno Digital viene desplegando las acciones correspondientes a la vigilancia y acompañamiento al cumplimiento de la regulación vigente en materia digital a fin de acelerar el logro de los objetivos de transformación digital del país Apruébese el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. en todas las entidades integrantes del Sistema Nacional de Informática. (Oficio Multiple D00037-PCM, 2020) (anexo 3).

1.6.2 Limitaciones

Para el proyecto a desarrollar se encontraron las siguientes limitaciones para el cual se aplicará la fase de Planificar del ciclo Deming en cual consisten en:

a. Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
b. Definir una política de seguridad que:
    - Incluya el marco general y los objetivos de seguridad de la información de la organización
c. Identificar los riesgos:
    - Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios
    - Identificar las amenazas en relación a los activos
    - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas
    - Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
    - Analizar y evaluar los riesgos:
d. Limitaciones establecidas por el oficio múltiple Nro D00037-2020-PCM-SEGDI. Que establece al cumplimiento y la regulación vigente en materia digital a fin de acelerar el logro de los objetivos de transformación digital del país y el cumplimiento de la resolución Ministerial N° 004-2016-PCM, En donde indica el uso obligatorio de la NTP ISO/IEC 27001:2014, Sistemas de Gestión de Seguridad de Información.

1.7 Metodología

1.7.1 Metodología de desarrollo de tesis.

1.7.1.1 Alcances

En el desarrollo de este proyecto de tesis se utilizó la metodología de investigación Descriptiva, mencionada por Roberto Hernández Sampieri, Carlos Fernández Collado y Pilar Bautista Lucio, el cual consiste en describir fenómenos, situaciones, contextos y sucesos que busca especificar las propiedades, las características y los perfiles de personas, grupos comunidades, procesos objetos, o cualquier otro fenómeno que se someta a un análisis por tanto, la presente investigación es Descriptiva porque busca identificar y describir las características fundamentales de la implementación del Sistema de Gestión de Seguridad de Información (teniendo como guía la NTP ISO/IEC 27001:2014) para su aplicación en la Municipalidad Distrital de Chamaca.

Una propuesta de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Municipalidad Distrital de Chamaca que sigue la norma técnica peruana (NTP) ISP 27001:2014 se consideraría descriptiva principalmente porque su objetivo es describir cómo se llevará a cabo la implementación del sistema. Aquí hay algunas razones para considerarla una metodología descriptiva:

a) **Detalle de procesos y procedimientos:** Una propuesta descriptiva detallará los procesos y procedimientos específicos que se seguirán para establecer y mantener el SGSI. Esto puede incluir la identificación de activos, la evaluación de riesgos, la implementación de controles, la formación del personal, entre otros.

b) **Descripción de controles y medidas de seguridad:** La propuesta describirá en detalle los controles y las medidas de seguridad que se implementarán para proteger la información. Esto puede incluir aspectos como el control de acceso, la gestión de incidentes, la protección contra malware, entre otros.

c) **Identificación de activos críticos:** Una parte importante de la propuesta descriptiva es la identificación de los activos críticos de información. Esto implica describir qué datos son esenciales para la municipalidad y, por lo tanto, deben ser protegidos de manera más rigurosa.

d) **Documentación de políticas y procedimientos:** La metodología descriptiva se centra en la documentación detallada. La propuesta describirá las políticas de seguridad de la información y los procedimientos operativos que la municipalidad seguirá para garantizar la seguridad.

e) **Mapeo de roles y responsabilidades:** La propuesta describirá claramente los roles y responsabilidades de las personas involucradas en el SGSI, desde el personal de nivel operativo hasta los responsables de la alta dirección.

f) **Especificación de indicadores de desempeño:** La propuesta puede incluir la especificación de indicadores clave de desempeño que se utilizarán para evaluar la efectividad del SGSI. Esto implica describir cómo se medirá el éxito y la mejora continua.

g) **Planificación de auditorías y revisiones:** Se describirá cómo se llevarán a cabo las auditorías internas y las revisiones del SGSI. Esto incluirá la frecuencia, los criterios de auditoría y el proceso para abordar las no conformidades.

h) **Enfoque iterativo del ciclo PDCA:** Si la propuesta sigue el ciclo PDCA (Planificar, Hacer, Verificar, Actuar), se describirán detalladamente las etapas de este ciclo y cómo se llevará a cabo la mejora continua.

1.7.1.2 Diseño

Explicar cómo se llevará a cabo la propuesta de implementación del SGSI en términos metodológicos.

Este diseño metodológico busca proporcionar una visión completa y detallada de la propuesta de SGSI en la Municipalidad Distrital de Chamaca, abordando describir las etapas, los métodos de recopilación de datos, las técnicas de análisis y las herramientas a utilizar. los aspectos clave según la metodología descriptiva de Sampieri.

a) **Identificación y descripción de procesos:** Describir los procesos específicos que se llevarán a cabo para implementar el SGSI. Esto incluye la identificación de activos de información, la evaluación de riesgos, la selección de controles y la gestión de incidentes.

b) **Recopilación de datos:** Detallar cómo se recopilarán los datos necesarios para la implementación del SGSI. Esto puede incluir entrevistas, revisión de documentos, análisis de sistemas, entre otros.

c) **Análisis de datos descriptivos:** Utilizar técnicas de análisis descriptivo para comprender el estado actual de la seguridad de la información. Esto puede incluir estadísticas descriptivas, gráficos, y tablas para representar la información.

d) **Formulación de estrategias de implementación:** Describir las estrategias específicas que se utilizarán para implementar el SGSI, basadas en los resultados del análisis descriptivo.

e) **Desarrollo de políticas y procedimientos:** Detallar el proceso de desarrollo de políticas y procedimientos de seguridad de la información, asegurando que sean específicos y aplicables al contexto municipal.

f) **Validación y confiabilidad:** Describir cómo se garantizará la validez y confiabilidad de los datos recopilados y del proceso de implementación del SGSI.

g) **Presentación de resultados y conclusiones:** Presentar los resultados obtenidos mediante descripciones detalladas. Concluir con base en la información recopilada y analizada.

h) **Recomendaciones y mejora continua:** Formular recomendaciones basadas en los hallazgos y proponer estrategias para la mejora continua del SGSI en la municipalidad.

1.7.2 Metodología de desarrollo del proyecto

William Edwards Deming, aplico el método científico y continuo el desarrollo del trabajo, esta rueda de Deming, en donde las organizaciones deben configurar planes de gestión y mejora continua con los que consigan mejorar su competitividad y calidad de sus procesos, reduciendo costes y fallos, optimizando la productividad y eliminando riesgos.

El ciclo Deming es el sistema más utilizado para implantar dicho plan de mejora continua. recibe el nombre de Edwards Deming, quien fue su principal impulsor, pero también se conoce

como ciclo PHVA que son las siglas de Planificar, Hacer, Verificar y Actuar, o PDCA en inglés (Plan, Do, Check, Act).

Figura 7. Metodología del ciclo Deming

Fuente: https://www.herramientaslean.com/wp-content/uploads/2022/12/Ciclo-de-Deming-o-PDCA.png

El ciclo de Deming conocido como "PDCA – Plan, Do, Check, Act"

1) **Planificar (Plan):**
   a) **Identificación de activos:** Identifica y clasifica los activos de información críticos para la Municipalidad Distrital de Chamaca.
   b) **Evaluación de riesgos:** Realiza una evaluación de riesgos para identificar las amenazas y vulnerabilidades asociadas a los activos de información.
   c) **Establecimiento de objetivos**: Define objetivos específicos de seguridad de la información basados en la evaluación de riesgos.

d) **Desarrollo de políticas y procedimientos:** Elabora políticas y procedimientos de seguridad basados en los objetivos establecidos y los requisitos de la norma NTP ISP 27001:2014.

2) **Hacer (Do):**

a) **Implementación de controles:** Implementa controles de seguridad de acuerdo con las políticas y procedimientos definidos.

a) **Formación y concienciación:** Proporciona formación y concienciación sobre seguridad de la información para el personal.

a) **Desarrollo de documentación:** Desarrolla la documentación necesaria, incluyendo registros, para respaldar la implementación de los controles.

3) **Verificar (Check):**

a) **Auditorías internas:** Realiza auditorías internas periódicas para evaluar la efectividad de los controles implementados.

b) **Monitorización y medición:** Establece indicadores clave de desempeño y medir el rendimiento del SGSI.

c) **Revisión de resultados:** Revisa regularmente los resultados de las auditorías internas y de las métricas para identificar áreas de mejora.

4) **Actuar (Act):**

a) **Acciones correctivas:** Toma acciones correctivas para abordar las no conformidades identificadas durante las auditorías internas.

a) **Mejora continua:** Busca oportunidades de mejora continua en el SGSI. Actualiza políticas y procedimientos según sea necesario.

b) **Adaptación a cambios:** Ajusta el SGSI en respuesta a cambios en el entorno, en las amenazas y en los activos de información.

Ciclo Continuo:

a) **Reinicia el ciclo:** Inicia nuevamente el ciclo PDCA, aplicando aprendizajes y mejoras acumuladas en cada iteración.

Al aplicar este enfoque cíclico a la Municipalidad Distrital de Chamaca puede asegurarse que su SGSI evolucione de manera continua para enfrentar nuevos desafíos y mantenerse alineado con los objetivos de seguridad de la información y la norma NTP ISP 27001:2014. Es importante involucrar a todas las partes interesadas relevantes y fomentar una cultura de mejora continua en todo el proceso.

Capítulo II
Marco teórico

CAPÍTULO II.

2 MARCO TEÓRICO.

2.1 Antecedentes de la investigación

2.1.1 Antecedentes internacionales

Según (Borrero Ochoa, 2019) en su trabajo de grado denominado: "**Identificación de Activos de Información, Riesgos y controles asociados para la Empresa Estrategias Empresariales de Colombia bajo la Norma ISO 27001 e ISO 31000"**.

Universidad nacional abierta y a distancia UNAD escuela de ciencias básicas, tecnología e ingeniería especialización en seguridad informática Cali - Colombia 2019.Menciona lo siguiente.

Resumen

Según indica el autor cada uno de los activos presenta características específicas que requieren protección y monitoreo particular, ya sea por el tipo de información que contienen, el estado en el que se conservan o importancia relativa para la función y desarrollo de la empresa. Así mismo, logró identificar, documentar y validar la responsabilidad del personal que tiene acceso a los activos, los roles que juegan en torno a su seguridad, de manera que se garantizará las propiedades de disponibilidad (accesible en todo momento con autorización), integridad (exactitud en la información), confidencialidad (restricción especifica), autenticidad (sin alteración) y trazabilidad (registro de acceso y gestión) de la información de la empresa.

El cuantificar estas variables, permitirá determinar el valor que posee cada activo y la gestión a realizar sobre cada uno. Para el desarrollo del trabajo, se utilizó como guía la Norma

ISO 27001:2013 sistema de seguridad de la información y la ISO 31000:2018 para la gestión de riesgos y controles.

Conclusiones.

1. La gestión de la seguridad de la información, es un gran reto para las empresas, por las implicaciones que tiene sobre los recursos físicos, financieros y humanos. La inversión que se deba realizar Estrategias Empresariales para el control de los activos de información, debe verse como algo que redunda en beneficio para la empresa de cara a la seguridad interna y a la imagen corporativa ante sus clientes y partes interesadas.
2. Se logró determinar los controles más apropiados que permiten salvaguardar de manera más específica, la integridad, disponibilidad y confidencialidad en cada activo utilizado para la gestión de la información, haciendo participes a los responsables de la misma, de manera que, al involucrarlos de manera activa al proyecto, se apropiaron del mismo y ahora son conscientes acerca de la importancia que representa para la empresa el velar de manera adecuada por la seguridad de los activos de información.

Interpretación

- La presente investigación aporta a mi proyecto en los procesos operativos de sus activos de información que estableció una metodología, donde se tienen en cuenta criterios como: valor para el riesgo, valor para los activos, tipo, criticidad y clasificación de cada activo de

información, de esta manera, se incluyen aspectos relevantes que apoyados en la ISO 27001:2013 e ISO 31000:2018 constituyen en un método de reconocido valor para la organización.

Según el proyecto desarrollo por: Rodriguez y Torres (2019) en su proyecto de trabajo de grado denominado: "**Análisis de riesgos de Seguridad de la Información del Área IT de la Empresa Royal Services S.A.**"

Facultad de Ingeniería/Programa de especialización en seguridad de la información/ Universidad Católica de Colombia.

Resumen

Indica que su proyecto se relacionaba con la línea de investigación: Gestión Integral y dinámica de las Organizaciones Empresariales del grupo GEGI (Gestión Empresarial & Gestión de Innovación) de la Universidad Católica de Colombia, ya que fue encaminado a la mitigación de riesgos informáticos con la utilización de mejores prácticas, técnicas, herramientas, metodologías o modelos de gestión, para la solución de la problemática existente sobre seguridad de la información en la empresa Royal Services S.A. ubicada en Bogotá.

El proyecto que fue desarrollado se relacionó con la línea de investigación: Gestión Integral y dinámica de las Organizaciones Empresariales del grupo GEGI (Gestión Empresarial & Gestión de Innovación) de la Universidad Católica de Colombia, ya que estaba encaminado a la mitigación de riesgos informáticos con la utilización de mejores prácticas, técnicas,

herramientas, metodologías o modelos de gestión, para la solución de la problemática existente sobre seguridad de la información en la empresa Royal Services S.A., ubicada en Bogotá.

Conclusiones

1. En el presente trabajo describió todos los conceptos e importancia de la gestión de riesgos presentes en la seguridad de la información la cual se administra a través de los diversos equipos, servicios y colaboradores del área de TI; además se utilizaron metodologías que facilitaron y desarrollo del análisis de riesgo en las organizaciones y más específicamente en la Empresa que realizamos el análisis Royal Services S.A. Magerit, Dafp, ISO 27001, Octave y ISO 31000 Fueron las metodologías que les guiaron en el caso de estudio realizado, para conocer las múltiples amenazas a las cuales están expuestos los activos que hacen parte de Royal Services S.A.
2. Análisis de riesgos que permitió conocer su estado y niveles de seguridad de la organización para posteriormente emitir y realizar unas recomendaciones y controles que permitan reducir los riesgos de seguridad de información.

Interpretación

- La presente investigación aporta a mi proyecto con el análisis de una gestión efectiva de riesgos en seguridad de la información, respaldada por metodologías reconocidas, para fortalecer la postura de seguridad de una organización como Royal Services S.A. y proteger sus activos ante las complejidades y amenazas presentes en el entorno actual de la tecnología de la información.

En el proyecto de tesis elaborado por (Arlenys Carolina, 2017), Desarrolló: "**Un Sistema de Gestión de la Seguridad de la Información (SGSI) basados en la norma ISO/IEC 27001:2013",**

Facultad de Ingeniería y Ciencias Básicas Especialización en Seguridad De La Información 2017 / Institución Universitaria Politécnico Grancolombiano – Colombia.

Resumen

Realizó una valoración y tratamiento de riesgos de Seguridad de la Información a los Activos de información y realizó un cronograma de capacitaciones en seguridad de la información que permitió evaluar la integridad, confidencialidad y disponibilidad de los activos (Hardware - Software) de información a las oficinas de Ingreso de Centros de Educación Técnica. En donde mencionó que la seguridad de la información surge como una medida de asegurar que la información tenga los niveles adecuados de protección en cuanto a Confidencialidad, Integridad y Disponibilidad.

El trabajo consistía en el diseño de SGSI de la oficina de Ingreso del Centro de Educación Técnica y Tecnológica del departamento del Cesar, todo lo anterior, se desarrolla dentro del marco conceptual y metodológico de un sistema de gestión de seguridad de información bajo la norma ISO 27001:2013

Conclusiones

1. La seguridad de la información es una responsabilidad de todos en una entidad que debe estar guiada por manuales y/o procedimientos de buen uso de los activos de información.
2. La valoración de los riesgos de los activos de información del Centro de Educación Técnica y Tecnológica del departamento del Cesar, permitió identificar que el desconocimiento del tema que pone en riesgo los procesos que se desarrollan en cuanto a

disponibilidad, integridad y confidencialidad y la seguridad de la información es responsabilidad de todos en una entidad que debe estar guiada por manuales y/o procedimientos de buen uso de los activos de información.

3. El diseño del Sistema de Gestión de Seguridad de la Información (SGSI), permitió identificar amenazas y vulnerabilidades de los activos de información, para posteriormente elaborar plan de tratamientos con la finalidad de mitigar los riesgos
4. Se concluyó con un plan de capacitación y sensibilización sobre seguridad de la información, permitirá crear ambientes de buen manejo y uso de los activos de información.

Interpretación

La presente investigación aporta a mi proyecto en establecer un marco de gestión de seguridad de la información conforme a la norma ISO 27001:2013, identificando riesgos, diseñando soluciones y proponiendo medidas de capacitación para mejorar la seguridad en la entidad educativa.

Según el trabajo desarrollado por (Pedraza Rodriguez, 2017), en su proyecto denominado: "**Plan de Implementación de un Sistema de Gestión de Seguridad de la Información en una Entidad del Sector Público basado en la NTC ISO 27001:2013"**.

Fundación Universidad De América/ Facultad De Educación Permanente y Avanzada Especialización En Gerencia De La Calidad, Bogotá, Colombia 2017.

Resumen

La connotación de seguridad se ha ido ampliando con el tiempo gracias a la inmersión de nuevos sistemas tecnológicos de información. Así mismo, los instrumentos para garantizar el

resguardo, la confidencialidad y el tratamiento de la información, se han convertido en estrategias fundamentales para la garantía de la seguridad de las organizaciones públicas y privadas. La elaboración de este plan comprende el análisis del estado actual de la organización y la evaluación de sus riesgos, así como la implementación del modelo Planear, Hacer, Verificar y Actuar (PHVA), con características procedimentales que apoyan de principio a fin todo el proceso de implantación y facilitan el debido proceso y la continuidad.

El resultado de ese diseño será un plan con cronograma de actividades, para que la organización vincule a todo el personal en torno al cumplimiento de la norma, la sensibilización con respecto a la importancia de la seguridad de la información y el desarrollo de actividades por fases que en los tiempos estipulados lograrán tener en pleno funcionamiento el SGSI.

Palabras clave: implementación, seguridad, información, riesgo, análisis, PHVA.

Conclusiones

1. El diseño del Plan de Implementación de un Sistema de Gestión de Seguridad de la Información apoyado en los lineamientos de seguridad que dicta la norma ISO/IEC 27001:2013, se considera una herramienta de gran ayuda para identificar los aspectos a tener en cuenta en el momento en el que las organizaciones toman la decisión de establecer un modelo de seguridad de la información en la organización podrá lograr la sostenibilidad del Sistema de Gestión de Seguridad de la Información.
2. El plan para la implementación de un Sistema de Gestión de Seguridad de la Información en una empresa del sector público basado en los requisitos de la norma NTC ISO 27001:2013 es un proceso dinámico que debe contemplar el análisis del contexto organizacional, además de evaluar los riesgos de la seguridad de la información en dicha empresa. En este proceso, el análisis e identificación de riesgos permitió conocer a

profundidad cuáles eran los niveles de vulnerabilidad más altos de la entidad en estudio y así se logró hallar la forma de mitigarlos.

3. La implementación del SGSI se considera beneficiosa para la entidad, ya que genera mayor seguridad en los sistemas de información y contribuye a obtener una mejora continua en cada proceso de auditoría interna, todo lo cual aumenta la confianza y mejora de imagen corporativa.
4. Este trabajo ya cuenta con un avance significativo: el análisis de la entidad, el diseño del Plan de Implementación y el cronograma de actividades. Ahora es fundamental el compromiso de la alta dirección, las áreas que tienen que ver directamente con la producción, uso y administración de la información, así como de los diferentes grupos de interés, para ejecutar en los tiempos señalados cada una de las fases

Interpretación

La presente investigación indica que los mecanismos para asegurar la protección, confidencialidad y tratamiento adecuado de la información se han vuelto fundamentales en la seguridad de las organizaciones tanto públicas como privadas. El plan de implementación aborda el análisis del estado actual de la organización, la evaluación de riesgos y la aplicación del modelo Planear, Hacer, Verificar y Actuar (PHVA), que proporciona un enfoque procedimental integral para facilitar la implantación y garantizar la continuidad del proceso.

2.1.2 Antecedentes nacionales

Según (Sandoval Alania, 2020). Desarrolló el proyecto denominado: "**Propuesta de Diseño de un Sistema de Gestión de Seguridad de la Información basado en la NTP-**

ISO/IEC 27001, para la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco".

Escuela Profesional De Ingeniería De Sistemas/Universidad Nacional Hermilio Valdizan Huánuco 2020.

Resumen

La organización no contempló entre sus procesos mecánicas, medidas o políticas que le ayuden a proteger sus activos de las amenazas y riesgos a los que están expuestos. Para el desarrollo del Sistema de Gestión de Seguridad de la Información, hizo uso de la Norma Técnica Peruana NTP – ISO/IEC 27001:2014 y la metodología MAGERIT en su versión 3 (v3) para el análisis y gestión de riesgos de los activos, partiendo desde la evaluación del estado inicial de la organización referente a la seguridad de la información para posteriormente empezar a planificar y diseñar el Sistema de Gestión de Seguridad de la Información, la aceptación que tendría este en la organización, definir sus alcance, sus políticas y su comité de seguridad para luego pasar al análisis y gestión de riesgos donde se determinó las amenazas y vulnerabilidades a las que están expuestos los activos de información. Una vez obtenido los resultados del análisis se realizó el tratamiento de riesgos para posteriormente elaborar los controles de seguridad y el diseño de la declaración de aplicabilidad de acuerdo al lineamiento de la Norma Técnica Peruana NTP – ISO/IEC 27001:2014.

Conclusiones

1. Se concluyó en primer lugar que, según la aplicación de los requisitos 4 (Contexto de la Organización) y 5 (Liderazgo) de la NTP – ISO/IEC 27001:2014, la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco se encontraba en un nivel básico de la

aplicación de la norma (no diseñado) con un 30% del cumplimiento de los requisitos de la NTP – ISO/IEC 27001:2014 y en una situación actual en la cual la organización comprendía la importancia y los beneficios que tiene un SGSI y posee el liderazgo para poder realizarlo, pero no se había establecido estrategias o metodologías para la evaluación de los riesgos informáticos y su tratamiento, al igual que ninguna documentación requerida por la NTP – ISO/IEC 27001:2014.

2. En segundo lugar, se concluyó que la elaboración de la documentación exigida por la NTP – ISO/IEC 27001, permitió comprender a la organización y su contexto tanto interno como externo, identificar las necesidades y expectativas de sus partes interesadas, formar el comité de seguridad de la información, establecer las políticas de seguridad de información y determinar el alcance que tendrá el Sistema de Gestión de Seguridad de la Información y los objetivos de este antes de realizar el diseño. Todo esto ayudó a tener una visión enriquecida de la organización y establecer las bases diseño del Sistema de Gestión de Seguridad de la Información para la organización.
3. Finalmente se concluyó que, el desarrollo del plan de tratamiento de riesgos ayudó a la organización a establecer los controles y acciones para mitigar los riesgos de las amenazas identificadas en los activos anteriormente, y junto a este se realizó el desarrollo de la declaración de aplicabilidad que permitió llevar el registro de los controles de seguridad que fueron aplicables y si estos se encuentran operando o todavía no.

Interpretación

La presente investigación concluye que la Dirección Regional de Trabajo y Promoción del Empleo – Huánuco se encontraba en un nivel básico de implementación de la norma, la

elaboración de la documentación requerida y el desarrollo del plan de tratamiento de riesgos fueron pasos significativos para mejorar la postura de seguridad de la información en la organización. Estos procesos sentaron las bases para el diseño y la implementación efectiva de un Sistema de Gestión de Seguridad de la Información en el futuro.

Según (Huaman Ancco, 2018) desarrollo su proyecto de tesis denominado: **"Modelo de Gestión de Seguridad de la Información con ISO/IEC 27001 Para Minimizar la Vulnerabilidad de la Información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2018".**

Escuela Profesional de Ingeniería de Sistemas/ Universidad Nacional José María Arguedas, Apurímac. 2018

Resumen

En su investigación como objetivo principal fue la minimización de la vulnerabilidad de la información a la que estaba expuesta la Municipalidad Distrital de Santa María de Chicmo (MDSMC) por falta de aplicación de los controles de la seguridad de la información basadas en las buenas prácticas de la norma ISO/IEC 27001. Para cumplir los objetivos planteados se realizó diagnóstico de la seguridad de la información en los terminales tecnológicos y personal que maneja la información a través de preguntas referidas al tema, luego se implementó todos los controles seleccionados a través de capacitación al personal y trabajos en terminales informáticos para garantizar buen manejo de información importante que todo trabajador almacena en su terminal y así evitar que esté en peligro toda información vital ya sea físicos o lógicos.

Su trabajo realizado fue de tipo cuantitativo ya que se hizo una encuesta para conocer la conciencia de la necesidad de seguridad de información por el personal que trabajan en las

diferentes áreas con respecto a seguridad de la información. Los datos recolectados los analizó con el software spss v24 y los resultados obtenidos dan a conocer que la minimización de la vulnerabilidad de la información en la institución fue satisfactoria y fue necesario también implementar controles de seguridad de la información lo cual ayudó a fortalecer tres aspectos importantes, la confidencialidad, integridad y la disponibilidad de la información.

Palabras claves: Seguridad de la Información, ISO/IEC 27001, minimización de vulnerabilidad.

Conclusiones

1. Para su conclusión de su proyecto se aplicó la prueba estadística T-Student y con los resultados estadísticos, se llegó a comprobar que la implementación de Modelo de Gestión de la Seguridad de la Información con ISO/IEC 27001, da como resultado una variación positiva en la minimización la vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo. Por lo tanto, se concluyó que hay una minimización de la vulnerabilidad de la información de manera significativa, ya que se determinó una variación positiva de 56,04% con respecto a la minimización de la vulnerabilidad de la información.
2. Con respecto a los trabajos realizados, con la implantación de MGSI para la minimización de la divulgación de la información en su objeto de estudio, determinó una variación positiva de 62,07%, lo cual nos indica que la divulgación de la información minimizó significativamente.
3. Se concluyó con la minimización de la alteración de la información con la implementación del MGSI se obtuvo un resultado significativo positivo de 53,03%, lo cual nos indica que la alteración de la información minimizó significativamente.

4. Por último, se concluyó, en la minimización de las amenazas de la información también se obtuvo una variación positiva de 53,12%, lo cual nos indica que la aplicación del MGSI para la minimización de las amenazas de la información es importante.

Interpretación

La presente investigación concluye con el respaldo de la efectividad de la implementación del MGSI basado en ISO/IEC 27001 en la Municipalidad Distrital de Santa María de Chicmo, mostrando mejoras significativas en la minimización de la vulnerabilidad, divulgación no autorizada, alteración y amenazas de la información. Estos resultados sugieren que el modelo ha contribuido de manera positiva a fortalecer la seguridad de la información en la minimización de la alteración de la información con la implementación del MGSI obtuvo un resultado significativo positivo de 53,03%, lo cual indicaba que la alteración de la información minimizó significativamente.

Según (Cosios Avila, 2020) desarrolló su proyecto denominado: **"Implementación de Auditoría Informática con la ISO 27001, en la Municipalidad Distrital de Suyo-Piura; 2020".**

Escuela Profesional De Ingeniería De Sistemas/ Universidad Católica Los Ángeles dse Chimbote Piura, Perú 2020.

Resumen

El proyecto fue desarrollado bajo la línea de investigación desarrollo de modelos y aplicación de las tecnologías de información y comunicaciones para la mejora continua de calidad de las organizaciones del Perú de la escuela profesional de Ingeniería de Sistemas, El tipo de investigación fue no experimental, descriptiva y de corte transversal, teniendo como objetivo

general Implementar una Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura.

Realizó la mejora del sistema de información con una muestra de 40 miembros los resultados obtenidos en el primer nivel de conocimiento de la información de Implementación de auditoria informática con la ISO 27001, el 50% de los trabajadores encuestados indicaron que NO tienen conocimiento de seguridad informática y seguridad de un sistema de información.

Palabras Clave: Auditoria, Información, ISO 27001, Seguridad

Conclusiones

1. En lo que respecta a la dimensión 01: Nivel de conocimiento. En la Tabla Nro. 15 se puede interpretar que el 50 % de los trabajadores encuestados contestaron que no tienen conocimiento acerca de seguridad de la información. Este resultado tiene una similitud con lo indicado en la hipótesis para esta dimensión.
2. Con respecto a la dimensión 02: Seguridad de la información, en la Tabla Nro.26 se puede examinar que el 55 % de los trabajadores encuestados contestaron que NO existe en la municipalidad seguridad de la información, por lo tanto, no cuenta con la seguridad adecuada para los activos de la municipalidad. Este resultado tiene una similitud con lo indicado en la hipótesis para esta dimensión, por lo tanto, se concluye que la hipótesis es aceptada.

Interpretación:

Las conclusiones resaltan que hay una carencia de conocimiento significativa sobre seguridad de la información entre los trabajadores de la Municipalidad Distrital de Suyo-Piura. Además, se destaca la percepción de que la seguridad de la información en la municipalidad es

insuficiente, respaldando así las hipótesis planteadas en ambas dimensiones. Estos hallazgos sugieren la necesidad de implementar medidas para mejorar el conocimiento y la seguridad de la información en la organización.

2.1.3 Antecedentes locales

Según la tesis desarrolla por Arisaca F. y Quispe S. (2017) Desarrolló su proyecto de tesis denominado: **"Desarrollo de una propuesta de implementación de la NTP–ISO/IEC 27001:2014, Sistema de Gestión de Seguridad de la Información, para la Oficina Funcional de Informática del Gobierno Regional del Cusco"**.

Escuela Profesional de Ingeniería Informática y de Sistemas/ Universidad Nacional de San Antonio Abad del Cusco, 2016.

Resumen

Como parte del proyecto desarrollado y en respuesta a que no cuenta con un sistema de gestión de seguridad de información en la oficina de Informática del gobierno regional del Cusco desarrolló el trabajo de tesis, que muestra las etapas de diseño y planificación de un Sistema de Gestión de Seguridad de la Información alineado a las especificaciones y requisitos de la NTP ISO/IEC 27001:2014, adaptando este proceso al contexto de la Oficina Funcional de Informática; para lo cual se adquirió y utilizó la NTP ISO/IEC 27001:2014 para su revisión e interpretación, donde identificaron los procesos claves de las etapas de desarrollo del proyecto, las cuales son: Organización, Planificación, Despliegue, Revisión y Consolidación.

El propósito de su proyecto fue desarrollar una propuesta de implementación de los requisitos de la NTP ISO/IEC 27001:2014, que se exige para la conformidad de un Sistema de Gestión de Seguridad de la Información. A principio se realizó un diagnóstico de la situación

actual de la Oficina Funcional de Informática en relación al cumplimiento de los requisitos de la norma, logrando así identificar las debilidades y falencias en temas de seguridad de la información relacionados al cumplimiento de la norma. Se identificaron los procesos y actividades que se llevaron a cabo en cada etapa del desarrollo del proyecto el cual fue alineado a la metodología del ciclo Deming – PHVA (Planificar, Hacer, Verificar y Actuar) donde a su vez se aplicaron conceptos y directrices sobre la gestión de proyectos.

Fue desarrollado esta propuesta para la institución como una guía y soporte para el inicio de sus actividades de implementación de un Sistema de Gestión de Seguridad de la Información como es exigido por ley (RM N° 004-2016-PCM).

Palabras clave: seguridad de la información, procesos, guía PMBOK, valoración de riesgo, proyecto de implementación, ISO 27001.

Conclusiones

1. En su proyecto de tesis concluyó con la revisión y estudio de los requisitos y especificaciones de la NTP ISO/IEC 27001:2014, asimismo con el diagnostico de su cumplimiento en la organización del Gobierno Regional del Cusco, lo cual permitió definir los procesos y actividades requeridos para el diseño y planificación del Sistema de Gestión de Seguridad de Información.
2. El proyecto de tesis fue desarrollado bajo las metodologías seleccionadas, logró consolidar el diseño del Sistema de Gestión de Seguridad de Información y la propuesta de implementación, los mismos que se construyen como un soporte para el inicio de sus actividades en la implementación de la NTP ISO /IEC 27001:2014.
3. Se concluyó con el estudio y evaluación de riesgos realizados en la oficina funcional de Informática ha permitido identificar los activos de información críticos, los riesgos

asociados a estos, los propietarios de cada riesgo y así los controles de seguridad requeridos para garantizar un nivel de seguridad adecuado.

4. En análisis de riesgos efectuado en la oficina funcional informática, la evaluación de criterios de aceptación de riesgos y elaboración de la declaración de aplicabilidad (SOA) permitieron identificar los controles de seguridad necesarios para elaborar el tratamiento de riesgos.

Interpretación

El proyecto de tesis concluye con la definición de procesos y actividades para el diseño y planificación del SGSI, bajo metodologías específicas. Además, ha permitido la identificación y tratamiento de riesgos, proporcionando a la Oficina de Informática del Gobierno Regional del Cusco una guía y soporte para iniciar las actividades de implementación de la norma ISO/IEC 27001:2014.

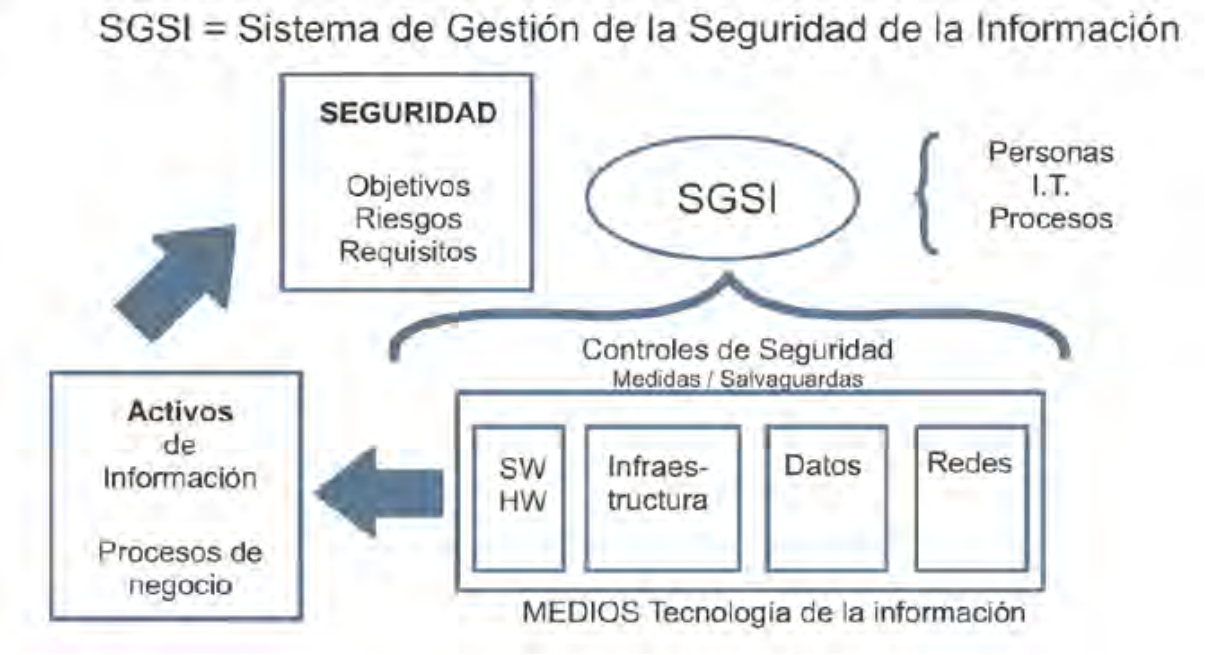
2.2 Marco conceptual

2.2.1 Sistema de gestión de seguridad de información.

Según (Ricardo Lopéz, 2017) El SGSI es un proceso sistemático, protocolizado y manejado por todos los miembros de la empresa que permite la confiabilidad, integridad y disponibilidad de la información de la misma.

El primer documento consolidado sobre gestión de seguridad de la información fue publicado por la BSI (British Standards Institution) conocido como la norma BS 7799 donde se compilan un conjunto de buenas prácticas para la SGSI pero fue en la versión de 1998 cuando se establecen los términos y requisitos para certificación.

Figura 8. Esquema de Sistema de Gestión de Seguridad de Información

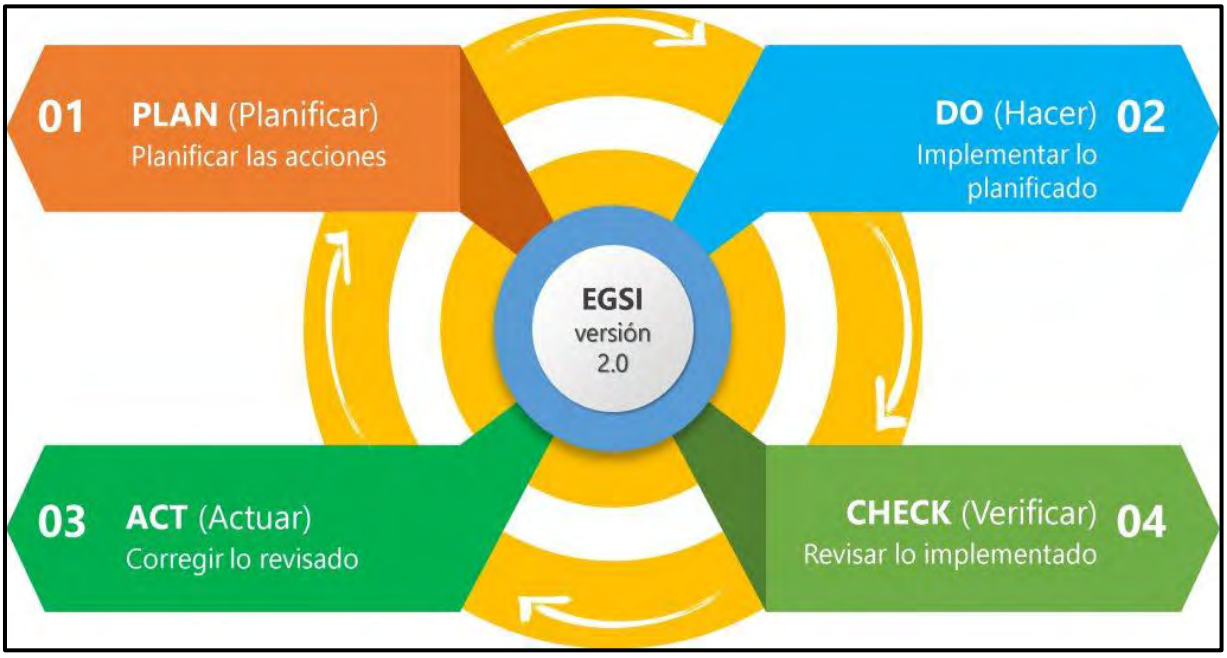


Fuente: https://enterpriseit.cl/wp-content/uploads/2020/06/SGSI.png

2.2.2 Seguridad de información según modelo PDCA.

Según (Calderon, 2004) Indica que la organización de la seguridad de la información cumple cuatro niveles repetitivos que comienzan por Planificar, Hacer, Actuar y termina en Verificar, consiguiendo así mejorar la seguridad, como se identifica en la siguiente figura 6.

Figura 9. Plan de PDCA



Fuente: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/08/Ciclo-de-PDCA-1024x522.jpg

- **Planificar (Plan**): Consiste en establecer el contexto, en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad.
- **Hacer (Do):** Consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.
- **Verificar (Check):** consiste en monitorear las actividades y hacer auditorías internas.
- **Actuar (Act):** Consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

2.2.3 ISO 27000

Según (Regina Baena, 2019)La serie de normas internacionales ISO/IEC 27000 ofrecen una serie de recomendaciones de mejores prácticas, para la gestión de la seguridad de la información, y esta puede ser aplicada en cualquier organización sin importar el tamaño que tenga, está orientada a que estas puedan mantener un Sistema de Gestión de la Seguridad, de las cuales más adelante solo se harán la descripción de la 27001,27002, 27003, 27004, 27005 y 27006, al ser las que se encuentran relacionadas más íntimamente con la puesta en marcha de un SGSI.

2.2.4 Familia ISO 27001

ISO 27001: Publicada el 15 de octubre de 2005. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. Sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados Desde el 28 de Noviembre de 2007, esta norma está publicada en España como UNE-ISO/IEC 27001:2007.

2.2.5 Familia ISO 27002

Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO27001 contiene un anexo que resume los controles de ISO 27002:2005. En España, aún no está traducida (previsiblemente, a lo largo de 2008). Desde 2006, sí está traducida en Colombia (como ISO 17799) y, desde 2007, en Perú (como ISO 17799; descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en ISO.org. (ISO -International Organization for Standardization, 2011)

2.2.6 Familia ISO 27003

Fue publicada en mayo del 2009. Consiste en un guía de implementación de SGSI acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases. Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación. (ISO -International Organization for Standardization, 2011)

2.2.7 Familia ISO 27004

Fue publicada en noviembre del 2008. Donde indica que especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase “Do” (Implementar y Utilizar) del ciclo PDCA. (ISO -International Organization for Standardization, 2011).

2.2.8 Familia ISO 27005

Publicada el 4 de junio de 2008. Establece las directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. El conocimiento de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001 e ISO/IEC 27002 es importante para un completo entendimiento de la norma ISO/IEC 27005:2008 (ISO -International Organization for Standardization, 2011)

2.2.9 Familia de normas ISO/IEC 27000

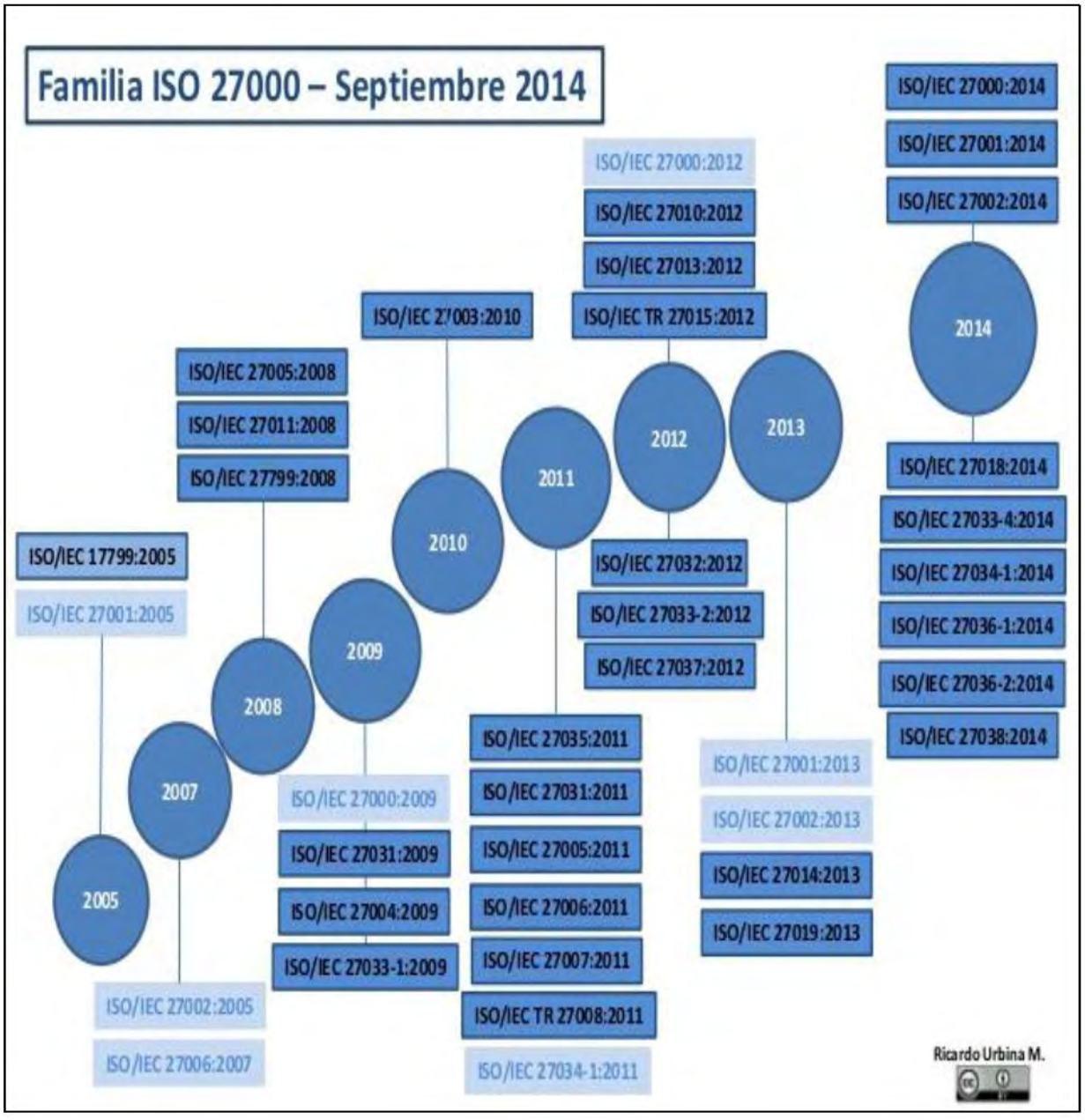
Tabla 1: Normas ISO/IEC 27000

Norma ISO/IEC	Fecha	Contenido
27000	2008	27000 2008 Términos y definiciones que estandarizan el vocabulario de la serie.
27001	2005, 2013 última actualización	27001 Sistema de Gestión de Seguridad de la Información. SGSI. Norma certificable.
27002	2005, 2007, 2013 última	Guía de buenas prácticas. Enumera los objetivos de control y controles a desarrollar en cuanto a seguridad informática. Antigua ISO 17799 derivada de BS799
27003	2010	Guía de implementación de SGSI
27004	2009	Especifica métricas y técnicas de medidas aplicables para determinar la eficacia del SGSI
27005	2008, Revisada 2011	Diseñada para ayudar a la aplicación de la seguridad informática desde un enfoque de gestión de riesgos.
27006	2007	Requisitos para la acreditación de entidades de auditoría y certificación.
27007	2011	Guía de auditoría.
27011	2008	Implementación del SGSI en el sector de telecomunicaciones.

Fuente: www.iso27000.es Familia de normas ISO 27000

NOTA: En esta tabla muestra la familia de las normas ISO con su respectivo contenido.

Figura 10. Familia ISO 27000



Fuente:https://image.slidesharecdn.com/iso27000evolucinslideshareruseр2014-141015125250-conversion-gate01/85/familia-isoiec-27000-evolucin-a-septiembre-2014-1-320.jpg?cb=1667582869

2.2.10 Norma técnica peruana ISO 27001:2014

Según (NTP ISO/IEC/ 27001, 2014) Se Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da Edición", en todas las entidades integrantes del Sistema Nacional de Informática, con la finalidad de coadyuvar con la infraestructura de Gobierno Electrónico, por considerar a la seguridad de la información, como un componente crucial para dicho objetivo; De conformidad con lo dispuesto en la Ley Nº 29158, Ley Orgánica del Poder Ejecutivo; la Ley Nº 27658, Ley Marco de Modernización de la Gestión del Estado; y, el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros aprobado mediante Decreto Supremo Nº 063-2007-PCM y sus modificatorias, para garantizar la confidencialidad, la integridad de la información.

La propuesta de la norma mediante la cual se establece el uso obligatorio por parte de las entidades de la administración pública de la NTP ISO/IEC 27001:2014, tecnología de la información. Técnicas de seguridad, Sistemas de gestión de seguridad de la información, los requisitos permiten garantizar el adecuado tratamiento de la información que permita conocer y manejar los riesgos asociados a los activos de información.

2.2.11 Activos de información.

Según (Rojas, 2016) Enfoca a la seguridad de la información para proteger los activos de información, como los conocimientos o datos que tienen valor para una organización, en sus diferentes formas y estados, a través de la reducción de riesgos a un nivel aceptable, mitigando las amenazas que están constante actividad.

Figura 11. Activos de Información

Fuente: https://www.redalyc.org/journal/6738/673870839003/673870839003_gf2.png

2.2.12 Diferencia entre ISO 27001 y la NTP ISO/IEC 27001:2014

Tabla 2: Diferencia entre ISO 27001 Y NTP:ISO/IEC 27001

N°	ISO 27001	NTP ISO/IEC 27001:2014
1	Alcance	Objeto y campo de aplicación
2	Referencias Normativas	Referencias normativas
3	Términos y definiciones	Términos y definiciones
4	Emprendimiento	Contexto de la organización
5	Liderazgo	Liderazgo
6	Planeación	Planificación
7	Soporte	Soporte
8	Operación	Operación
9	Evaluación de desempeño	Evaluación del desempeño
10	Mejora	Mejora continua

Fuente: Elaboración propia

2.2.13 Ciclo Deming (PDCA)

El ciclo Plan, Do, Check y Act (PDCA), ciclo Deming (Edwars Deming, 1982) o de mejora continua (Laurett y Mendes, 2019), provee un medio para la implementación sistemática de un sistema de garantía de calidad, a partir de un sistema de planificación inicial. Es la planificación inicial la que sienta las bases para las acciones posteriores, siempre orientadas a verificar la adecuación, idoneidad y promover la mejora continua en diferentes instituciones.

El ciclo Deming provee un marco útil para implementar y evaluar proyectos de calidad y se ha utilizado ampliamente en diversas organizaciones para la mejora de procesos: desde la industria productiva, hasta servicios como la salud y la educación (Chen, 2012). Como se ha señalado, en su versión tradicional, es un ciclo que consta de cuatro etapas principales: Plan, Do, Check, Act.

Figura 12. Ciclo Deming PDCA

Fuente: http://crisaza.com/wp-content/uploads/2019/08/Ciclo-de-Deming-PDCA-Planear-Hacer-Verificar-Actuar-Camilo-Rodriguez-Isaza.png

Tabla 3: Procesos del Ciclo Deming (PDCA)

Ciclo PDCA	**Procesos**
Planear (*Plan*)	• Establecer el contexto. • Alcance y Limites • Definir Política del SGSI • Definir Enfoque de Evaluación de Riesgos • Identificación de riesgos • Análisis y Evaluación de riesgos • Evaluar alternativas para el Plan de tratamiento de riesgos • Aceptación de riesgos • Declaración de Aplicabilidad
Hacer (*Do*)	• Implementar plan de tratamiento de riesgos • Implementar los controles seleccionados • Definir las métricas • Implementar programas de formación y sensibilización • Gestionar la operación del SGSI • Gestionar recursos • Implementar procedimientos y controles para la gestión de incidentes de • seguridad
Verificar (*Check*)	• Ejecutar procedimientos de seguimiento y revisión de controles. Realizar revisiones regulares de cumplimiento y eficacia de los controles y del SGSI. • Medir la eficacia de los controles y verificación de satisfacción de los • requerimientos de seguridad. • Revisión de la evaluación de riesgos periódicamente. • Realizar auditorías internas • Revisión de alcance y líneas de mejoras del SGSI por la Dirección. • Actualizar los planes de seguridad • Registrar acciones que podrían impactar la eficacia y/o eficiencia del SGSI.
Actuar (*Act*)	• Implementar las mejoras identificadas para el SGSI • Implementar las acciones correctivas y preventivas pertinentes. • Comunicar acciones y mejoras a todas las partes involucradas. • Asegurarse que las mejoras logren los objetivos previstos.

Fuente: (Gustavo Pallas Mega, 2009, p 10 de 186)

Ciclo de Deming (PHVA) aplicado a la norma ISO/IEC 27001

2.2.14 Pilares de la seguridad de la información

Según el autor (Ricardo Lopéz, 2017) indica que la seguridad de la información según la ISO/IEC 27001 se basa en tres pilares fundamentales la confidencialidad, la disponibilidad y la integridad, estos factores se deben garantizar en una adecuada gestión de seguridad de la información.

a) Confidencialidad de la información

El uso cada vez mayor de la red requiere la circulación de información y datos tanto de empresas como de ciudadanos del común. Cualquier tipo de consulta, transacción y acceso a la web deja una huella de nuestra identificación que queda perennemente en el sistema.

Desde la huella digital, hasta la IP, así como datos personales pueden ser de libre acceso a cualquier persona sino se contará con un SGSI que protegiera dicha información disminuyendo su vulnerabilidad.

b) Disponibilidad de la información

La disponibilidad de la información hace referencia al almacenamiento de la información y su accesibilidad al usuario, es la posibilidad de tener la información en el tiempo y espacio requerido. Brindar la información, mantener actualizado el sistema y facilitar su acceso asegura enormes beneficios para la empresa. Sin embargo, debe optimizarse el control de riesgos y disminuir la vulnerabilidad de este flujo.

c) Integridad de la información

La integridad hace referencia a la inmutabilidad de la información por personal no autorizado, da cuenta de la certeza de los datos que sean precisos, válidos y coherentes.

Un incidente en la integridad de la información puede resultar nefasto para la empresa, un cambio en el flujo de procesos o de formulación tendría un costo demasiado alto. Por tanto, el control de la integridad de datos y su eficaz protección son fundamentales en el SGSI.

La integridad es el factor más importante de la seguridad de la información ya que de nada sirve una información disponible y confidencial si su integridad ha sido vulnerada es decir no es exacta ni valida.

2.2.15 Marco normativo nacional e internacional

Tabla 4: Entidades Normalizadoras de las Normas ISO

Entidades Normalizadoras	
IUT-T	International Telecommunication Unión, las comisiones de estudio del sector de normalización de las telecomunicaciones, quienes elaboran recomendaciones UIT para las TIC con el objeto de estandarizar un lenguaje común para su uso global.
ISO / IEC*	International Organization for Standarization. Organización encargada de crear normas de estandarización internacional. La ISO/IEC es un marco internacional de las prácticas de seguridad informática reconociendo la información como un activo de gran valor para las empresas.
CEN/CENELAC	Comité europeo de normalización electrónica que junto a la ETSI produce normas aplicables a nivel mundial en torno a las TIC
ICONTEC	Instituto Colombiano de normas técnicas y certificación. Es el organismo que emite las certificaciones de calidad en nuestro país.
BSI	British Standards Institution (BSI), institución Británica encargada de la creación de normas para la estandarización de procesos, centra sus actividades en la certificación, auditoria y formación de normas. Es una entidad colaboradora de la ISO y proveedora de normas.

Fuente: www.ISO27000.es

2.2.16 Resolución Directoral para la elaboración del SGSI de la Municipalidad Distrital de Chamaca 2020

La Municipalidad Distrital de Chamaca aprobó la implementación del Sistema de Gestión de Seguridad de Información conformando el comité encargado de la elaboración de mismo que se menciona en el anexo 4.

2.2.17 Población objetivo el proyecto de investigación

2.2.17.1 Población

La población objetivo del presente proyecto de investigación es finita y está constituido por 45 terminales informáticos compuestas por las oficinas administrativas de la Municipalidad Distrital de Chamaca de los cuales se consideró 21 terminales tecnológicos más relevantes e importantes de la Municipalidad Distrital de Chamaca como son:

Tabla 5: Población objetivo para la aplicación de encuestas

N° Terminal	TERMINALES TECNOLÓGICOS	ABREVIATURA
1	Recursos Humanos	RR. HH
2	Procuraduría Municipal	PROCUR
3	Gerencia de desarrollo social	DSOCIAL
4	Contabilidad	CONTA
5	Logística y Abastecimiento	LOGISTI
6	Oficina de proyecto	OPMI
7	Gerencia de Infraestructura	INFRAEST
8	Gerencia de desarrollo ambiental	DES. AMBI
9	Área de presupuesto	PRESUP
10	Demuna	DEMUN
11	Área técnica Municipal	ATM
12	Desarrollo Ambiental	AMBIEN
13	Alcaldía	ALCALDIA
14	Supervisión	SUPERV
15	Rentas	RENT
16	Secretaria general	SECRET
17	Obras	OBRAS
18	Oficinas de Informática y de Sistemas	INFORM
19	Abastecimiento	ABASTEC
20	Tesorería	TESORERIA
21	Mantenimiento y maquinarias	MAQUIN
	TOTAL	

Fuente: Elaboración propia

2.2.17.2 Muestra

Para la presente investigación, la muestra se seleccionó a 21 trabajadores de las oficinas de la Municipalidad Distrital de Chamaca, no se utilizó ninguna técnica estadística por ser los involucrados directos en la seguridad de información.

Hernández R, Fernández C y Baptista P. (37), definieron a la muestra como un subgrupo de la población. Un subconjunto de elementos dentro de un conjunto que posee características similares, a la cual se le considera la población. Adicionalmente, estos autores mencionaron que cuando en el caso se incluye todos los elementos del universo o población, se le denomina censo.

2.2.17.3 Técnicas e Instrumentos de recolección de datos

En la presente investigación se utilizó la encuesta como técnica y el cuestionario

- La técnica que se maneja es la encuesta.

Encuesta: Es el conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de población, que se considera por determinadas circunstancias funcionales al trabajo, representativa de esa población, con el objetivo de conocer la opinión de los trabajadores de la Municipalidad Distrital de Chamaca.

- El instrumento que se utiliza es el cuestionario

Cuestionario: Es un procedimiento considerado clásico en las ciencias sociales para la obtención y registro de datos. Su versatilidad permite utilizarlo como instrumento de investigación y como instrumento de evaluación de personas, procesos y programas de formación. Es una técnica de evaluación que puede abarcar aspectos cuantitativos y cualitativos. Su característica singular radica en que, para registrar la información solicitada de los trabajadores de la Municipalidad Distrital de Chamaca.

Capítulo III

Desarrollo del Proyecto

CAPÍTULO III.

3 DESARROLLO DE LA PROPUESTA DE SGSI.

3.1 Objetivos del SGSI en la MDCH.

Establecer políticas estándares de seguridad de información para proteger los activos de información bajo los estándares de la NTP/ISO/IEC:27001 y procedimientos para la adecuada gestión de los activos de información en la Municipalidad Distrital de Chamaca**.**

Fortalecer la estructura organizacional considerando los procesos internos, el crecimiento físico, tecnológico y desarrollo de las capacidades del talento humano en conjunto con iniciativas en el ámbito financiero que posibiliten el mejoramiento de la capacidad de gestión de la Municipalidad Distrital de Chamaca.

3.2 Desarrollo del ciclo Deming en la propuesta del SGSI

Este ciclo Deming aplicado al SGSI, proporciona un enfoque sistemático para gestionar la seguridad de la información de manera efectiva, adaptándose y mejorando continuamente para hacer frente a los cambios en el entorno de amenazas y los requisitos organizativos.

3.3 Fase Plan: Establecer la propuesta del SGSI

Para el desarrollo de este proyecto se utilizó la fase de planificar que es la más influyente, mediante métodos como la realización de encuestas a los trabajadores y búsqueda de nuevas tecnologías que se debía de definir:

Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases

Figura 13. Fase planificar del proyecto

Fuente: www.iso27000.es

3.3.1 Alcance de la propuesta del SGSI en la MDCH.

En función de características de la Municipalidad Distrital de Chamaca, localización, activos y tecnología, definir el alcance corresponde a los límites del Sistema de Gestión de Seguridad de la Información el cual debe ser aprobado por el responsable de seguridad de la información del área de tecnología de la Municipalidad Distrital de Chamaca.

3.3.2 Políticas generales de seguridad de información en la Municipalidad Distrital de Chamaca.

De manera general se muestran las políticas estándares de seguridad de Información para proteger los activos de información en la Municipalidad Distrital de Chamaca, este es base del desarrollo del documento ya que contempla los principios

básicos a tener en cuenta en su elaboración dentro de la planeación del sistema de gestión de seguridad de la información en la Municipalidad Distrital de Chamaca.

Es muy importante destacar que la política tiene que estar adaptada a las características de la Municipalidad, comunicándose a todos los interesados y contar con el compromiso de la Municipalidad Distrital de Chamaca. La norma ISO 27001 establece todos los puntos que las entidades públicas y privadas tienen que cumplir, así como los objetivos de seguridad de la información. Uno de los más importantes es que sean medibles, para lo cual ayudará a tener presente los tres principios claves de este estándar internacional:

- **Confidencialidad:** solo las personas autorizadas para ello deben conocer los datos.
- **Integridad:** la información tiene que ser completa, válida, veraz, exacta y no estar manipulada.
- **Disponibilidad**: la información ha de ser accesible de forma que los usuarios autorizados para ello puedan disponer de ella cuando la necesiten y garantizar su protección.

La Gerencia de la Municipalidad Distrital de Chamaca, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de la NTP ISO/IEC 27001:2014 y en concordancia con la misión y visión de la Municipalidad Distrital de Chamaca, es así que se plantean los siguientes objetivos:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.

- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus trabajadores, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Municipalidad Distrital de Chamaca.
- Garantizar la continuidad del negocio frente a incidentes.
- Municipalidad Distrital de Chamaca ha decidido definir, **implementar, operar y mejorar** de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a los requerimientos de la NTP ISO/IEC 27001:2014, y a los requerimientos regulatorios.

A continuación, se establecen 11 políticas de seguridad que soporta el SGSI en la Municipalidad Distrital de Chamaca:

1) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los trabajadores, proveedores, funcionarios de la Municipalidad Distrital de Chamaca.

2) La Municipalidad Distrital de Chamaca protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o usuarios).

3) La Municipalidad Distrital de Chamaca protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

4) La Municipalidad Distrital de Chamaca protegerá su información de las amenazas originadas por parte del personal que labora en la Municipalidad.

5) La Municipalidad Distrital de Chamaca protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

6) La Municipalidad Distrital de Chamaca controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

7) La Municipalidad Distrital de Chamaca implementará control de acceso a la información, sistemas y recursos de red.

8) La Municipalidad Distrital de Chamaca garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

9) La Municipalidad Distrital de Chamaca garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

10) La Municipalidad Distrital de Chamaca garantizará la disponibilidad de sus procesos administrativos y la continuidad de su operación basada en el impacto que pueden generar los eventos.

.

3.3.3 Identificación de los activos de información de la MDCH

Tabla 6: Activos de información de la MDCH

CATEGORIA	TIPO DE ACTIVO
Información	• Copias de respaldo • Información escrita • Proyectos y Planificación Urbana • Información de Emergencia • Código fuente de los sistemas de información
Software	• Servidor de aplicaciones • Sistema de Gestión de Base de datos • Antivirus • Ofimática • Sistema Operativo • Sistemas de Información • Autocad, Adobe • Sistema de Tramite Documentario • SIAF
Físicos	• Equipo de procesamiento • Equipo de comunicaciones • Medio de Almacenamiento • Infraestructura Tecnológica • Equipos de escritorio • Documentos Oficiales • Impresoras y Escáner
Servicios	• Procesamiento y comunicaciones • Correo Electrónico • Energía eléctrica • Agua
Personal	• Personal Interno • Administrador de Sistemas • Datos Personales • Trabajadores de la Municipalidad. •

Fuente: Elaboración propia

3.3.4 Identificación de amenazas en la Municipalidad Distrital de Chamaca

Se realizó la identificación de amenazas asociados a los activos de información. En esta etapa es especialmente importante la participación del personal designado para la implementación de la ´propuesta del Sistema de Gestión de Seguridad de la Información (SGSI).

Tabla 7: Tipos de amenazas

TIPO	N°	TIPO DE AMENAZA
AMENAZAS A LA INFORMACIÓN	1	Acceso no autorizado a la información
	2	Eliminación no autorizada a la información
	3	Modificación no autorizada a la información
	4	Robo de activos de información
	5	Inadecuada eliminación de activos de información
AMENAZAS AL SOFTWARE	6	Adulteración del software
	7	Cambios no autorizados sobre el software
	8	Actualizaciones no controladas del software
	9	Hacking/Cracking
	10	Virus informáticos
AMENAZAS A ACTIVOS FÍSICOS (EQUIPOS)	11	Corto Circuito
	12	Filtraciones de agua
	13	Desconexión de equipos
	14	Robo de equipos o de sus componentes
	15	Incumplimiento del plan de mantenimiento
AMENAZAS A SERVICIOS	16	Falla de servicios para las telecomunicaciones
	17	Degradación de servicios para las telecomunicaciones
	18	Falla de la provisión de energía eléctrica
	19	Incumplimiento de fechas por parte de proveedores
	20	Provisión de servicios defectuosos(personal)
AMENAZAS AL PERSONAL	21	Contaminación del ambiente
	22	Uso de credenciales falsificadas
	23	Bloqueo del acceso al centro de trabajo
	24	Dificultad en el desplazamiento hacia el centro de trabajo
	25	Contaminación del ambiente
AMENAZAS A UBICACIONES FISICAS	26	Sismo
	27	Inundación
	28	Hundimiento de suelos
	29	Incendio
	30	Destrucción intencional de los ambientes (protestas)

Fuente Elaboración propia.

3.3.5 Identificación de vulnerabilidades

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información críticos. Para facilitar la identificación de las vulnerabilidades se clasifican de acuerdo con las distintas fuentes que las puedan originar, tal como se propone a continuación:

Tabla 8: Cuadro de Vulnerabilidades

Tipo	N°	VULNERABILIDADES	EJEMPLO AMENAZAS
HARDWARE	1	Mantenimiento insuficiente	Ruptura de la mantenibilidad del sistema de información
	2	Falta de esquema de reemplazo periódicos	Destrucción de equipos o medio
	3	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento
	4	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	5	Falta de control eficiente del cambio de configuración	Error en el uso
SOFTWARE	6	Errores conocidos en el software	Abuso de derechos
	7	No hacer “logout” cuando se sale de las estaciones de trabajo	Abuso de derechos
	8	Software ampliamente distribuido	Corrupción de datos
	9	Asignación equivocada de derechos de acceso	Abuso de derechos
	10	Falta de documentación	Error en uso
	11	Falta de identificación y autentificación de receptor y destinatario	Falsificación de derechos

Tipo	N°	VULNERABILIDADES	EJEMPLO AMENAZAS
RED	12	Arquitectura de red insegura	Espionaje remoto
	13	Transferencia de contraseñas autorizadas	Espionaje remoto
	14	Gestión inadecuada de la red	Saturación del sistema de información
	15	Conexión de red pública sin protección	Uso no autorizado del equipo
PERSONAL	16	Ausencia de personal	Ruptura de la disponibilidad del personal
	17	Procedimientos inadecuados de contratación	Destrucción de equipos o medio
	18	Capacitación insuficiente en seguridad	Error en el uso
	19	Uso incorrecto de Software y Hardware	Error en el uso
	20	Falta de conciencia de seguridad	Error en el uso
SITIO	21	Uso inadecuado o descuido del control de acceso a las edificaciones o recintos	Inundación
	22	Red inestable de energía eléctrica	Perdida de suministro eléctrico
	23	Falta de protección física del edificio puertas y ventanas.	Robo de equipos

Fuente: Elaboración propia

3.3.6 Conformación del comité de seguridad de información en la MDCH

Tabla 9: Comité de seguridad

Nombre	Unidad Organizativa	Cargo	Correo electrónico
Antonio Huamán Arias	Alcaldía	Alcalde	alcaldia@munichamaca.gob.pe
Juan Cancio Vega Pimentel	Gerencia Municipal	Gerente General	gerenciamunicipal@munichamaca.gob.pe
Hugo Flores Orcon	Presupuesto	Jefe de Presupuesto	presupuesto@munichamaca.gob.pe
Alcides Larota Cuito	Informática y Estadística	Responsable de Informática	informatica@munichamaca.gob.pe
Elías Aguirre García	Asesoría Legal	Asesor legal	asesorialegal@munichamaca.gob.pe

Fuente: Resolución de conformación de comité de seguridad de información de la MDCH. Anexo 4

3.4 Fase Do: Implementar controles para la propuesta del SGSI.

3.4.1 Identificar controles de riesgos de acceso a la información

Una vez identificadas las amenazas y vulnerabilidades relacionadas con los activos de información, se procede a detallar el riesgo de seguridad de la información.

3.4.2 Evaluación de riesgos

La evaluación del riesgo es el componente por el cual se estima la valoración del riesgo del activo de soporte, mediante técnicas cualitativas de valorización del riesgo, con la finalidad de estimar el impacto si llegase a ocurrir, y con qué frecuencia (dentro de período de tiempo de un año) para cada riesgo. En un segundo nivel de evaluación, también se tiene en cuenta los controles existentes, así como su efectividad.

Tabla 10: Niveles de riesgo

Nivel de Riesgo	Descripción
Extremo	Si el riesgo llega a materializarse tendría un impacto o efecto extremo
Alto	Si el riesgo llega a materializarse, tendría un alto impacto.
Moderado	Si el riesgo llega a materializarse, tendría impacto moderado.
Bajo	Si el riesgo llega a materializarse, tendría un efecto bajo.

Fuente: Elaboración propia

El riesgo de un activo de información corresponde al nivel de riesgos sin considerar los controles existentes o planificados para disminuir la frecuencia.

Tabla 11: Nivel de impacto

Nivel	Valor	Compatibilidad
Raro	1	Raro
Improbable	2	Improbable
Posible	3	Moderado
Probable	4	Probable
Casi Seguro	5	Casi Certeza

Fuente: Elaboración propia

El nivel de impacto se estima como la magnitud de la consecuencia de la perdida de la confidencialidad, integridad y disponibilidad del activo de información.

Tabla 12: Nivel de importancia

Nivel de Importancia	Valor	Nivel de Impacto
Muy Alto	5	Catastrófico
Alto	4	Mayor
Mediano	3	Moderado
Bajo	2	Menor
Muy Bajo	1	Insignificante

Fuente: Elaboración propia

El valor del riesgo se estima mediante una función de los valores de la frecuencia y el impacto del riesgo.

3.4.3 Evaluación del estado inicial de la MDCH con respecto a los requisitos de la NTP ISO/IEC 27001:2014

Para evaluar el estado inicial de la Municipalidad Distrital de Chamaca, con respecto a los requisitos de la NTP ISO/IEC 27001:2014, se ha definido dos maneras de presentar los resultados: una descriptiva y otra cuantificable (Ver Tabla 6). Esta técnica se basa en calificar el estado de los requerimientos en función a una escala aplicando cinco opciones que van de menor a mayor.

Tabla 13: Criterio para evaluar el estado inicial de la MDCH

Criterio de Calificación	Valoración
No diseñado: Las actividades/métodos demuestran que no se tiene el requisito y/o no se ha bosquejado su implementación.	0%
Parcialmente diseñado: Las actividades/métodos demuestran que se tiene el requisito definido, pero este no es del todo conforme con el requisito de la NTP ISO/IEC 27001:2014.	25%
Diseñado: Los métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, pero sin evidencias de aplicación**.**	50%
Parcialmente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, pero con pocas evidencias de aplicación.	75%
Completamente implementado: Las actividades/métodos son conformes con el requisito de la NTP ISO/IEC 27001:2014, y se cuenta con evidencias de aplicación permanentes.	100%

Fuente: Elaboración propia

Nota: Adaptado del proyecto "Diseño de un Sistema de Gestión de Seguridad de la Información bajo la NTP ISO/IEC 27001:2014 para la Municipalidad Provincial de Huamanga, 2016" (Tesis), p. 57,(Ccesa Quincho, 2017).

Se elaboró la línea base y requerimientos de la norma y se realizó la evaluación de la siguiente manera:

• Se puntuó cada requisito.

• De acuerdo al puntaje obtenido se colocó la evidencia/sugerencia para el cumplimiento de la NTP ISO/IEC 27001:2014.

• Para el porcentaje por capítulo, se sacó el promedio de los requisitos por capítulo.

El resultado que se obtuvo de la evaluación del estado inicial de la Municipalidad Distrital de Chamaca, respecto a los requisitos de la NTP ISO/IEC 27001:2014 se muestra en forma de tabla. Un extracto de esta evaluación se muestra a continuación.

Tabla 14: Estado inicial de la MDCH respecto a la NTP ISO/IEC 27001:2014

N°	REQUERIMIENTO	ESTADO	EVIDENCIA/SUGERENCIA	VALORACION
8	**CONTEXTO DE LA ORGANIZACIÓN**	**No Diseñado**	**Se sugiere realizar el análisis del contexto de la MDCH,** para comprender, tanto los aspectos externos como internos, las partes interesadas y requisitos relevantes al SGSI y, elaborar y documentar el alcance del SGSI.	**6%**
8.1	**Comprender la Organización y contexto**. La organización **debe** determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este SGSI	Parcialmente diseñado	La MDCH posee documentos visibles de su Misión, Visión, Matriz FODA y las Estrategias. Pero no contempla de manera clara ítems de seguridad de la información. Se sugiere establecer objetivos de seguridad de la Información que estén alineados con los objetivos estratégicos.	25%
8.2	**Comprender las necesidades y expectativas de las partes interesadas.** La organización **debe** determinar las partes interesadas y los requisitos de las mismas.	No Diseñado	**Sugerencia:** Determinar las partes interesadas y comprender las necesidades y expectativas de éstas, referentes a la seguridad de la información.	0%

Fuente: Elaboración propia

Tabla 15: Evaluación del estado inicial de la MDCH.

N°	REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? ¿QUÉ SE TENDRÍA QUE HACER?	VALORACIÓN
1	**Determinar el alcance del SGSI.**	No Diseñado	**Sugerencia.** Determinar el alcance del SGSI teniendo en consideración los aspectos referidos en 7.1, los requisitos de 7.2, documentarlo y ponerlo a disposición de las partes interesadas.	1 %
2	**Sistema de Gestión de Seguridad de la información.** La organización **debe** establecer, implementar, mantener y mejorar continuamente un SGSI, en conformidad con los requisitos de esta Norma Técnica Peruana	No diseñado	**Sugerencia.** Establecer un plan para la mejora continua del SGSI conforme a la NTP Vigente	1 %
3	**Términos y definiciones**	No Diseñado	**Para** propósitos de estos documentos se aplican los términos y definiciones proporcionados en ISO/IEC 27000	1 %
4	**Contexto de la organización:** Comprender la organización, comprender las necesidades, determinar el alcance del sistema	No Diseñado	La MDCH debe determinar **aspectos externos e internos** y que afectan su capacidad de logar resultados	3%
5	**Liderazgo y compromiso.** La alta dirección **debe** demostrar liderazgo y compromiso respecto al SGSI. **Política.**	No Diseñado	El titular de la entidad debe mostrar liderazgo y compromiso Establecer la Política de Seguridad de la Información acorde al propósito de la MDCH, incluir los objetivos de seguridad de la Información, mantenerla disponible y comunicada.	2%
6	**PLANIFICACION** Responsabilidades y autoridades organizacionales.	No Diseñado	La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la Seguridad de la Información estén asignadas y comunicadas.	1%
7	**Soporte, recursos,** competencia, concientización, comunicación, información documentada	No diseñado	Establecer un soporte de los recursos de seguridad de información, para mantener una comunicación general en la MDCH	0%

N°	REQUERIMIENTO DE LA NTP ISO/IEC 27001:2014	ESTADO	EVIDENCIA/SUGERENCIA (¿CÓMO LO CUMPLE? ¿QUÉ SE TENDRÍA QUE HACER?	VALORACIÓN
8	**Operación:** Planificación y control, evaluación de riesgos, tratamiento de riesgos de seguridad de información	No diseñado	La MDCH debe planificar y controlar los procesos necesarios e implementar las acciones en la sección 6, implementar planes para lograr los objetivos de seguridad de información	0%
9	**Evaluación de desempeño: Monitoreo, medición y evaluación, auditoría interna, revisión por la gerencia,**	No diseñado	La Municipalidad debe revisar el SGSI para asegurar la conveniencia, adecuación y debe tener la información documentada como evidencia de los resultados.	0%
10	**Mejoras: No conformidades y acción correctiva, Mejora continua**	No diseñado	La MDCH debe controlar y corregir las causas de la no conformidad y también debe mejorar continuamente la conveniencia, adecuación y la efectividad del SGSI.	0%
PUNTAJE TOTAL DE LA EVALUACIÒN DE REQUISITOS DE LA NTP ISO/IEC 27001:2014 en la MDCH				**9%**

Fuente: NTP ISO/IEC 27001: 2014

3.4.4 Responsabilidad

- Los Gerentes, Subgerentes, secretario general, Procurador Publico Municipal y demás funcionarios públicos de la Municipalidad Distrital de Chamaca son los responsables para aprobar la propuesta del Sistema de Gestión de Seguridad de la Información en la MDCH.
- La responsabilidad recae también en todos los trabajadores independientemente del régimen laboral que tengan con al Municipalidad Distrital de Chamaca, tratándose de un mecanismo de seguridad de la información.
- La Gerencia de Tecnologías de la Información es responsable de la implementación de la propuesta del Sistema de Gestión de Seguridad de la Información para su

seguimiento y supervisión para el estricto cumplimiento de esta propuesta de SGSI a la Municipalidad Distrital de Chamaca.

3.4.5 Análisis de Riesgos en la Municipalidad Distrital de Chamaca

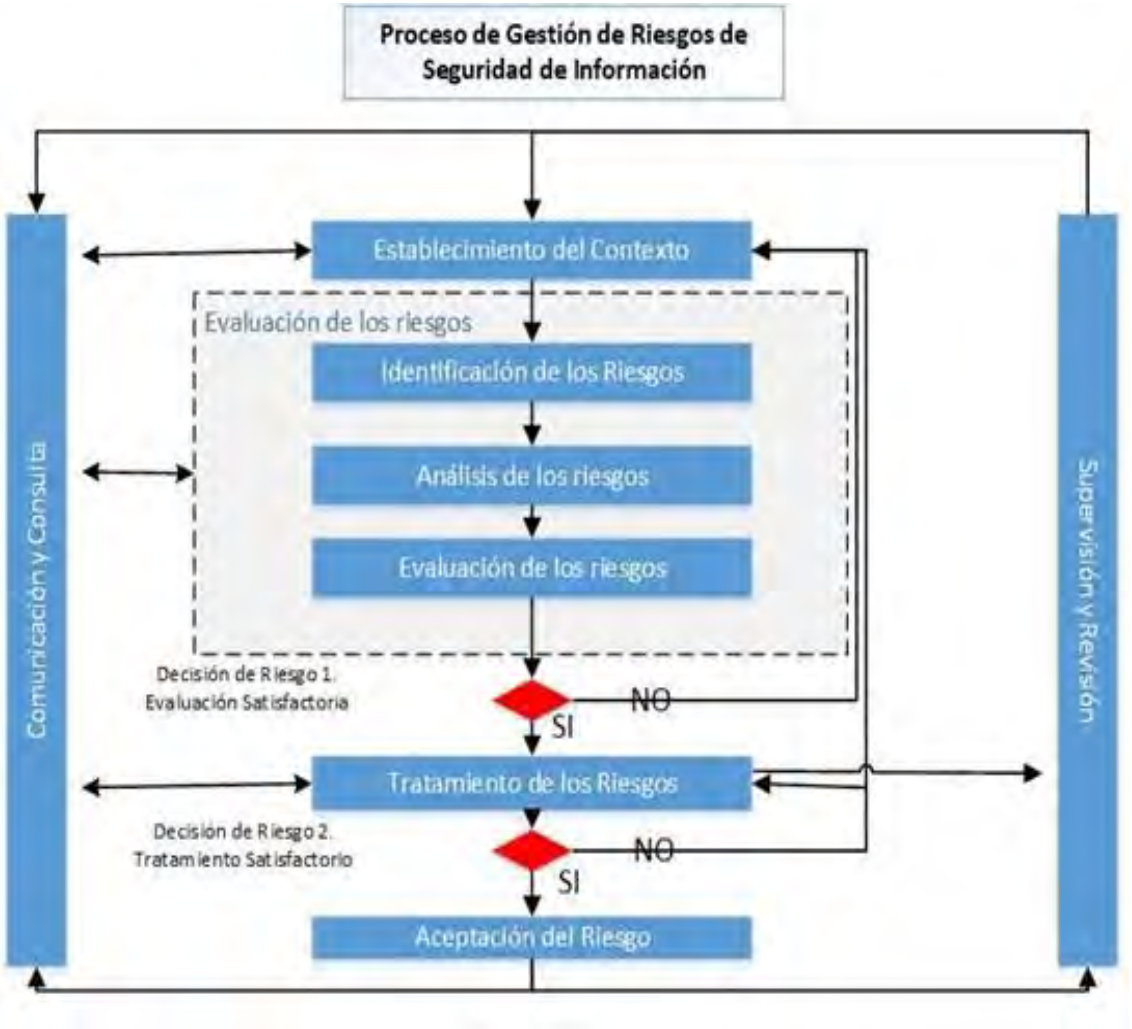
En esta etapa se identificaron los riesgos de los activos de información que puedan afectar con un impacto negativo sobre la confidencialidad, integridad y disponibilidad de los mismos en la Municipalidad Distrital de Chamaca. El análisis de los riesgos de seguridad de información se inicia con el cuestionamiento de lo que puede fallar a causa de las amenazas que pueden explotar en vulnerabilidades de los activos y la consecuencia de la falla. El enfoque metodológico de la etapa de análisis de riesgos de seguridad de información

1. Identificar amenazas.
2. Identificar vulnerabilidades
3. Identificar controles de riesgo

3.4.6 Visión general para administración del riesgo de seguridad de la información

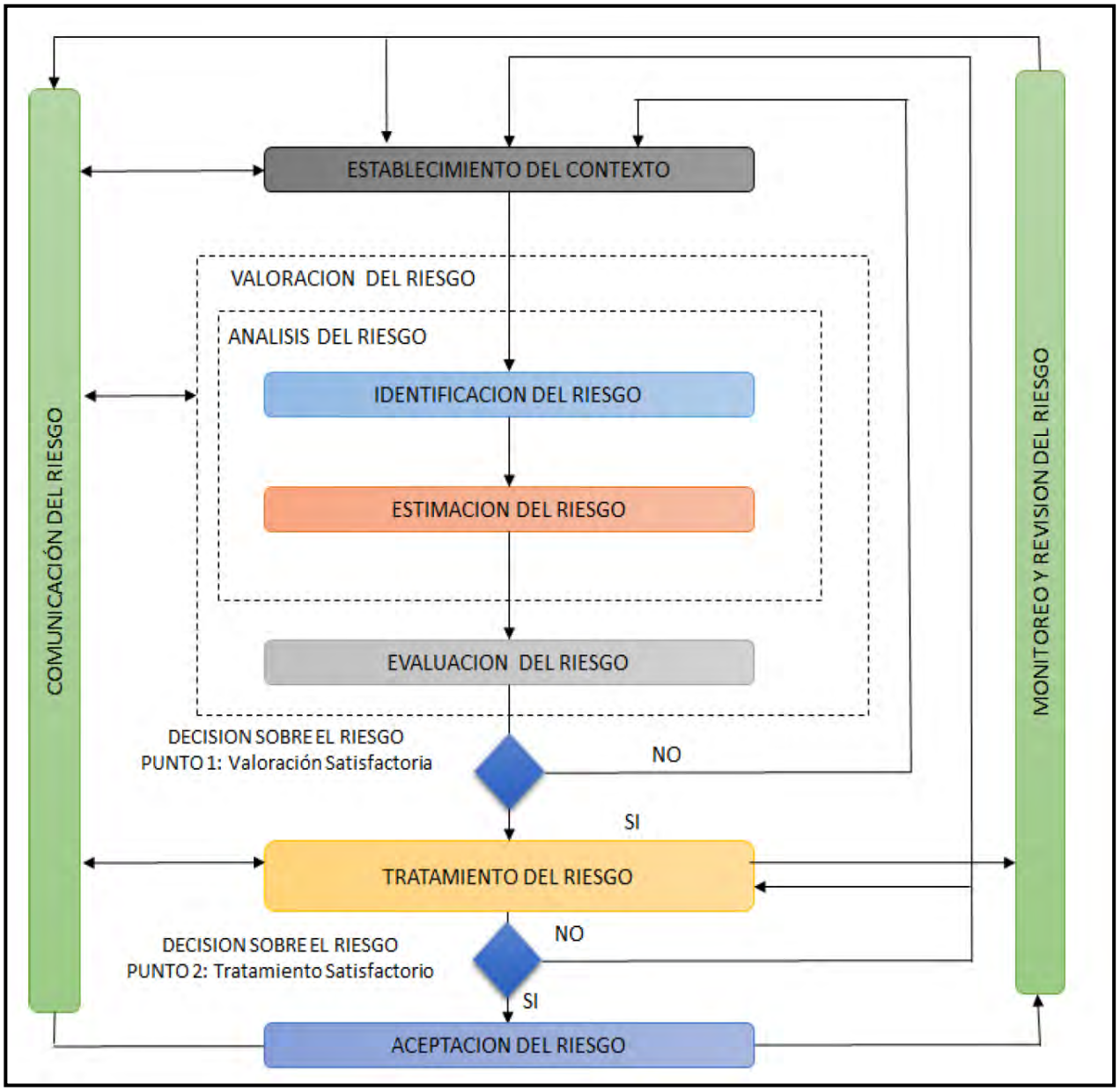
Según (MINTIC, 2016) El proceso de gestión de riesgo en la seguridad de la información consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento. Proceso para la administración del riesgo:

Figura 14. Diagrama del proceso de gestión de riesgos.



Fuente: https://www.hkmexico.com/wp-content/uploads/Fig-1.jpg

Figura 15. Visión de proceso de riesgo en seguridad de la información



Fuente: Tomado de la norma ISO/IEC 27005.

La siguiente tabla resume las actividades de gestión del riesgo en la seguridad de la información que son pertinentes para las cuatro fases del proceso de elaboración del Sistema de Gestión de Seguridad de Información en la Municipalidad Distrital de Chamaca

Tabla 16: Procesos de gestión de riesgos a lo largo del SGSI

ETAPAS DEL SGSI	PROCESO DE GESTION DEL RIESGO EN LA SEGURIDAD DE LA INFORMACION
Planear	• Establecer Contexto • Valoración del Riesgo • Planificación del Tratamiento del Riesgo • Aceptación del Riesgo
Implementar	• Implementación del Plan de Tratamiento de Riesgo
Gestionar	• Monitoreo y Revisión Continuo de los Riesgos
Mejora Continua	• Mantener y Mejorar el Proceso de Gestión del Riesgo en la Seguridad de la Información.

Fuente: Elaboración propia

3.4.7 Criterios básicos de riesgos de seguridad de información en la Municipalidad Distrital de Chamaca

Los criterios de evaluación de riesgos según (MINTIC, 2016) Se recomienda desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo en la seguridad de la información de la organización teniendo en cuenta los siguientes aspectos

- El valor estratégico del proceso de información para la entidad
- La criticidad de los activos de información involucrados en el proceso
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales

- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

3.4.8 Criterios de impacto.

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, considerando los siguientes aspectos:

- Nivel de clasificación de los activos de información del proceso.
- Brechas en la seguridad de la información (ejemplo: perdidas de confidencialidad, integridad y disponibilidad de la información)
- Operaciones deterioradas
- Perdida del negocio y del valor financiero
- Alteración de planes y fechas limites
- Daños para la reputación
- Incumplimiento de los requisitos legales.

3.4.9 Criterios de aceptación del riesgo

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la organización y de las partes interesadas. La organización debería definir sus propias escalas para los niveles de aceptación del riesgo. Durante el desarrollo, se deberían considerar los siguientes aspectos:

- Los criterios de aceptación del riesgo pueden incluir umbrales múltiples, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado
- Los diferentes criterios de aceptación del riesgo pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos si esto se especifica como un requisito contractual

Los criterios de aceptación del riesgo pueden diferir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos:

- Criterios del negocio
- Aspectos legales y reglamentarios
- Operaciones
- Tecnología
- Finanzas

3.4.10 Valoración de riesgos en la MDCH.

El riesgo de un activo de información corresponde al nivel de riesgos sin considerar los controles existentes o planificados para disminuir la frecuencia. El valor de la frecuencia se estima mediante el valor la frecuencia el cálculo del promedio del valor de la frecuencia de la vulnerabilidad y el valor de la amenaza.

Tabla 17: Lista de riesgos analizados en la Municipalidad Distrital de Chamaca.

Matriz de Riesgo						
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**
R1	Hardware	Mantenimiento insuficiente	Ruptura de la mantenibilidad del sistema de información	Posible	Menor	Moderado
R2	Hardware	Falta de esquema de reemplazo periódicos	Destrucción de equipos o medio	Improbable	Moderado	Moderado
R3	Hardware	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento	Posible	Moderado	Alto
R4	Hardware	Susceptibilidad a variaciones de voltaje	Pérdida del suministro eléctrico	Probable	Menor	Alto
R5	Hardware	Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico	Probable	Insignificante	Moderado
R6	Hardware	Almacenamiento no protegido	Robo de medios	Probable	Moderado	Alto
R7	Hardware	Falta de cuidado al descartarlo	Robo de medios	Probable	Moderado	Alto
R8	Hardware	Copia no controlada	Robo de medios	Probable	Menor	Alto
R9	Software	Errores conocidos en el software	Abuso de derechos	Probable	Insignificante	Moderado
R10	Software	No hacer “logout” (cerrar sesión)	Abuso de derechos	Casi Seguro	Menor	Alto
R11	Software	Software ampliamente distribuido	Corrupción de datos	Raro	Moderado	Moderado
R12	Software	Asignación equivocada de derechos de acceso	Abuso de derechos	Improbable	Mayor	Alto
R13	Software	Falta de documentación	Error en uso	Posible	Menor	Moderado

Matriz de Riesgo						
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**
R14	Software	Mala administración de claves	Falsificación de datos	Probable	Moderado	Alto
R15	Software	Falta de copias de respaldo	Adulteración del software	Probable	Moderado	Alto
R16	Software	Líneas de comunicación no protegidas	Intercepción	Posible	Menor	Moderado
R17	Software	Pruebas al software inexistentes o insuficientes	Abuso de derechos	Raro	Moderado	Moderado
R18	Software	Punto de falla único	Falla del equipo de telecomunicaciones	Improbable	Menor	Bajo
R19	Red	Arquitectura de red insegura	Espionaje remoto	Improbable	Moderado	Moderado
R20	Red	Transferencia de contraseñas autorizadas	Espionaje remoto	Probable	Moderado	Alto
R21	Red	Gestión inadecuada de la red	Saturación del sistema de información	Probable	Menor	Alto
R22	Red	Conexión de red pública sin protección	Uso no autorizado del equipo	Posible	Menor	Moderado
R23	Personal	Ausencia de personal	Ruptura de la disponibilidad del personal	Raro	Moderado	Moderado
R24	Personal	Procedimientos inadecuados de contratación	Destrucción de equipos o medio	Probable	Moderado	Alto
R25	Personal	Capacitación insuficiente en seguridad	Error en el uso	Probable	Insignificante	Moderado
R26	Personal	Uso incorrecto de Software y Hardware	Error en el uso	Posible	Menor	Moderado
R27	Personal	Falta de conciencia de seguridad	Error en el uso	Probable	Menor	Alto

Matriz de Riesgo						
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**
R28	Sitio	Uso inadecuado o descuido del control de acceso a las edificaciones o recintos	Inundación	Casi Seguro	Menor	Alto
R29	Sitio	Red inestable de energía eléctrica	Perdida de suministro eléctrico	Probable	Moderado	Alto
R30	Sitio	Falta de protección física del edificio puertas y ventanas.	Robo de equipos	Probable	Moderado	Alto

Fuente: Elaboración propia

Una vez realizado el análisis y evaluación de riesgo en base a los criterios de aceptación de riesgos, se debe decidir cuales acciones se han de tomar con los riesgos priorizados, las opciones de tratamiento.

3.5 Fase Check: Verificar los controles de la propuesta del SGSI

La fase "Check" del ciclo Deming en el contexto de la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI) en la Municipalidad Distrital de Chamaca, implica la evaluación y verificación de las actividades implementadas durante la fase "Do". Aquí se describen algunas acciones específicas que podrían llevarse a cabo durante la fase de "Check" en el SGSI de una municipalidad:

3.5.1 Auditorías Internas:

Realizar auditorías internas periódicas para evaluar la efectividad de los controles de seguridad implementados. Verificar el cumplimiento de las políticas y procedimientos de seguridad de la información.

3.5.1.1 Definición de objetivos:

Establece claramente los objetivos de la auditoría interna. Por ejemplo, pueden querer evaluar la conformidad con normas específicas (como NTP ISO/IEC 27001: 2014), identificar áreas de mejora, o asegurarte de que se están considerando todos los aspectos relevantes de la seguridad de la información.

3.5.1.2 Evaluación de riesgos:

Evalúa la identificación y análisis de riesgos. Asegúrate de que se hayan identificado todos los riesgos relevantes para la organización y que se hayan establecido controles adecuados para mitigarlos.

3.5.1.3 Revisión de controles:

Verificar la implementación de los controles de seguridad propuestos. Asegurándose que los controles sean apropiados para los riesgos identificados y que estén alineados con las mejores prácticas de seguridad.

3.5.1.4 Pruebas de funcionalidad:

Se deber realizar pruebas de funcionalidad de los controles y procesos de seguridad. Esto podría incluir simulacros de incidentes de seguridad para evaluar la capacidad de respuesta del SGSI.

3.5.1.5 Informe de auditoría:

Elaborar un informe detallado que destaque los hallazgos de la auditoría, incluyendo áreas de cumplimiento, áreas de mejora y recomendaciones específicas. Asegúrate de proporcionar una evaluación equilibrada y objetiva.

3.5.1.6 Seguimiento y mejora continua:

Después de la auditoría, realiza un seguimiento de la implementación de las recomendaciones y verifica la mejora continua del SGSI. Esto garantizará que el sistema evolucione para abordar los desafíos cambiantes de seguridad de la información.

3.5.2 Monitorización de incidentes:

Analizar incidentes de seguridad ocurridos durante la fase "Do" y evaluar la respuesta y gestión de estos incidentes. Identificar patrones o tendencias en los incidentes para mejorar las medidas preventivas. respuesta rápida y mitigación de posibles amenazas y violaciones de seguridad en la propuesta del Sistema de Gestión de Seguridad de la Información (SGSI). Aquí hay algunas acciones clave que puedes llevar a cabo como parte de la monitorización de incidentes:

1. Registro de Eventos
2. Análisis de Vulnerabilidades
3. Configuración de Alertas
4. Supervisión de Tráfico de Red
5. Análisis de Malware
6. Supervisión de Accesos no Autorizados
7. Revisión de Actualizaciones de Seguridad

8. Monitoreo de Cuentas de Usuario

3.5.3 Conformidad legal y normativa:

Verificar la conformidad del SGSI con los requisitos legales y normativos aplicables a la municipalidad. Actualizar y ajustar políticas y procedimientos para cumplir con cambios en la normativa.

3.5.4 Revisión de vulnerabilidades:

Evaluar la efectividad de las medidas de seguridad para abordar las vulnerabilidades identificadas durante la fase de planificación.

Realizar pruebas de vulnerabilidad y analizar los resultados para realizar mejoras.

3.5.5 Recolección y análisis de datos:

Recopilar datos relacionados con el rendimiento del SGSI, incidentes de seguridad y otras métricas relevantes. Analizar datos para identificar áreas de mejora y tomar decisiones informadas.

3.5.6 Retroalimentación de los usuarios:

Obtener retroalimentación de los usuarios y partes interesadas en relación con la seguridad de la información. Utilizar la retroalimentación para realizar ajustes y mejoras en la implementación de la propuesta del SGSI.

3.6 Fase Actuar: monitorear

La fase "Actuar" del ciclo PDCA es crucial para cerrar el ciclo de mejora continua y garantizar que la propuesta del SGSI se adapte y evolucione en respuesta a los cambios en las amenazas y en el entorno de seguridad de la información

3.6.1 Recopilación de datos:

Analizar los datos recopilados durante la fase de "Verificar". Esto incluye información sobre incidentes, auditorías internas, pruebas de seguridad y cualquier otra métrica relacionada con la seguridad de la información.

3.6.2 Evaluación de resultados:

Evaluar los resultados obtenidos durante la fase de "Verificar" en comparación con los objetivos y metas establecidos en la fase de "Planificar". Determinar si se han alcanzado los resultados esperados.

3.6.3 Generación de soluciones:

Desarrollar soluciones y planes de acción basados en el análisis de datos y en la identificación de causas raíz. Estas soluciones deben abordar las áreas de mejora identificadas durante la fase de "Verificar".

3.6.4 Implementación de acciones:

Llevar a cabo la implementación de las acciones correctivas y preventivas planificadas. Esto puede incluir actualizaciones de políticas, procedimientos, capacitación del personal, mejoras en la tecnología, etc.

1. Realizar auditorías internas y revisiones periódicas para evaluar el cumplimiento de las políticas de seguridad y la efectividad de los controles implementados.
2. Implementar herramientas de monitoreo continuo para detectar comportamientos y actividades inusuales en la red y sistemas, y responder proactivamente a posibles amenazas.

3. Revisar regularmente las políticas y procedimientos de seguridad, y ajustarlos según sea necesario. Buscar constantemente oportunidades para mejorar la postura de seguridad de la información.
4. Colaborar con otras municipalidades, entidades gubernamentales y organizaciones para compartir información sobre amenazas y mejores prácticas de seguridad.

3.6.5 Comunicación interna:

Comunicar de manera efectiva los cambios y mejoras a todo el personal relevante. Asegurar que todos estén informados sobre las actualizaciones en las políticas y procedimientos de seguridad.

3.6.6 Capacitación y concientización:

Proporcionar capacitación y concienciación al personal sobre las nuevas medidas de seguridad implementadas. Asegurar que comprendan su papel y responsabilidad en la seguridad de la información. Se debe realizar un recorrido por las normas ISO que refuerzan esa implementación de la norma ISO 27001 enfocada a las buenas prácticas referentes a los controles y protección de datos para los servicios de los proveedores y trabajadores.

3.6.6.1 Sesiones iniciales de concientización

Impartir sesiones introductorias para sensibilizar al personal sobre la importancia de la seguridad de la información. Explicar las posibles amenazas y el impacto que podrían tener en la organización.

3.6.6.2 Políticas y procedimientos:

Detallar las políticas y procedimientos de seguridad de la información. Asegurarse de que el personal comprenda y cumpla con las políticas establecidas para proteger los activos de información.

3.6.6.3 Uso Seguro de contraseñas:

Enseñar buenas prácticas para la creación y gestión de contraseñas seguras. Destacar la importancia de no compartir contraseñas y la necesidad de cambiarlas regularmente.

3.6.6.4 Identificación de amenazas comunes:

Capacitar al personal en la identificación de amenazas comunes, como ataques de phishing, malware y ataques de ingeniería social. Proporcionar ejemplos prácticos para mejorar la conciencia.

3.6.6.5 Uso Seguro de dispositivos móviles:

Brindar pautas para el uso seguro de dispositivos móviles, incluyendo la instalación de aplicaciones solo desde fuentes confiables y la configuración de funciones de seguridad, como bloqueo remoto.

3.6.6.6 Seguridad en redes y Wi-Fi:

Proporcionar orientación sobre cómo utilizar redes y Wi-Fi de manera segura. Incluir prácticas para evitar la conexión a redes no seguras y el uso de VPN cuando sea necesario.

3.6.6.7 Protección contra ransomware:

Educar sobre las medidas preventivas contra ransomware, como no hacer clic en enlaces sospechosos y no abrir archivos adjuntos de fuentes no confiables.

3.6.6.8 Respuesta a incidentes:

Proporcionar información sobre los pasos a seguir en caso de incidentes de seguridad. Asegurarse de que el personal sepa cómo informar incidentes y colaborar en la respuesta.

3.6.6.9 Evaluaciones y pruebas de conocimientos:

Realizar evaluaciones periódicas para medir la comprensión del personal sobre las prácticas de seguridad de la información. Esto puede incluir cuestionarios, simulacros y actividades prácticas.

3.6.6.10 Actualizaciones continuas:

Mantener al personal actualizado sobre las últimas amenazas y técnicas de ataque. Organizar sesiones de actualización periódicas para garantizar que estén al tanto de las tendencias actuales en seguridad de la información.

3.6.6.11 Simulacros de phishing:

Realizar simulacros de phishing para entrenar al personal en la identificación de correos electrónicos fraudulentos y reforzar la conciencia de seguridad.

3.6.6.12 Monitoreo continuo:

Implementar un sistema de monitoreo continuo para evaluar la efectividad de las acciones implementadas. Esto podría incluir la revisión regular de métricas clave y la realización de auditorías internas.

3.6.6.13 Revisión de documentación:

Actualizar la documentación del SGSI, incluyendo políticas, procedimientos y registros, para reflejar los cambios realizados durante la fase "Actuar".

3.6.6.14 Preparación para la próxima iteración:

Prepararse para el próximo ciclo PDCA. Reflexionar sobre lo aprendido y considerar cómo se puede aplicar la mejora continua en futuras iteraciones del SGSI.

Capítulo IV
Análisis de los requisitos de la NTP ISO/IEC 2700:2014

CAPÍTULO IV

4 ANÁLISIS DEL ISO 27001:2014 EN LA MDCH.

4.1 Análisis de requisitos del ISO 27001:2014 en la MDCH.

En esta fase se presentan las actividades que se realizaron para conocer la situación de la Municipalidad Distrital de Chamaca, frente a la seguridad de la información.

Los resultados obtenidos en la situación actual sobre la seguridad de la información ayudan a la Municipalidad Distrital de Chamaca en la implementación del Sistema de Gestión de Seguridad de Información con la Norma Técnica Peruana ISO/IEC 27001:2014, que mitigan las vulnerabilidades y pérdidas de la información importantes que ha ocurrido hasta el momento.

Con el fin de verificar la seguridad de la información en la MDCH, se realizó una encuesta a una parte de los trabajadores y también se visualizó todos los terminales tecnológicos donde se tiene información importante como: Presupuesto, Subgerencia de Desarrollo Social, Sub gerencia de Medio Ambiente, Tesorería, Logística, recursos humanos, secretaria.

4.2 Cumplimiento de los requisitos de la NTP ISO/IEC 27001:2014 en el SGSI

Según la (NTP-ISO/IEC 27001, 2014) Esta Norma Técnica Peruana ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo.

El sistema de gestión de la seguridad de información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente. Es importante que el sistema de gestión de la seguridad de la información sea parte y esté integrado con los procesos de la organización y la estructura de gestión general y que la seguridad de la información se considere en el diseño de procesos, sistemas y controles de la información. Se espera que la implementación de un sistema de gestión de seguridad de la información crezca a escala en concordancia con las necesidades de la organización.

4.2.1 Objeto y campo de aplicación del SGSI.

Esta Norma Técnica Peruana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información en la Municipalidad Distrital de Chamaca, dentro del contexto de la organización. Esta Norma Técnica Peruana también incluye requisitos para la evaluación y tratamiento de los riesgos de seguridad de la información orientados a las necesidades de la Municipalidad. Los requisitos establecidos en esta Norma Técnica Peruana son genéricos y están hechos para aplicarse a todas las organizaciones.

4.2.2 Referencias normativas

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. Para referencias fechadas sólo se aplica la edición citada. Para referencias no fechadas se aplica la edición más reciente del documento referenciado (incluida cualquier enmienda). ISO/IEC 27000.

Base legal

- Constitución política del Perú.
- Ley N° 27972 ley organica de Municipalidades.
- Ley 27444 ley de Procedimiento Administrativo General y sus modificatorias.
- Decreto Supremo N° 033-2005-PCM, Reglamento de Codigo de Etica de la Funcion Pública.
- Resolución Ministerial n°004-2016-PCM, Aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 27001:2014, Tecnología de Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2da edición en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución N° 000- 2020-mdch resolución que aprueba la implementación del Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Chamaca.

4.2.3 Términos y definiciones

Para propósitos de este documento, se aplican los términos y definiciones proporcionados en ISO/IEC 27000.

4.2.4 Contexto de la organización

4.2.4.1 Comprender la organización y su contexto

La Municipalidad Distrital de Chamaca debe determinar los aspectos externos e internos que son relevantes para este propósito y que afectan su capacidad de lograr el(los) resultado(s) deseados de este sistema de gestión de seguridad de la información.

4.2.4.2 Comprender las necesidades y expectativas de las partes interesadas

La organización debe determinar:

a) las partes interesadas relevantes al sistema de gestión de seguridad de la información.

b) los requisitos de estas partes interesadas relevantes a la seguridad de la información.

4.2.4.3 Determinar el alcance del sistema de gestión de seguridad de la información

La Municipalidad Distrital de Chamaca debe determinar los límites y la aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.

Cuando se determina este alcance la organización debe considerar:

a) los aspectos externos e internos referidos en 5.2. 4.1.

b) los requisitos referidos en 5.2.4.2.

c) las interfaces y dependencias entre actividades realizadas por la organización y las que son realizadas por otras organizaciones.

4.2.4.4 Sistema de gestión de seguridad de la información

La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, en conformidad con los requisitos de esta Norma Técnica Peruana.

4.2.5 Liderazgo

4.2.5.1 Liderazgo y compromiso

La alta dirección de la Municipalidad Distrital de Chamaaca debe demostrar liderazgo y compromiso respecto del sistema de gestión de seguridad de la información:

a) Asegurando que la política de seguridad de la información y los objetivos de seguridad de la información son establecidos y compatibles con la dirección estratégica de la organización;

b) Asegurando la integración de los requisitos del sistema de gestión de seguridad de la información en los procesos de la organización;

c) Asegurando que los recursos necesarios para el sistema de gestión de seguridad de la información estén disponibles;

d) Comunicando la importancia de una efectiva gestión de seguridad de la información y en conformidad con los requisitos del sistema de gestión de seguridad de la información;

e) Asegurando que el sistema de gestión de seguridad de la información logre su(s) resultado(s) previsto(s);

f) Dirigiendo y apoyando a las personas para que contribuyan con la efectividad del sistema de gestión de seguridad de la información;

g) Promoviendo la mejora continua.

h) Apoyando a otros roles relevantes de gestión para demostrar su liderazgo tal como se aplica a sus áreas de responsabilidad.

4.2.5.2 Políticas

La alta dirección de la Municipalidad Distrital de Chamaca debe establecer una política de seguridad de la información que:

a) Es apropiada al propósito de la organización;

b) Incluye objetivos de seguridad de la información o proporciona el marco de referencia para fijar los objetivos de seguridad de la información;

c) Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información.

d) Incluye un compromiso de mejora continua del sistema de gestión de seguridad de la información.

e) Estar disponible como información documentada.

f) Estar comunicada dentro de la organización.

g) Estar disponible a las partes interesadas, según sea apropiado.

4.2.5.3 Roles, responsabilidades y autoridades organizacionales

La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas.

La alta dirección debe asignar la responsabilidad y la autoridad para:

a) Asegurar que el sistema de gestión de seguridad de la información esté conforme a los requisitos de esta Norma Técnica Peruana; y

b) Reportar sobre el desempeño del sistema de gestión de seguridad de la información a la alta dirección.

4.2.6 Planificación

4.2.6.1 Acciones para tratar los riesgos y las oportunidades

A) Generalidades

Cuando se planifica para el sistema de gestión de seguridad de la información, la organización debe considerar los asuntos referidos en el numeral 5,2,4,1 y los requisitos

referidos en el numeral 5.2.4.2 y determinar los riesgos y oportunidades que necesitan ser tratados para:

a) Asegurar que el sistema de gestión de seguridad de la información pueda lograr su(s) resultado(s) esperado(s);

b) Prevenir, o reducir, efectos indeseados.

c) Lograr la mejora continua. La organización debe planificar:

B) Valoración del riesgo de Seguridad de la Información

La Municipalidad Distrital de Chamaca debe definir y aplicar un proceso de valoración del riesgo de seguridad de la información que:

a) Establezca y mantenga criterios de riesgo de seguridad de la información que incluyan.

b) Asegure que las valoraciones repetidas de riesgos de seguridad de la información produzcan resultados consistentes, válidos y comparables.

c) Identifique los riesgos de seguridad de la información

d) Analice los riesgos de seguridad de la información.

e) Evalúe los riesgos de seguridad de la información.

C) Tratamiento de riesgos de seguridad de información

La organización debe definir y aplicar un proceso de tratamiento de riesgos de seguridad de la información para:

a) Seleccionar opciones de tratamiento de riesgos de seguridad de la información apropiadas, tomando en cuenta los resultados de la valoración de riesgos.

b) Determinar todos los controles que son necesarios para implementar la(s) opción(es) elegida(s) de tratamiento de riesgos de seguridad de la información.

D) Objetivos de seguridad de la información y planificación para conseguirlos

La organización debe establecer objetivos de seguridad de la información a niveles y funciones relevantes.

Los objetivos de seguridad de la información deben:

a) Ser consistentes con la política de seguridad de la información.

b) Ser medibles (si es práctico).

c) Tomar en cuenta requisitos aplicables de seguridad de la información y resultados de la valoración y tratamiento de riesgos.

d) Ser comunicados.

e) Ser actualizados según sea apropiado.

4.2.7 Soporte

4.2.7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información.

4.2.7.2 Competencia

La organización debe:

a) Determinar la competencia necesaria de las personas que trabajan bajo su control que afecta su desempeño en seguridad de la información.

b) Asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados.

c) Cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y evaluar la efectividad de las acciones tomadas.

d) Retener información documentada apropiada como evidencia de competencia.

4.2.7.3 Concientización

Las personas que trabajan bajo el control de la organización deben ser conscientes de:

a) la política de seguridad de información;

b) su contribución a la efectividad del sistema de gestión de seguridad de la información, incluyendo los beneficios de un mejor desempeño de la seguridad de la información; y

c) las implicancias de no tener conformidad con los requisitos del sistema de gestión de seguridad de la información.

4.2.7.4 Comunicación

La organización debe determinar la necesidad de comunicaciones internas y externas relevantes al sistema de gestión de seguridad de la información incluyendo:

a) Qué comunicar.

b) Cuándo comunicar.

c) A quién comunicar.

d) Quién debe comunicar.

e) Los procesos por los cuales la comunicación debe ser efectuada.

4.2.7.5 Información documentada

El sistema de gestión de seguridad de la información de la organización debe incluir:

a) Información documentada requerida por esta Norma Técnica Peruana.

b) Información documentada determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.

4.2.8 Planificación y control operacional

La Municipalidad Distrital de Chamaca debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas. La organización debe también implementar planes para lograr los objetivos de seguridad de la información determinados.

La Municipalidad Distrital de Chamaca debe mantener información documentada en la medida necesaria para estar segura de que los procesos se han llevado a cabo tal como fueron planificados.

La Municipalidad Distrital de Chamaca debe controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario. La organización debe asegurar que los procesos tercerizados son determinados y controlados.

4.2.8.1 Evaluación de riesgos de seguridad de la información

La Municipalidad Distrital de Chamaca debe realizar evaluaciones de riesgos de seguridad de la información en intervalos planificados o cuando cambios significativos se propongan u ocurran, tomando en cuenta los criterios establecidos.

La organización debe retener información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información.

4.2.8.2 Tratamiento de riesgos de seguridad de la información

La Municipalidad Distrital de Chamaca debe implementar el plan de tratamiento de riesgos de seguridad de la información.

La organización debe retener información documentada de los resultados del tratamiento de riesgos de seguridad de la información.

4.2.9 Evaluación del desempeño

4.2.9.1 Monitoreo, medición, análisis y evaluación

La Municipalidad Distrital de Chamaca debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información.

La organización debe determinar:

a) Qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información.

b) Los métodos para monitoreo, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos.

c) Cuándo el monitoreo y medición debe ser realizado.

d) Quién debe monitorear y medir.

e) Cuándo los resultados del monitoreo y medición deben ser analizados y evaluados.

f) Quién debe analizar y evaluar estos resultados.

4.2.9.2 Auditoría interna

La Municipalidad Distrital de Chamaca debe conducir auditorías internas en intervalos planificados para proporcionar información sobre si el sistema de gestión de seguridad de la información:

a) Está en conformidad con:

1) Los requisitos de la propia organización para su sistema de gestión de seguridad de la información.

2) Los requisitos de esta Norma Técnica Peruana;

b) Está efectivamente implementado y mantenido.

La organización debe:

c) Planificar, establecer, implementar y mantener uno o varios programas de auditoría, incluyendo la frecuencia, métodos, responsabilidades, requisitos e informes de planificación. Los programas de auditoría deben tomar en consideración la importancia de los procesos concernientes y los resultados de auditorías previas.

d) Definir los criterios y el alcance de cada auditoría.

e) Seleccionar a los auditores y conducir auditorías que aseguren objetividad e imparcialidad del proceso de auditoría.

4.2.10 Mejoras.

4.2.10.1 No conformidades y acción correctiva

Cuando ocurre la no conformidad, la Municipalidad Distrital de Chamaca debe:

a) Reaccionar a la no conformidad y, según sea aplicable:

1) Tomar acción para controlarla y corregirla.

2) Ocuparse de las consecuencias.

b) Evaluar la necesidad de la acción para eliminar las causas de la no conformidad con el fin de que no recurra u ocurra en otro lugar de las siguientes maneras:

1) Revisando la no conformidad.

2) Determinando las causas de la no conformidad.

3) Determinando si existen no conformidades similares o si podrían ocurrir Potencialmente.

c) Implementar cualquier acción necesaria.

d) Revisar la efectividad de cualquier acción correctiva tomada.

e) hacer cambios al sistema de gestión de seguridad de la información, si fuera necesario.

f) La naturaleza de las no conformidades y cualquier acción subsiguiente tomada.

g) Los resultados de cualquier acción correctiva.

4.2.10.2 Mejora continua

La Municipalidad debe mejorar continuamente la conveniencia, adecuación y efectividad de la propuesta del sistema de gestión de seguridad de la información.

4.2.11 Resultados del tratamiento de los riesgos

Una vez realizado el análisis y evaluación de riesgo en base a los criterios de aceptación de riesgos, se debe decidir cuales acciones se han de tomar con los riesgos priorizados.

En el presente trabajo de investigación se estableció que a los niveles alto y extremo se aplicaran controles, que ayuden a reducir el riesgo producido por las amenazas a un nivel aceptable.

Se priorizó el tratamiento de riesgos del nivel alto, aplicará de manera urgente las medidas de seguridad. Así mismo el nivel moderado y bajo serán monitoreados para el tratamiento se presenta la siguiente tabla.

Tabla 18: Acciones frente a los riesgos

Medida Frente al riesgo	
Aceptar	Aceptar la posibilidad que pueda ocurrir el riesgo sin tomar medidas de acción concretas.
Mitigar	Mitigar el impacto o la probabilidad de ocurrencia mediante la implementación de un control de seguridad de información.
Evitar	Eliminar la fuente del proceso que genera la amenaza, se utiliza cuando el nivel de riesgo es alto, la actividad del proceso o sistema que lo genera no es de gran impacto.
Transferir	Transferir el impacto de riesgo a terceros. Se utiliza cuando no se puede mitigar la probabilidad de ocurrencia de un riesgo.

Fuente: Elaboración propia

4.2.12 Controles de Seguridad de Información bajo la NTP ISO/IEC 27001:2014

Se determinaron los controles que ayudarán a reducir los riesgos a un nivel aceptable. Se detallan en la tabla 18, los controles para reducir los riesgos. Finalmente se elaboró la declaración de aplicabilidad cual incluye todos los controles identificados. Este documento puede ser estudiado en el ANEXO N° 06 del presente trabajo de investigación

Tabla 19: Controles de seguridad de información en la MDCH

CONTROLES PARA EL TRATAMIENTO DE RIESGO										
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**	**Jerarquía de Control**	**Control Especifico**	**Control Alineado al ISO 27002:2013**	**Responsable**
R3	Hardware	Susceptibilidad a la humedad, al polvo y a la suciedad	Polvo, corrosión, congelamiento	Posible	Moderado	Alto	Mitigar	11 seguridad física y ambiental (anexo 8)	11.2.4 Mantenimiento de equipos (anexo 8)	Jefe de área de Informática
R5	Hardware	Falta de control eficiente del cambio de configuración	Error en el uso	Probable	Moderado	Alto	Mitigar	12 seguridad Operativa (anexo 10)	12.1.2 Gestión de cambios (anexo 10)	Jefe de área Informática
R6	Hardware	Susceptibilidad a variaciones de voltaje	Pérdida del suministro eléctrico	Probable	Menor	Alto	Mitigar	11 seguridad física (anexo 9)	11.1.4 Protección contra las amenazas (anexo9)	Soporte Técnico / Mantenimiento
R8	Hardware	Almacenamiento no protegido	Robo de medios	Probable	Moderado	Alto	Mitigar	12 seguridad Operativa (anexo 10)	12.3.1 Copia de seguridad de la información (anexo 10)	Administrador de servidores BD
R9	Hardware	Falta de cuidado al descartarlo	Robo de medios	Probable	Moderado	Alto	Mitigar	8 gestión de activos anexo 11	8.3.1 Gestión de soporte extraíbles anexo 11	Jefe de área Informática
R10	Hardware	Copia no controlada	Robo de medios	Probable	Menor	Alto	Mitigar	8 gestión de activos anexo11	12.5.1 Control de Software en explotación	Jefe de área Informática
R12	Software	No hacer “logout” cuando se sale de las estaciones de trabajo	Abuso de derechos	Casi Seguro	Menor	Alto	Mitigar	9 control de Acceso Anexo12	9.4.2 Procedimiento seguro de inicio de sesión anexo12	Jefe de área Informática
R14	Software	Asignación equivocada de derechos de acceso	Abuso de derechos	Improbable	Mayor	Alto	Mitigar	9 control de Acceso Anexo12	9.2.2 Gestión de los derechos acceso asignado a usuario Anexo12	Jefe de área Informática

CONTROLES PARA EL TRATAMIENTO DE RIESGO										
Id de Riesgo	**Activo**	**Vulnerabilidad**	**Amenaza**	**Posible Amenaza**	**Impacto**	**Nivel de Riesgo**	**Jerarquía de Control**	**Control Especifico**	**Control Alineado al ISO 27002:2013**	**Responsable**
R17	Software	Mala administración de claves	Falsificación de datos	Probable	Moderado	Alto	Mitigar	9 control de Acceso Anexo13	9.4.3 Gestión de Contraseña de usuarios anexo13	Jefe de área de Informática
R19	Software	Falta de copias de respaldo	Adulteración del software	Probable	Moderado	Alto	Mitigar	12 seguridad Operativa	12.3.1 Copia de seguridad de la información	Jefe de área de Informática
R25	Red	Transferencia de contraseñas autorizadas	Espionaje remoto	Probable	Moderado	Alto	Mitigar	13 seguridad en las telecomunicaciones 9 Control de Acceso Anexo13	13.1.2 Mecanismo de seguridad asociados a servicios en red. Anexo12	Jefe de área Informática
R26	Red	Gestión inadecuada de la red	Saturación del sistema de información	Probable	Menor	Alto	Mitigar	13 seguridad en las telecomunicaciones Anexo12	13.1.1 Controles de red Anexo12	Jefe de área de Informática
R29	Personal	Procedimientos inadecuados de contratación	Daños a los equipos o medios	Probable	Moderado	Alto	Mitigar	8 gestión de activos Anexo11	8.3.2 Eliminación de soporte Anexo11	Jefe de área de Informática

Fuente: Elaboración propia

Una vez realizado el análisis de riesgos de acceso a la información luego se dio con la interpretación de controles a los riesgos de nivel alto como se muestra en la tabla 21, el área de informática de la MDCH es encargado de realizar los tratamientos adecuados para un correcto control de los riesgos de acceso a la información en la Municipalidad Distrital de Chamaca.

Capítulo V
Resultados

CAPÍTULO V

5 RESULTADOS DE LA EVALUACIÓN

5.1 Con respecto a las encuestas aplicadas en la MDCH

Según la evaluación realizada, de un total de 100% de los encuestados se obtuvo los resultados de la tabla anterior donde muestra también que la seguridad de la Información dentro de la institución no es segura y que la propuesta del SGSI implicará un mayor esfuerzo, y dependerá del compromiso y disponibilidad del personal de la MDCH.

Se muestra el resultado del análisis de todas las respuestas con el porcentaje de aprobación por parte de cada uno de los encuestados a los trabajadores de la MDCH con los siguientes cuadros muestran los resultados.

5.2 Resultados del análisis de riesgos de activos de información en los terminales tecnológicos de la MDCH.

5.3 Interpretación de datos

En la encuesta realizada por cada respuesta seleccionada se puso un puntaje según el siguiente cuadro.

Tabla 20: Puntaje de las respuestas

Respuestas	Puntaje	Detalle
Si	2	Esta alternativa nos indica que el terminal tecnológico fue implementado sobre seguridad de la información y la vulnerabilidad minimizará muy significativamente
Parcialmente	1	Esta respuesta nos indica que tiene implementada algunas de los controles de la seguridad de la información quieren decir que está en mejora
No	0	Quiere decir que en el terminal tecnológico no se implementó la seguridad de la información y la vulnerabilidad de la información es muy alta

Fuente: Elaboración propia

NOTA: Adaptado al proyecto "Modelo De Gestión De Seguridad De La Información Con ISO/IEC 27001 Para Minimizar La Vulnerabilidad De La Información En La Municipalidad Distrital De Santa María De Chicmo, Andahuaylas 2018" (Ancco & Yuver, 2018)

Puntaje obtenido de aplicación del Sistema de Gestión de Seguridad de la Información para minimizar de la vulnerabilidad de la información con ISO/IEC 27001 en la Municipalidad Distrital de Chamaca, Chumbivilcas, Cusco 2020 - 2021, donde.

T= Terminal tecnológico de la municipalidad

N= Número de pregunta

P= Puntajes

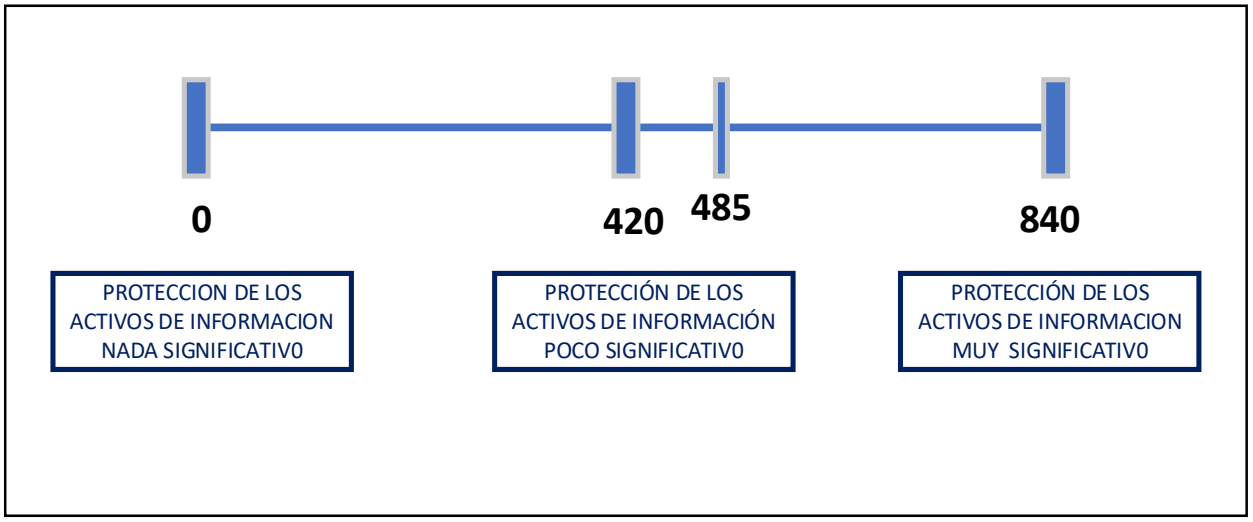
En la siguiente tabla se muestran los resultados de la encuesta realizada a los trabajadores de la Municipalidad distrital de Chamaca:

Tabla 21: Resultados de la aplicación de la encuesta en la MDCH

RESULTADOS DE LA APLICACIÓN DE LA ENCUESTA A LA MDCH																							
DIMENSONES	**PROTECCION DE LOS ACTIVOS DE INFORMACIÓN**										**P**	**RIESGOS DE ACCESO A LA INFORMACIÓN DE LA MDCH**										**P**	**P**
TERMINAL	1	2	3	4	5	6	7	8	9	10		11	12	13	14	15	16	17	18	19	20		PUNT TOTAL
T1-RR.HH	1	2	1	2	2	2	2	2	1	0	15	1	1	1	0	0	2	0	2	1	1	9	24
T2-PROCUR	2	2	1	2	2	2	2	2	1	0	16	0	2	2	2	2	2	2	2	0	1	15	31
T3-DSOCIAL	1	0	2	1	2	2	2	1	2	0	13	0	0	0	1	1	2	1	0	1	1	7	20
T4-CONTA	1	2	2	2	2	2	2	1	1	0	15	0	1	1	0	1	2	0	1	0	0	6	21
T5-LOGISTI	0	1	2	2	2	2	2	2	2	0	15	2	2	2	2	2	2	1	2	0	1	16	31
T6-OPMI	0	1	2	2	2	2	2	1	0	0	12	0	0	2	0	0	2	1	2	0	1	8	20
T7-INFRAES	2	2	2	1	2	2	2	2	2	0	17	2	1	2	2	2	2	2	2	1	1	17	34
T8-DES ECON	2	2	2	2	2	2	2	0	2	2	18	2	2	2	2	2	0	2	2	2	2	18	36
T9-PRESUP	0	1	2	2	2	2	2	1	1	0	13	0	0	0	1	1	1	2	2	0	1	8	21
T10-DEMUN	1	2	1	2	1	2	1	2	2	1	15	1	1	2	2	2	1	2	1	0	0	12	27
T11-ATM	0	0	1	2	2	1	2	1	1	0	10	1	0	1	0	1	0	1	1	0	0	5	15
T12-ALCALD	0	1	0	2	2	1	2	1	1	0	10	0	0	0	1	1	0	0	1	0	1	4	14
T13-ARCHIV	0	1	1	0	1	2	2	1	0	0	8	0	1	0	0	1	1	0	2	0	0	5	13
T14-SUPERV	0	1	2	2	2	2	2	1	1	0	13	1	0	0	0	1	1	1	0	0	0	4	17
T15-RENTAS	0	1	1	2	2	2	2	0	1	0	11	1	1	2	1	1	1	1	1	0	1	10	21
T16-SECRET	1	2	2	2	2	2	2	1	1	1	16	2	0	0	0	1	1	1	2	1	2	10	26
T17-OBRAS	0	0	2	2	2	2	1	2	1	0	12	1	0	1	1	0	1	0	2	2	1	9	21
T18-INFOR	0	2	2	2	2	2	0	2	1	0	13	2	2	2	0	1	2	0	2	2	2	15	28
T19-ABASTEC	2	2	2	2	2	2	2	2	2	0	18	0	1	2	0	0	0	1	1	1	1	7	25
T20-TESOR	0	0	1	2	2	2	2	2	1	0	12	0	1	1	2	1	2	0	2	1	0	10	22
T21-MAQUI	0	0	2	2	2	1	2	1	0	0	10	0	1	1	1	1	0	0	2	1	1	8	18
	PUNTAJE										282	PUNTAJE										203	485

Fuente: Elaboración propia

Figura 16. Nivel de seguridad ante la aplicación del SGSI



Fuente: Elaboración propia

El nivel de seguridad de la información en la figura 16, que O (cero) puntos obtenidas demuestra que los terminales tecnológicos no tendrían implementado la seguridad de la información para la protección de los activos de información entonces el riesgo de los activos de información es muy alta, mientras si obtenemos 420 puntos, este puntaje nos indica que los terminales del grupo experimental demuestran que se implementó algunos controles sobre la seguridad de la información, el puntaje máximo que podemos obtener es de 840 puntos, en la cual el terminal tecnológico tendría implementado todos los controles propuestos de la seguridad de la información, por lo tanto los riesgos de perder información sería muy mínimo, en este caso en la encuesta se obtuvo un puntaje de 485 puntos el cual nos indica que la seguridad de los activos de información en la Municipalidad Distrital de Chamaca está encima de poco significativo y los riesgos de acceso a la información sería considerable de acuerdo a la encuesta que aplicamos en la Municipalidad Distrital de Chamaca.

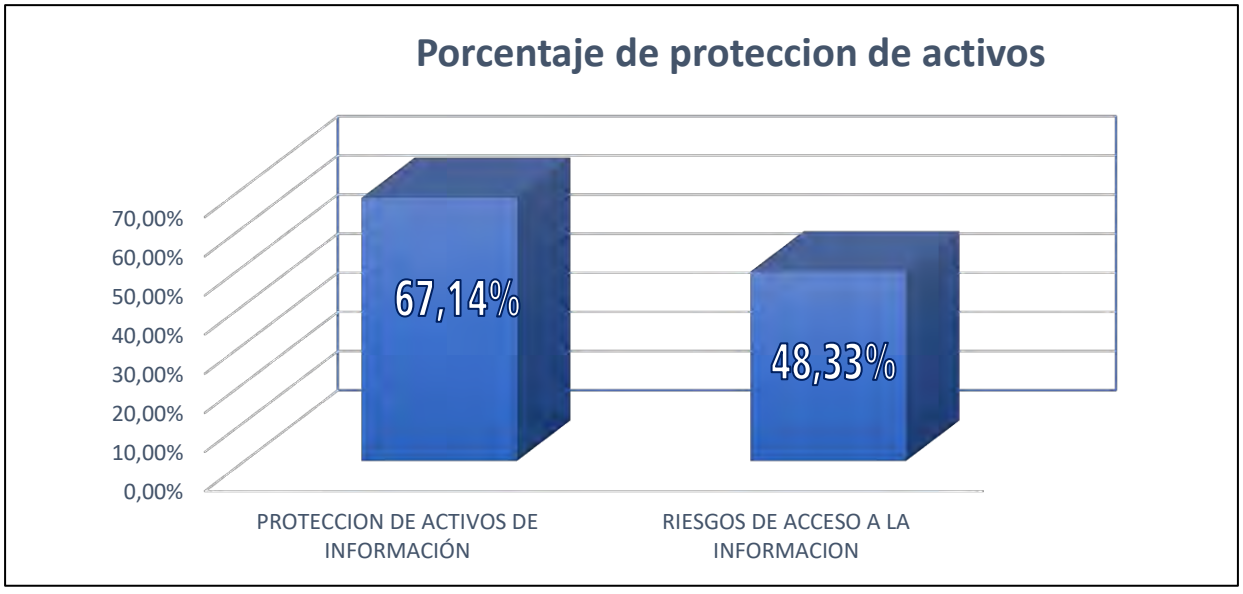
Tabla 22: Verificación de porcentaje de los activos de información

DIMENSIONES	PUNTAJE	PORCENTAJE
PROTECCION DE ACTIVOS DE INFORMACIÓN	282	67,14%
RIESGOS DE ACCESO A LA INFORMACION	203	48,33%
TOTAL	482	

Fuente: Elaboración propia

INTERPRETACION: En la tabla 21; se observa que, la variación de la protección de los activos de información es de 67,14 %, quiere decir que protección de los activos de información no es muy significativo, la variación de los riesgos de acceso a la información es de 48,33% lo que quiere decir es muy vulnerable el acceso a la información en la Municipalidad Distrital de Chamaca y que la protección de la información no es muy significativo para todos los que laboran en la Municipalidad Distrital de Chamaca.

Figura 17. Porcentaje de Protección de Activos y riesgos de información en la MDCH



Fuente: Elaboración Propia

5.4 Resultados de las encuestas

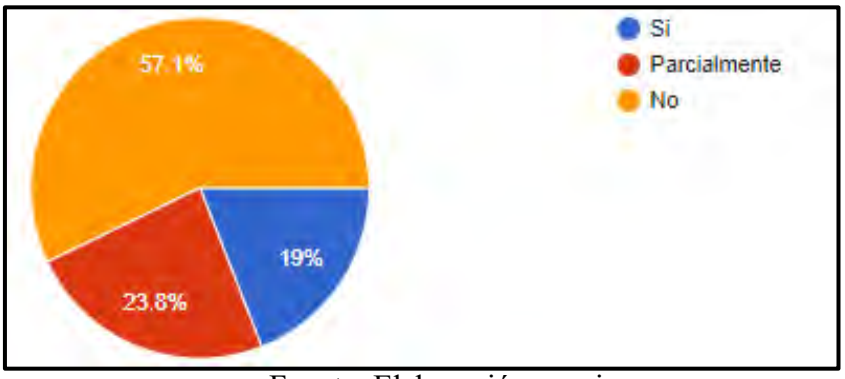
La recolección de datos se realizó mediante la encuesta mostrada en el Anexo (7) de esta investigación. La encuesta consistió en veinticuatro (24) preguntas para medir actitudes, opiniones respecto a la protección de los activos de información y el estado básico de los riesgos de acceso a la información y los activos disponibles en la Municipalidad Distrital de Chamaca. Esto con el fin de corroborar el estado de la seguridad de los activos de información y la posibilidad de aceptación de la propuesta del SGSI.

5.4.1 Existencia de un SGSI en la Municipalidad Distrital de Chamaca.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Tiene conocimiento si en la Municipalidad Distrital de Chamaca existe un Sistema de Gestión de Seguridad de la Información?

Figura 18. Encuestados saben de la existencia de un SGSI en la MDCH.



Fuente: Elaboración propia

Interpretación Del gráfico anterior, se observa que, de los 21 trabajadores encuestados, el 57,1% afirma que no tienen conocimiento que exista un Sistema de Gestión de Seguridad de

Información en la MDCH, el 19% afirma que tiene conocimiento respecto a un SGSI y el 23,8% conoce parcialmente un SGSI dentro de la Municipalidad Distrital de Chamaca.

Conclusión:

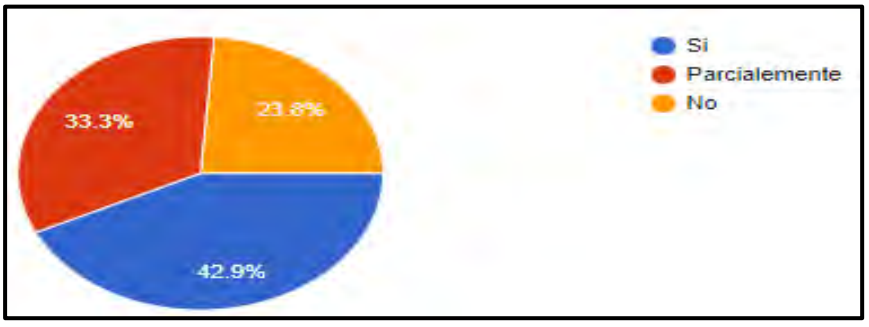
La Municipalidad Distrital de Chamaca en coordinación con la oficina de Informática (área responsable de la seguridad de la información dentro de la MDCH), requiere con urgencia el diseño e implementación de un SGSI, para levantar las no conformidades, producto del oficio Múltiple D00037-2022-PCM, que exige la implementación del Sistema de Gestión de Seguridad de Información con la NTP ISO/IEC: 27001:2014.

5.4.2 Tiene conocimiento sobre un Sistema de Gestión de Seguridad de la Información

Se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Tiene conocimiento sobre un Sistema de Gestión de Seguridad de la Información?

Figura 19. Encuestados que tienen conocimiento que es un SGSI



Fuente: Elaboración propia

Interpretación: Del gráfico anterior, se observa que, de los 21 trabajadores encuestados, el 42,9% afirma que, si tiene conocimiento respecto a un Sistema de Gestión de Seguridad de

Información, el 23,8% afirma que no tiene conocimiento respecto a un SGSI y el 33,8% conoce parcialmente un Sistema de Gestión de Seguridad de Información.

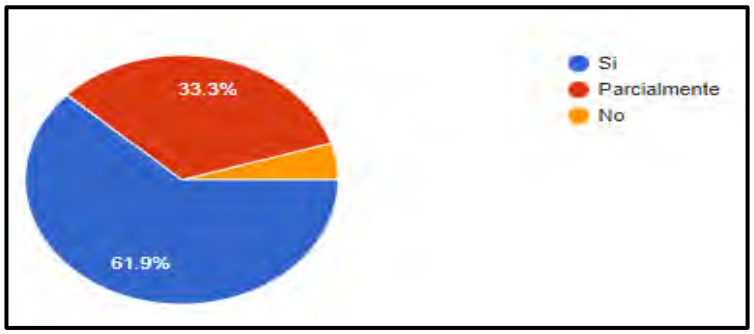
Conclusión:

La Municipalidad Distrital de Chamaca en coordinación con la oficina de Informática (área responsable de la seguridad de la información dentro de la MDCH), requiere con urgencia el diseño e implementación de un SGSI, para levantar las no conformidades, producto del oficio Múltiple D00037-2022-PCM, que exige la implementación del SGSI en la MDCH.

5.4.3 Implementado un SGSI mejorará la seguridad de información de la MDCH.

Se muestra el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca. Para la pregunta, ¿Cree usted que implementado un SGSI mejorará la seguridad de información de su área de trabajo de la Municipalidad Distrital de Chamaca?

Figura 20. Encuestados que afirman que mejorará la seguridad información con un SGSI



Fuente: Elaboración propia

Interpretación: En la figura 20, se observa que, de los 21 trabajadores encuestados, el 61,9% afirma que con la Implementación de un SGSI mejorará bastante la seguridad de los activos de información en la MDCH, el 33,3% afirma que mejorará parcialmente la seguridad de

información que tiene la MDCH con la implementación de SGSI y 4,8% afirma que no mejorará la seguridad de los activos de información implementación un SGSI en la Municipalidad Distrital de Chamaca.

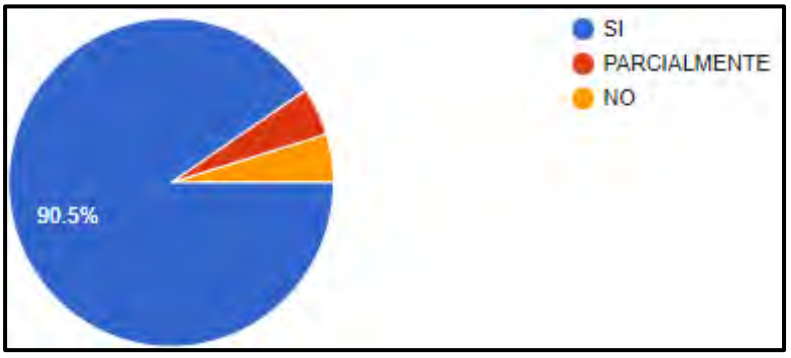
Conclusión:

La Municipalidad Distrital de Chamaca en coordinación con la oficina de Informática (área responsable de la seguridad de la información dentro de la MDCH), requiere con urgencia el diseño e implementación de un SGSI, para levantar las no conformidades, producto del oficio Múltiple D00037-2022-PCM, que exige la implementación del Sistema de Gestión de Seguridad de Información con la NTP ISO/IEC: 27001:2014.

5.4.4 Aprobación para la implementación del SGSI en la MDCH

Para la pregunta, ¿Aprobaría usted la implementación del SGSI en la Municipalidad Distrital de Chamaca? La frecuencia de respuesta fue la siguiente:

Figura 21. Encuestados que aprueban la implementación del SGSI en la MDCH



Fuente: Elaboración propia

Interpretación: En la Figura 21, se puede observar que el 90,5% de los encuestados están de acuerdo con implementación de un SGSI en la Municipalidad Distrital de Chamaca.

Conclusión: Se puede concluir que todos los trabajadores de MDCH son conscientes del beneficio que traerá la implementación de un Sistema de Gestión de Seguridad de la Información.

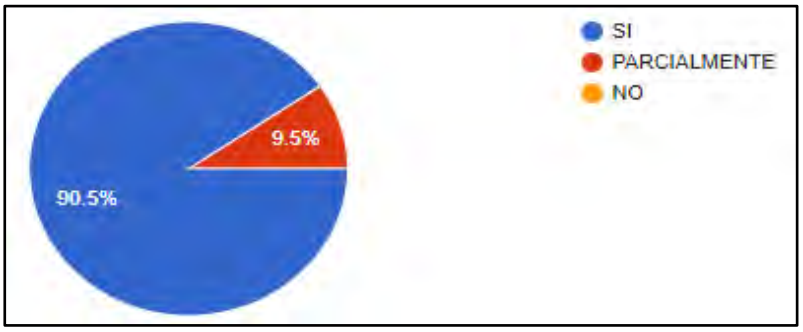
5.4.5 Se logrará un cambio positivo con la aplicación del SGSI.

A continuación, se muestra la figura 21 el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Cree Ud. que en la Municipalidad Distrital de Chamaca se logrará un cambio positivo con la implementación de este SGSI?

La frecuencia de respuesta fue la siguiente:

Figura 22. Encuestados que indican que el SGSI logrará un cambio positivo en la MDCH



Fuente: Elaboración propia.

Interpretación:

En la Figura 22, se puede observar que el 90,5% de los encuestados afirman que logrará grandes cambios positivos para la seguridad de los activos de información con la implementación de un SGSI y 9,5% afirma que mejorará parcialmente la seguridad de información.

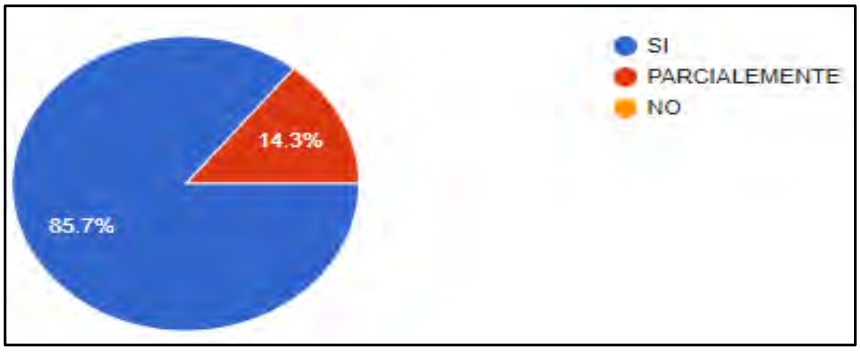
Conclusión: Se puede concluir que todos los trabajadores de la Municipalidad Distrital de Chamaca son conscientes del beneficio que traerá la implementación de un sistema de gestión de seguridad de la información que genera grandes cambios positivos para MDCH.

5.4.6 Considera que existe información que debe ser protegida en la MDCH.

A continuación, se muestra la figura 22 el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Considera Ud. que en la Municipalidad Distrital de Chamaca y su area de trabajo existe información que debe ser protegida?

Figura 23. Encuestados que consideran la información debe ser protegida



Fuente: Elaboración propia

Interpretación:

En la Figura 23, se puede observar que el 85,7% de los encuestados afirman que su información debe estar protegida con un SGSI están de acuerdo a la implementación de un SGSI que protege los activos de información de la MDCH.

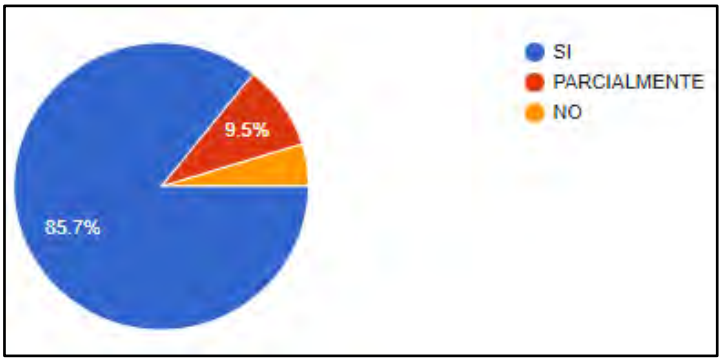
Conclusión: Se puede concluir que todos los trabajadores de la Municipalidad Distrital de Chamaca son conscientes del beneficio que traerá la implementación de un sistema de gestión de seguridad de la información que genera protección de los activos de información para la MDCH.

5.4.7 Cuenta con un computador para realizar sus funciones en la MDCH.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Cuenta con un computador para realizar sus funciones en la Municipalidad Distrital de Chamaca? La frecuencia de respuesta fue la siguiente:

Figura 24. Encuestados que cuentan con un computador para su trabajo



Fuente: Elaboración propia

Interpretación:

En la Figura 24, se puede observar que el 85,7% de los encuestados afirman que cuentan con un computador para realizar sus actividades laborales y el 9,5% indican que parcialmente cuentan con un computador para desarrollar su trabajo y el 4,8% no cuentan con un computador para desarrollar sus labores en la Municipalidad Distrital de Chamaca.

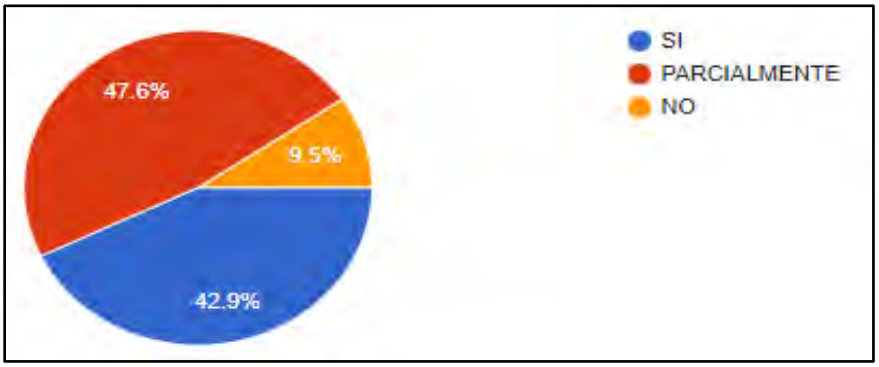
Conclusión: Se puede concluir que todos los trabajadores de la Municipalidad Distrital de Chamaca son conscientes del beneficio que traerá la implementación de un sistema de gestión de seguridad de la información con adecuado uso de un computador que genera la protección de los activos de información en la MDCH.

5.4.8 Apaga correctamente los equipos informática de su trabajo en la MDCH.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Usted apaga los equipos informáticos debidamente después de utilizarlos? La frecuencia de respuesta fue la siguiente:

Figura 25. Encuestados que apagan sus equipos informáticos correctamente



Fuente: Elaboración propia

Interpretación: En la Figura 25, se puede observar que el 42,9% de los encuestados afirman que apagan debidamente los equipos informáticos y el 47,6% indican que apagan parcialmente los equipos y el 9,5% no apagan correctamente los equipos informáticos que utilizan para desarrollar sus labores en la Municipalidad Distrital de Chamaca.

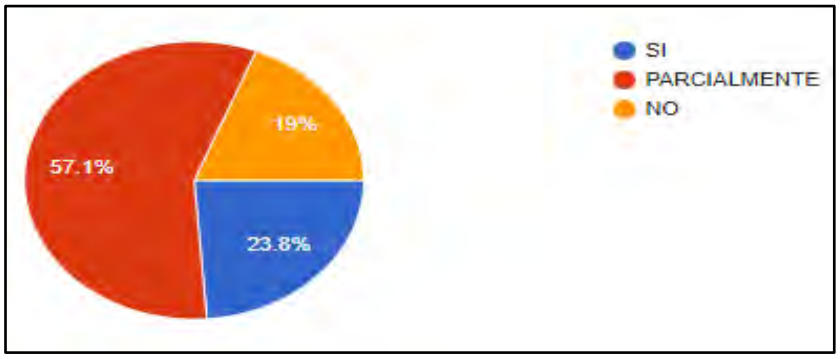
Conclusión: Se puede concluir que todos los trabajadores de la Municipalidad Distrital de Chamaca son conscientes del beneficio que traerá la implementación de un sistema de gestión de seguridad de la información con apagado adecuado de los equipos informáticos que genera la protección de los activos de información en la MDCH.

5.4.9 Seguridad de los ambientes de trabajo en la Municipalidad Distrital de Chamaca

Se muestra el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿se siente seguro en los ambientes cerca de los equipos informáticos en la Municipalidad Distrital de Chamaca?

Figura 26. Encuestados que se sientes seguros en los lugares de trabajo



Fuente: Elaboración propia

Interpretación: En la Figura 26, se puede observar que el 23,8% de los encuestados afirman que se encuentran seguros en los lugares de trabajo cerca a lo equipos informáticos, mientras el 57,1% se encuentra parcialmente seguro en lugar de trabajo y el 19% afirma que no se encuentra seguro en su lugar de trabajo frente a los equipos informáticos que se encuentran en las oficinas de la Municipalidad Distrital de Chamaca.

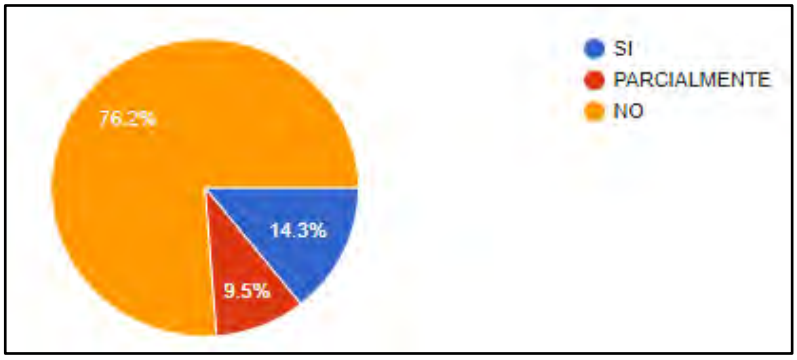
Conclusión: Se puede concluir que todos los trabajadores de la Municipalidad Distrital de Chamaca son conscientes del beneficio que traerá la implementación de un sistema de gestión de seguridad de la información.

5.4.10 Existe algún extintor cerca de los equipos informáticos

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Existe algún extinguidor cerca de los equipos informáticos de su área de trabajo en la Municipalidad Distrital de Chamaca?

Figura 27. Encuestados que cuentan con un extintor cerca a los equipos informáticos



Fuente: Elaboración propia

Interpretación: En la Figura 27, se puede observar que el 76,2% de los encuestados no cuentan con un extintor cerca a los equipos informáticos o cerca de la oficina de su trabajo mientras el 9,5% afirma que cuentan con un extintor parcialmente que se encuentran cerca a los equipos informativos y el 14,3% afirma que si cuentan con un extintor cerca a los equipos informáticos en su oficina de trabajo en la Municipalidad Distrital de Chamaca.

Conclusión:

Se puede concluir que todos los trabajadores de la Municipalidad Distrital de Chamaca son conscientes del beneficio que traerá la implementación del Sistema de Gestión de Seguridad de la Información con respecto a la importancia de usar un equipo extintor y que se ubiquen cerca a los equipos informáticos en las oficinas de la Municipalidad Distrital de Chamaca.

5.5 Resultado de encuestas respecto a riesgos de acceso a la información en la MDCH

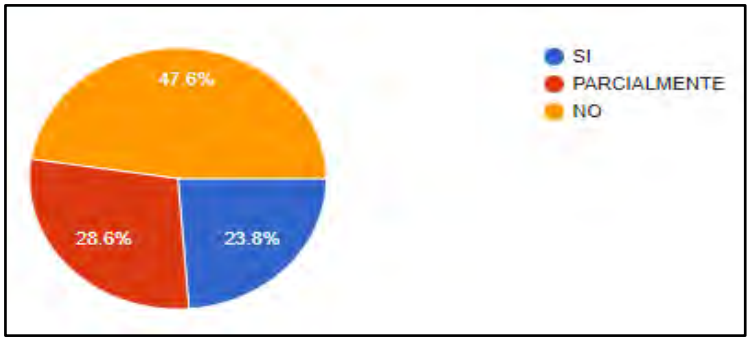
Según la evaluación realizada, de un total de 100% de los requisitos de la NTP ISO/IEC 27001:2014 que se deben cumplir, la MDCH obtuvo un puntaje total de 5%, por lo que se puede determinar que la MDCH se encuentra en una etapa básica de cumplimiento de la norma.

5.5.1 Contraseñas de acceso a los computadores tiene caracteres especiales

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Las contraseñas de acceso de usuario a las computadoras donde se tiene información vital son descifradas o combinados con caracteres especiales? La frecuencia de respuesta fue la siguiente:

Figura 28. Encuestados con usuario y contraseña para acceso a su computador



Fuente: Elaboración propia

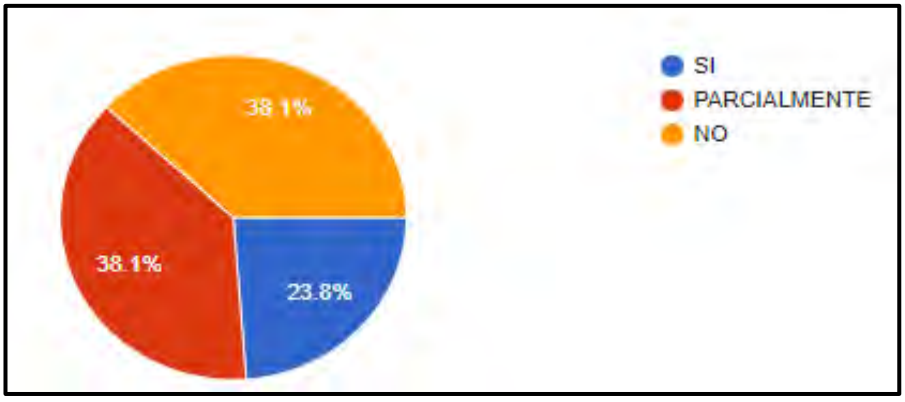
Interpretación: En la Figura 28, se puede observar que el 23.8% de los encuestados cuentan con usuario y contraseña para proteger el acceso a su computador mientras el 28,6% tienen parcialmente protegido con usuario y contraseña el acceso a su computador y el 47,8% no cuenta con usuario y contraseña para el acceso a su computador en la Municipalidad Distrital de Chamaca.

Conclusión: Se puede concluir que el 47,6% de todos los encuestados no tienen protegido con usuario y contraseña su computador por ello el riesgo de perder información es alto es por ello que se implementará un Sistema de Gestión de Seguridad de la Información para la Municipalidad Distrital de Chamaca.

5.5.2 La información está protegida contra posibles alteraciones

Para la pregunta, ¿La información que maneja en su oficina de trabajo está protegida contra posibles alteraciones por parte de personas extrañas?.

Figura 29. Encuestados que afirman posibles alteraciones de información



Fuente: Elaboración propia

Interpretación: En la Figura 29, se puede observar que el 23.8% de los encuestados afirma que si existe la posibilidad de una alteración de información por parte de personas extrañas mientras que el 38,1% menciona que parcialmente puedo ser alterada la información y el 38.1% afirma que no es posible la alteración de información que maneja en la Municipalidad Distrital de Chamaca.

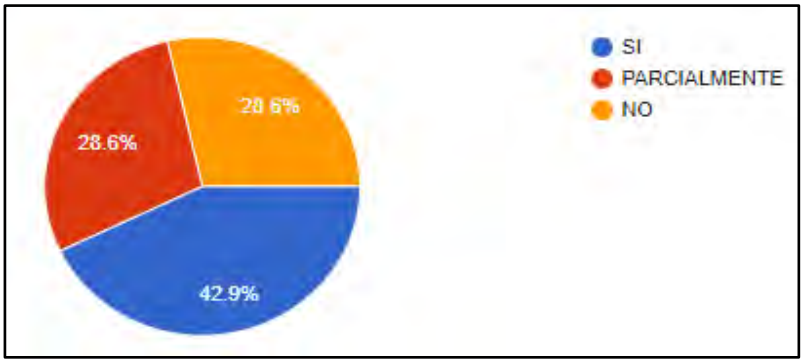
Conclusión: Se puede concluir que el mayor porcentaje de riesgo de posibles alteraciones de información por ello no cuenta con controles de acceso a la información, es por ello que se implementará un Sistema de Gestión de Seguridad de la Información para la Municipalidad Distrital de Chamaca.

5.5.3 Se restringen la instalación de otras aplicaciones o software

A continuación, se muestra en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Se restringen la instalación de otras aplicaciones o software que no sea de su trabajo en la Municipalidad Distrital de Chamaca?

Figura 30. Encuestados que indican la restricción en la instalación de otras aplicaciones



Fuente: Elaboración propia

Interpretación: En la Figura 30, se puede observar que el 42,9% de los encuestados afirman la restricción en la instalación otros aplicativos o softwares y el 28,6 % indica que no existe ninguna restricción para la instalación de otros programas o aplicativos.

Conclusión:

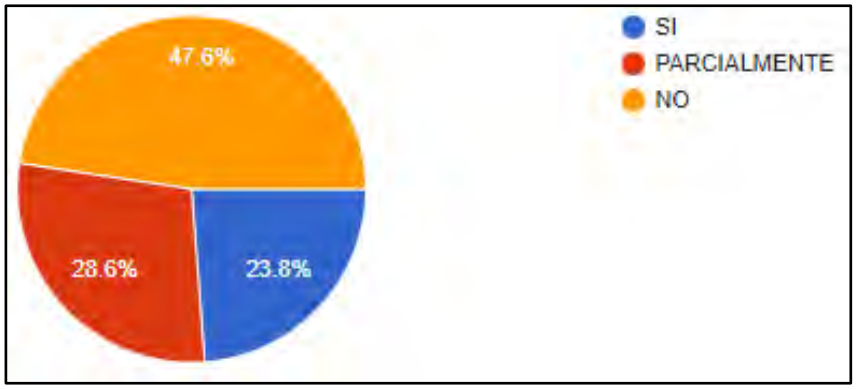
Se puede concluir que existe un riesgo en la instalación otros aplicativos o softwares que no son de uso exclusivo por ello corre el riesgo de acceso a la información y que todos los trabajadores son conscientes del beneficio que traerá el diseño de un Sistema de Gestión de Seguridad de la Información.

5.5.4 Controles de acceso al personal de la institución y público en general

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿La municipalidad Distrital de Chamaca cuenta con controles de acceso al personal de la institución y público en general?

Figura 31. Encuestados que indican sobre la existencia de control en el acceso de personal a la MDCH.



Fuente: Elaboración propia

Interpretación: En la Figura 31, se puede observar que el 23,8% de los encuestados indican si existe control de acceso al personal mientras el 28,6% indica que el control es parcialmente y el 47,6% indica que no existe control de acceso al personal al interior de la MDCH.

Conclusión:

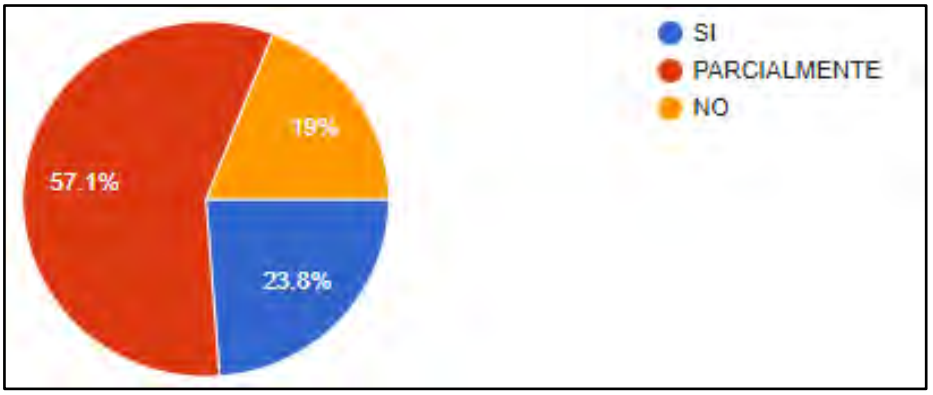
Se puede concluir que no existe los controles de acceso al personal de manera correcta por ello existe el riesgo que puedan acceder a la información de la MDCH por ello trabajadores son conscientes del beneficio que traerá la Implementación de un sistema de gestión de seguridad de la información.

5.5.5 Las puertas y ventanas de las áreas de trabajo se encuentran seguras

Para la pregunta, ¿La puerta y las ventanas de las áreas de trabajo se encuentran seguras en la Municipalidad Distrital de Chamaca?

La frecuencia de respuesta fue la siguiente:

Figura 32. Encuestados que afirman la seguridad de puertas y ventanas de la MDCH



Fuente: Elaboración propia

Interpretación:

En la Figura 32, se puede observar que el 23,8% de los encuestados indican si existe en la puertas y ventanas mientras el 57,1% indica que la seguridad es parcialmente y el 19% indica que no existe seguridad con las puertas y ventanas al interior de la MDCH.

Conclusión: Se puede concluir que existe una mínima seguridad en las puertas y ventanas por ello existe el riesgo que puedan acceder a la información de la MDCH por ello trabajadores son conscientes del beneficio que traerá la Implementación de un sistema de gestión de seguridad de la información.

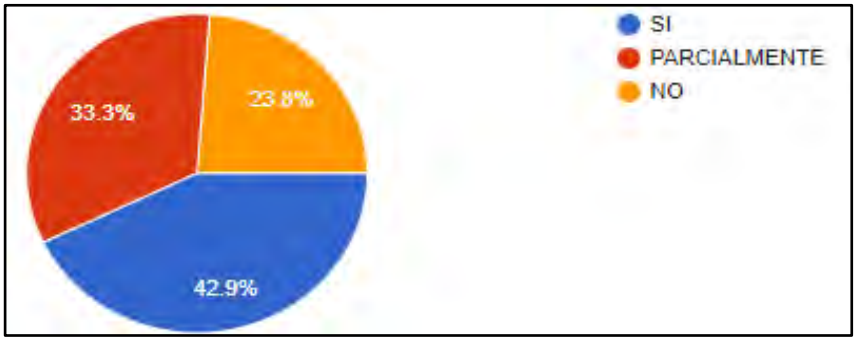
5.5.6 Si un computador presente averías, es asistido por un personal especializado

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿En caso que su computadora presente averías, es asistido por un personal especializado dentro la Municipalidad Distrital de Chamaca

La frecuencia de respuesta fue la siguiente:

Figura 33. Encuestados que son asistidos por un especialista en caso lo requieran



Fuente: Elaboración propia

Interpretación: En la Figura 33, se puede observar que el 42,9% de los encuestados indican si son asistidos por especialista en caso presente averías en su computador mientas el 33,3% refiere ser asistido por un especialista y el 23,8% indica que no es asistido por ningún especialista en el área de informática para solucionar sus problemas en su computador.

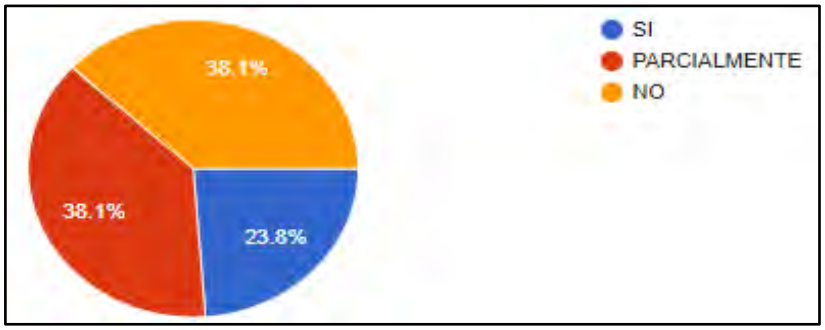
Conclusión: Se puede concluir que no hay una asistencia frecuente técnica especializa en caso exista problemas con el computador por ello existe el riesgo que puedan acceder a la información de la MDCH por ello los trabajadores son conscientes del beneficio que traerá la Implementación de un sistema de gestión de seguridad de la información.

5.5.7 Seguridad del lugar de trabajo.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿El área de trabajo está bien ubicado y seguro contra amenazas externas? Ejemplo inundaciones.

Figura 34. Encuestados que se sienten seguros en sus lugares de trabajo



Fuente: Elaboración propia

Interpretación: En la Figura 34, se puede observar que el 23,8% de los encuestados indican si se sienten seguros en los lugares de trabajo mientras que el 38,1% se sienten parcialmente seguros de los lugares de trabajo y el 38,1% no se sientes seguros de los lugares de trabajo son asistidos por especialista en caso presente averías en su computador mientas el 33,3% refiere ser asistido por un especialista y el 23,8% indica que no es asistido por ningún especialista en el área de informática.

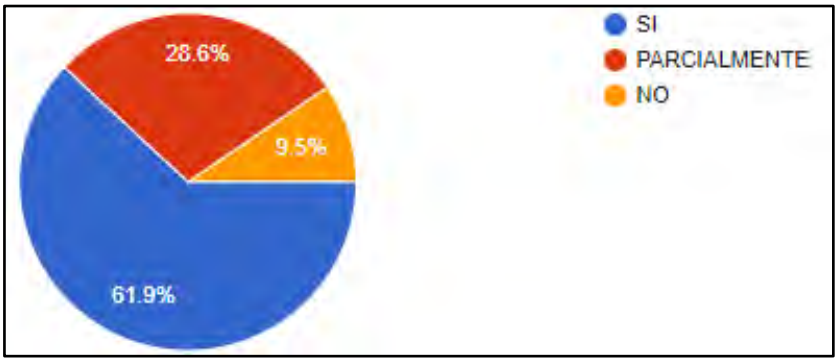
Conclusión: Se puede concluir que no hay una asistencia frecuente técnica especializa en caso exista problemas con el computador por ello existe el riesgo perder información de la MDCH.

5.5.8 Problemas de conexión de internet

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿En caso de alguna falla del internet en su computadora y/o dispositivo móvil Ud. conoce donde ir para su pronta verificación?

Figura 35. Encuestados que saben dónde recurrir en caso falle la conexión de internet



Fuente: Elaboración propia

Interpretación: En la Figura 34, se puede observar que el 61,9% de los encuestados indican si saben dónde recurrir en caso exista problemas de conexión de internet mientras el 28,6% saben parcialmente a donde acudir en los problemas de conexión de internet y el 9,5% no saben dónde acudir para solucionar los problemas de conexión de internet sus problemas en su computador.

Conclusión:

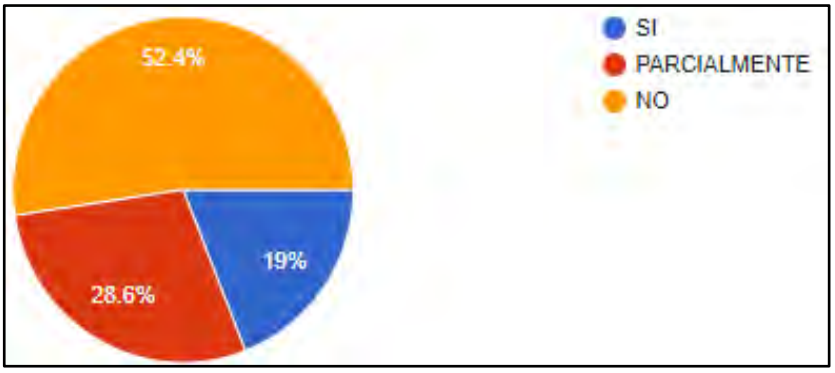
Se puede concluir que la mayoría tienen conocimiento a donde acudir en caso presente problemas de internet en su computador que vendría a ser la oficina de informática de la MDCH por ello los trabajadores son conscientes del beneficio que traerá la Implementación de un sistema de gestión de seguridad de la información

5.5.9 Se realiza mantenimiento periódico del hardware y software

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Se realiza mantenimiento periódico del hardware y software en la Municipalidad Distrital de Chamaca?

Figura 36. Encuestados que realizan el mantenimiento de hardware y software



Fuente: Elaboración propia

Interpretación:

En la Figura 35, se puede observar que el 19% de los encuestados afirman que si se realiza el mantenimiento de hardware y software periódicamente mientras el 28,6% indican que se realiza parcialmente el mantenimiento y el 52,4% indica que no se realiza el mantenimiento de hardware y software periódicamente lo que implica el riesgo de perder.

Conclusión: Se puede concluir que no se realiza el mantenimiento de hardware y software constantemente en la MDCH lo que genera gran riesgo de perder información por ello los trabajadores son conscientes del beneficio que traerá la implementación de un sistema de gestión de seguridad de la información.

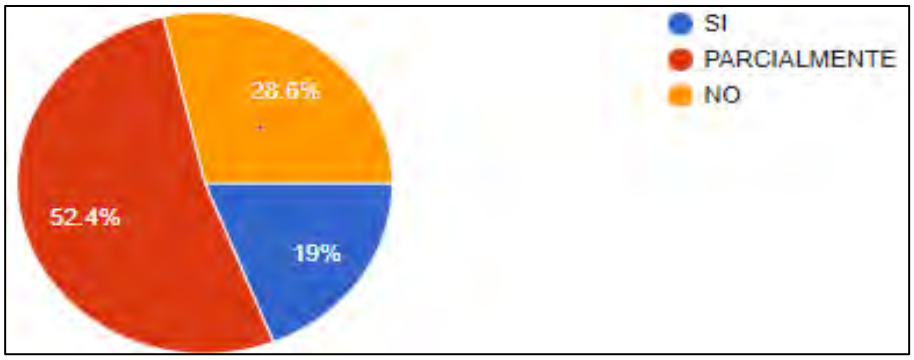
5.5.10 Se realiza copia de seguridad periódicamente de sus activos de información

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

Para la pregunta, ¿Se realiza copias de seguridad (buckup) de información que maneja en el terminal tecnológico de trabajo dentro de la Municipalidad Distrital de Chamaca?

La frecuencia de respuesta fue la siguiente:

Figura 37. Encuestados que realizan copias de seguridad de información



Fuente: Elaboración propia

Interpretación: En la Figura 36, se puede observar que el 19% de los encuestados realizan copias de seguridad de información mientras que el 52,4% realiza parcialmente las copias de seguridad y el 28,6% no realiza ninguna copia de seguridad de su información lo cual corre el riesgo de perder información, es por ello que los trabajadores están de acuerdo en que el diseño de un SGSI en la Municipalidad Distrital De Chamaca.

Conclusión:

Se puede concluir que muy pocos trabajadores realizan copias de seguridad de información de la Subgerencia de Sistemas y Tecnología son conscientes del beneficio que traerá el diseño de un sistema de gestión de seguridad de la información.

5.6 Activos de Información disponibles de la Municipalidad Distrital de Chamaca

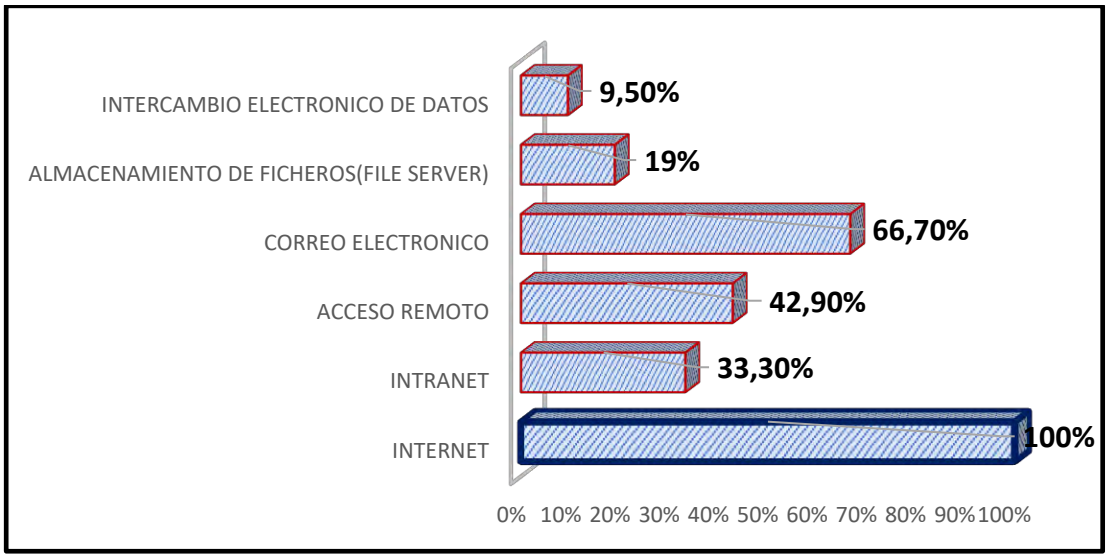
5.6.1 Activos de tipo servicio que son fundamentales para la MDCH

La recolección de datos se realizó mediante la encuesta mostrada en el Anexo 7 de esta investigación. La encuesta consistió en veinticuatro (6) preguntas para medir actitudes, opiniones y el estado básico de los riesgos de los activos de información en la Municipalidad Distrital de Chamaca. Esto con el fin de corroborar el estado de la seguridad y el riesgo de los activos de información y la posibilidad de aceptación de la implementación del SGSI.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

La frecuencia de respuesta fue la siguiente:

Figura 38. Activos de información de tipo servicio disponibles en la MDCH



Fuente: Elaboración propia.

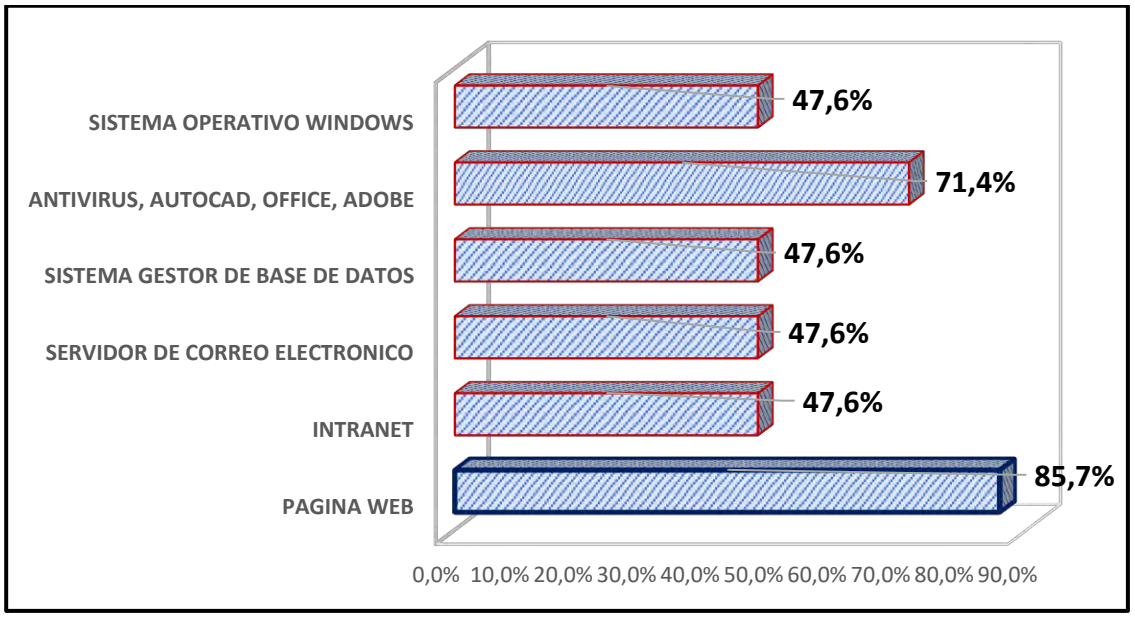
Interpretación: En el gráfico anterior, se puede observar que el activo de tipo servicio más utilizado es el internet y quiere decir que está expuesto a una mayor cantidad de riesgos de seguridad de información en la Municipalidad Distrital de Chamaca.

5.6.2 Qué activos de tipo software son fundamentales para el área de su trabajo en la Municipalidad Distrital de Chamaca

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

La frecuencia de respuesta fue la siguiente:

Figura 39. Activos de información de tipo software fundamentales



Fuente: Elaboración propia

Interpretación: En el gráfico anterior, se puede observar que el activo de tipo software más utilizado es el página web, office y antivirus, quiere decir que está expuesto a una mayor riesgo de seguridad de información en la Municipalidad Distrital de Chamaca.

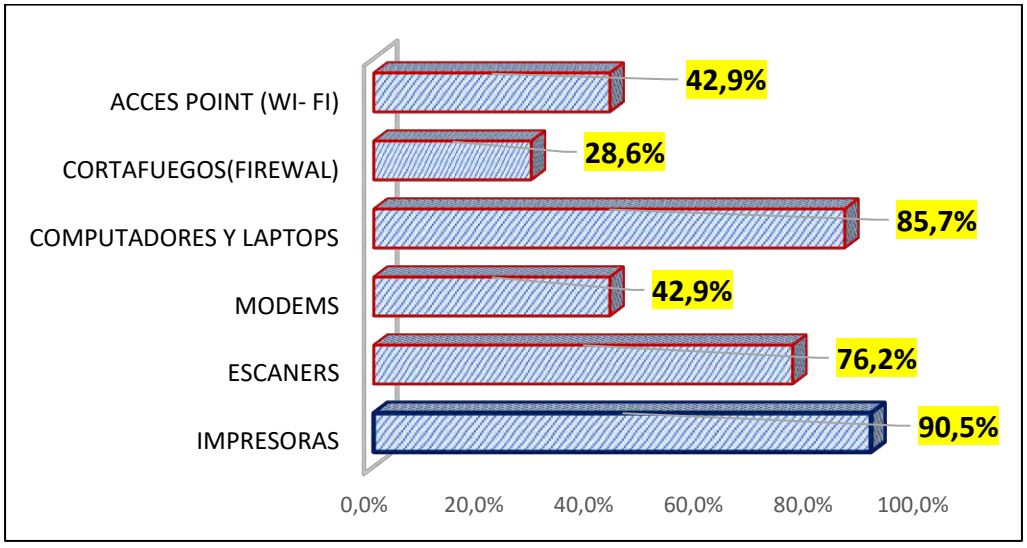
5.6.3 Activos de tipo de hardware fundamentales para el área de su trabajo dentro de la MDCH.

La recolección de datos se realizó mediante la encuesta mostrada en el Anexo 7 de esta investigación. La encuesta consistió en seis (6) preguntas para medir respecto a los activos de información de tipo hardware disponibles en la MDCH.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

La frecuencia de respuesta fue la siguiente:

Figura 40. Activos de información de tipo hardware que tiene la MDCH



Fuente: Elaboración propia

Interpretación:

En el gráfico anterior, se puede observar que el activo impresoras, computadores y laptops está expuesto a una mayor cantidad de riesgos de seguridad de Información en la Municipalidad Distrital de Chamaca.

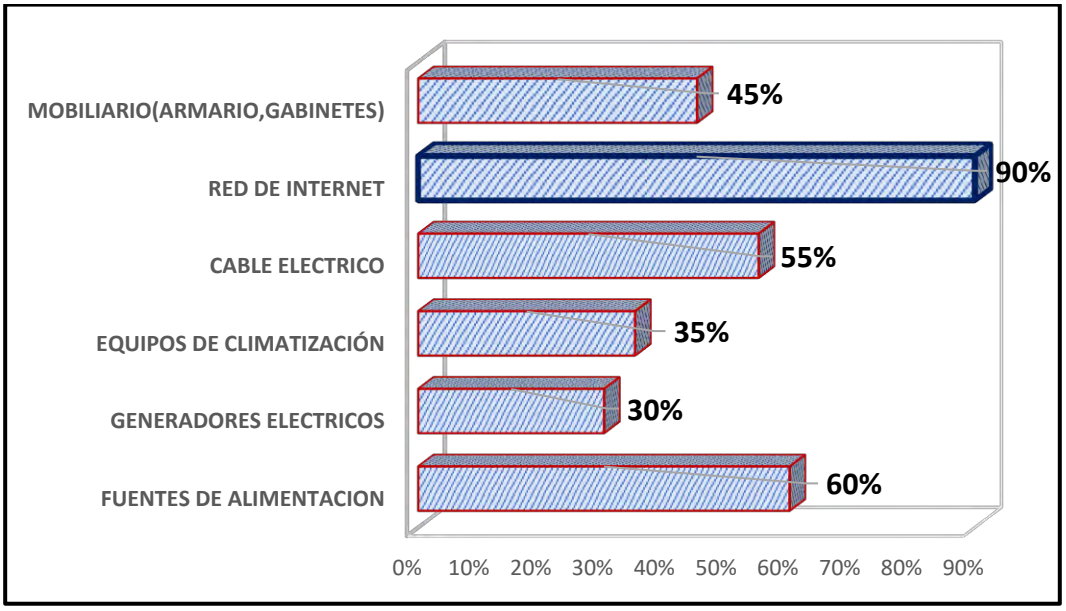
5.6.4 Activos de tipo equipamiento fundamentales

La recolección de datos se realizó mediante la encuesta mostrada en el Anexo B de esta investigación. La encuesta consistió en seis (6) preguntas para medir respecto a los activos de información de tipo hardware disponibles en la MDCH.

A continuación, se muestra, en gráficos, el resultado de la encuesta aplicada a los trabajadores de diferentes oficinas de la Municipalidad Distrital de Chamaca.

La frecuencia de respuesta fue la siguiente:

Figura 41. Activos de tipo equipamiento disponibles en la MDCH



Fuente: Elaboración propia

Interpretación: En el gráfico anterior, se puede observar que el activo red de internet, mobiliario son los activos que se encuentran expuestos a una mayor cantidad de riesgos dentro de la Municipalidad Distrital de Chamaca.

Capítulo VI
Análisis y discusión de resultados

CAPÍTULO VI

6 ANALISIS Y DISCUSIÓN DE RESULTADOS

6.1 Análisis y discusión

En el desarrollo de este proyecto se realizó con la finalidad de minimizar los riesgos de los activos de información como propuesta para el desarrollo del Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Chamaca, donde se obtuvo como resultado para la protección de los activos de información en un 67,14% quiere decir que protección de los activos de información no es muy significativo y la variación de la vulnerabilidad de acceso a la información es de 48,33% lo que quiere decir es muy vulnerable el acceso a la información en la Municipalidad Distrital de Chamaca.

El proyecto de propuesta de un Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Chamaca es fundamental para salvaguardar los activos de información de manera eficiente.

- **El diagnóstico de Seguridad de la Información**:

  El análisis inicial reveló la falta de un sistema de gestión de seguridad de la información en la Municipalidad Distrital de Chamaca. El diagnóstico se centró en los terminales tecnológicos y el personal, identificando la necesidad urgente de implementar medidas para proteger la información confidencial y valiosa.

- **Normas y buenas prácticas**: el desarrollo de la propuesta del Sistema de Gestión de Seguridad de Información se basó en las normas estándares de seguridad de información, específicamente la norma técnica peruana NTP ISO/IEC 27001:2014. Este enfoque garantiza que las prácticas adoptadas sean reconocidas y aceptadas

internacionalmente, contribuyendo así a la eficacia del SGSI en la Municipalidad Distrital de Chamaca.

- **Metodología del ciclo Deming (PDCA):** La aplicación de la metodología del ciclo Deming permitió un enfoque sistemático para mejorar continuamente la seguridad de la información. Esto incluyó solamente el proceso de planificación, la identificación de controles, la verificación de su eficacia y la acción correctiva cuando fuera necesario.
- **Fortalecimiento de aspectos claves**: La implementación de controles de seguridad se centró en fortalecer la confidencialidad, integridad y disponibilidad de los activos de información, tanto de software como de hardware. Estos aspectos son cruciales para garantizar la protección adecuada de la información sensible.
- **Cumplimiento legal y normativo:** El proyecto abordó la obligatoriedad legal, citando la Resolución Ministerial N° 004-2016-PCM y el Oficio Múltiple N° D000037-2020-PCM-SEGDI. Cumplir con estos requisitos legales es esencial para evitar sanciones y garantizar la conformidad con las regulaciones vigentes.

El proyecto ha logrado establecer un propuesta sólida y eficaz para la gestión de la seguridad de la información en la Municipalidad Distrital de Chamaca. La aplicación de normas reconocidas, la metodología del ciclo Deming y la atención a los aspectos clave de la seguridad de la información han contribuido a mejorar la postura de seguridad de la entidad y a cumplir con las exigencias legales y normativas establecidas.

CONCLUSIONES

- Se concluye con el desarrollar alcances de políticas de Seguridad de Información como se muestra en el numeral 3.3.2 políticas que son muy importantes para proteger los activos de información y que los trabajadores deben tener conocimiento para el correcto uso de los activos de información en la Municipalidad Distrital de Chamaca bajo la norma técnica peruana ISO/ IEC 27001:2014
- Se concluyó con la identificación de los riesgos de los activos de información mediante una encuesta realizada a los trabajadores de la Municipalidad Distrital de Chamaca como se muestra en capítulo 3, en numeral 3.3.3 y luego de ello se analizó y desarrollo cada uno de las fases de la metodología del ciclo Deming (PDCA) en su fase de planear donde se idéntico los riesgos, los controles que se deberían de seguir para su respectivo tratamiento y el conocimiento del personal respecto a la seguridad de los activos de información que se encuentran en la Municipalidad Distrital de Chamaca.
- Con concluye con el desarrollo de los controles de acceso a la información correspondientes, después de realizar un análisis de los riesgos como se aprecia en el numeral 5.7, los que se presentan frecuentemente con los activos de información que son vulnerables por parte de los trabajadores y personas ajenas a la Municipalidad se ejecutó los controles de acceso a la información bajo la norma ISO/IEC 27001:2014.

RECOMENDACIONES

- Se recomienda la implementar el Sistema de Gestión de la Seguridad de la Información para mitigar los riesgos de los activos de información en la Municipalidad Distrital de Chamaca .
- Se recomienda establecer el comité de seguridad de información de forma anual conformada por el Alcalde, Gerente Municipal, jefe de Planeamiento y presupuesto, responsable de informática y asesor legar para la implementación del Sistema de Gestión de la Seguridad de la Información.
- Se recomienda a los responsables del área de tecnología de información de las entidades públicas adoptar los lineamientos propuestos por la NTP ISO/IEC 27001:2014, por tener un carácter de obligatoriedad por parte de la Presidencia del Consejo de ministros conjuntamente con la Secretaría del Gobierno Digital.
- Se recomienda implementar un Sistema de Gestión de Seguridad de Información con las especificaciones de la NTP ISO/IEC 27001:2014 que mediante resolución Ministerial N°004-2016-PCM, el estado peruano aprueba el uso obligatorio de esta norma y de esta forma cumplir con los requisitos legales respecto a la Seguridad de Información.
- Se recomienda utilizar la NTP ISO/27001 en su versión actualizada 2022 para futuros proyectos similares, donde especifica los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de la información dentro del contexto de la organización.

REFERENCIAS BIBLIOGRÁFICAS

Ancco, H., & Yuver. (2018). “Modelo de Gestión De Seguridad de la Información con Iso/Iec 27001 Para Minimizar la Vulnerabilidad de la información en la Municipalidad Distrital de Santa María de Chicmo, Andahuaylas 2018.” *Uiversidad Nacional Jose Maria Arguedas APURIMAC*,1–83. http://revistas.unitru.edu.pe/index.php/agroindscience/article/view/114/131

Ariasca Suma, F. L., & Quispe Borda, S. K. (2016). Desarrollo de una propuesta de implementación de la ntp iso/iec 27001 :2014, sistema de gestión de seguridad de la información, para la oficina funcional de informática del gobierno regional Cusco. *Universidad Nacional de San Antonio Abad Del Cusco*. http://repositorio.unsaac.edu.pe/handle/UNSAAC/2454

Arlenys Carolina, N. (2017). Diseño de un Sistema de Gestión de La Seguridad de la Información (SGSI) Basados en La Norma ISO/IEC 27001:2013 Trabajo De Grado Participantes. *Institución Universitaria Politécnico Grancolombiano*.

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. *Universidad Nacional Abierta Y A Distancia Unad De Colombia*. https://repository.unad.edu.co/

Calderon Arateco, L. L. (2004). Seguridad informatica y Seguridad de Informacion. *Universidad Piloto de Colombia.*

Cosios Avila, T. V. (2020). Implementación De Auditoría Informática Con La Iso 27001 En La Municipalidad Distrital De Suyo-Piura; 2020. *Universidad Catolica Los Angeles Chimbote*, 1–187. https://hdl.handle.net/20.500.13032/23722

Deming Edward, W. (2016). Metodologia del Ciclo Deming..

Hernandez Sampieri, R. (2014). *Metodologia de la Investigación* (6ta Edicion).

ISO -International Organization for Standardization. (2011). *Familias de las Normas ISO 27000*.

Magerit versión 2. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las AdminisTraciones Públicas*. *2006*. http://administracionelectronica.gob.es/

MINTIC. (2016). Guía de gestión de riesgos. *Ministerio de Tecnologías de La Información*, *7*, 39.http://www.mintic.gov.co/

NTP-ISO/IEC 27001. (2014). Tecnologia de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. *Norma Técnicas Peruana*, *2da Edicio*, 1–45.https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/1bsmkkknl_60425.pdf?ver=1624594708991

Oficio Multiple D00037-PCM. (2020). *OFICIO MULTIPLE N ° D000037-2020-PCM-SEGDI*. 2016.

Pedraza Rodriguez, G. (2017). *Plan de Implementación de un Sistema de Gestión De Seguridad de la Información en una Entidad del Sector Publico basado en la Ntc Iso 27001:2013*. Bogota, Colombia. https://repository.uamerica.edu.co/handle/20.500.11839/7008

Regina Baena, G., Mendoza Mendez, R. V., & Joel Coronado, E. dorantes. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. *Contribuciones a La Economía*, *2019–02*. Mexico. https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html.

Ricardo Lopéz. (2017). *Sistema de Gestión de la Seguridad Informática*. Fundación Universitaria del Área Andina. Bogota. https://digitk.areandina.edu.co/handle/areandina/1238

Rodriguez Arevalo, Javier; Torres Calderon, W. (2019). Analisis de Riesgos de Seguridad de la Informacion del Area IT de la Empresa Royal Services S.A. *Universidad Nacional Hermilio Valdizan, Bogota Colombia*, *6*(1), 5–44. https://repository.ucatolica.edu.co/server/api/core/bitstreams/5fdf46d3-6ec9-4583-b19f-4fd160fceac5/content

Rojas Valduciel. (2016). La seguridad informática y la seguridad de la información. *Activos de Información*. https://doi.org/10.23857/pc.v2i12.420

Sandoval Alania, J. C. (2020). Propuesta De Diseño De Un Sistema De Gestión De Seguridad De La Información Basado En La Ntp-Iso/Iec 27001 Para La Dirección Regional De Trabajo Y Promoción Del Empleo – Huánuco”. *Universidad Nacional Hermilio Valdizan*,. Huanuco, Perú. https://repositorio.unheval.edu.pe/handle/20.500.13080/6447?show=full

ANEXOS

Anexo 1. Resolución Ministerial de aprobación de la NTP ISO/IEC 27001:2014

ANEXO 2

RELACIÓN DE REPRESENTANTES DEL GOBIERNO NACIONAL ANTE COMISIÓN INTERGUBERNAMENTAL DEL SECTOR AGRICULTURA Y RIEGO, CONFORMADA EN EL MARCO DEL DECRETO SUPREMO Nº 047-2009-PCM

	CARGO	DEPENDENCIA / INSTITUCIÓN	CARGO
1	Viceministro (a) de Política Agrarias	Despacho Viceministerial	Presidente Comisión Intergubernamental
2	Director (a) de la Oficina General de Planeamiento	Oficina General de Planeamiento y Presupuesto	Miembro
3	Profesional		Miembro Alterno
4	Profesional	Oficina General de Asesoría Jurídica	Miembro
5	Profesional	Oficina General de Administración	Miembro
6	Profesional	Oficina General de Gestión de Recursos Humanos	Miembro
7	Director (a) General de Articulación Intergubernamental	Dirección General de Articulación Intergubernamental	Miembro
8	Director (a) de Gestión Descentralizada		Miembro
9	Director de Seguimiento y Evaluación de Políticas (a)	Dirección General de Seguimiento y Evaluación de Políticas	Miembro
10	Director (a) de Estadística Agraria		Miembro Alterno
11	Director (a) General de Políticas Agrarias	Dirección General de Políticas Agrarias	Miembro
12	Director (a) de Políticas y Normatividad Agraria		Miembro
13	Profesional	Dirección General de Negocios Agrarios	Miembro
14	Profesional		Miembro Alterno
15	Profesional	Dirección General de Asuntos Ambientales Agrarios	Miembro
16	Profesional	Dirección General de Infraestructura Agraria y Riego	Miembro
17	Profesional	Servicio Nacional Forestal y de Fauna Silvestre	Miembro
18	Profesional		Miembro
19	Profesional	Programa de Desarrollo Productivo Agrario Rural - AGRORURAL	Miembro
20	Profesional		Miembro Alterno
21	Jefe (a) del Programa	Programa de Compensaciones para la Competitividad - AGROIDEAS	Miembro
22	Jefe (a) de la Unidad de Planificación, Seguimiento y Evaluación		Miembro
23	Director (a) de Gestión del Riego	Programa Sub Sectorial de Irrigaciones (PSI)	Miembro
24	Profesional		Miembro Alterno
25	Director (a) de la Unidad de Estudios y Cooperación de la Oficina de Planificación y Desarrollo Institucional	Servicio Nacional de Sanidad Agraria (SENASA)	Miembro
26	Profesional		Miembro
27	Director (a) General de la Oficina de Planeamiento y Presupuesto	Instituto Nacional de Innovación Agraria (INIA)	Miembro
28	Profesional		Miembro Alterno
29	Director (a) de Conservación y Planeamiento de Recursos Hídricos	Autoridad Nacional del Agua (ANA)	Miembro

1332846-1

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

RESOLUCIÓN MINISTERIAL
Nº 004-2016-PCM

Lima, 8 de enero de 2016

CONSIDERANDO:

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

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

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

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

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

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo Nº 081-2013-PCM, prevé determinados Lineamientos Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema

Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

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

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

SE RESUELVE:

Artículo 1.- De la aprobación

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

Artículo 2.- Publicación

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

Artículo 3.- De la implementación

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

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

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

Artículo 4.- De la certificación de la norma

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

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

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

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

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial Nº 129-2012-PCM.

Regístrese, comuníquese y publíquese.

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

1333015-1

AGRICULTURA Y RIEGO

Delegan facultades a diversos funcionarios del Ministerio durante el Ejercicio 2016

RESOLUCIÓN MINISTERIAL
Nº 0006-2016-MINAGRI

Lima, 12 de enero de 2016

CONSIDERANDO:

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

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

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

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

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

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

REPÚBLICA DEL PERÚ

Resolución Ministerial

N° 004-2016-PCM

Lima, - 8 ENE. 2016

CONSIDERANDO:

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

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

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

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

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

Que, la actual Política Nacional de Gobierno Electrónico 2013 – 2017, aprobada mediante el Decreto Supremo N° 081-2013-PCM, prevé determinados Lineamientos

Estratégicos para el Gobierno Electrónico en el Perú, entre otros, el relacionado con la Seguridad de la Información, el mismo que busca velar por la integridad, seguridad y disponibilidad de los datos debiendo establecerse lineamientos de seguridad de la información a fin de mitigar el riesgo de exposición de información sensible del ciudadano, correspondiendo que en uso de las funciones atribuidas al ente rector del Sistema Nacional de Informática, para el caso ONGEI-PCM, a cargo de implementar dicha Política Nacional, articular la implementación efectiva del acotado lineamiento por parte de los distintos entes del sector público;

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

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

SE RESUELVE:

Artículo 1.- De la aprobación

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

Artículo 2.- Publicación

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

Artículo 3.- De la implementación

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

Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de

Resolución Ministerial

implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros.

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

Artículo 4.- De la certificación de la norma

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

Artículo 5.- Del Comité de Gestión de Seguridad de la Información

Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por:

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

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

Artículo 6.- De la responsabilidad de la implementación

La responsabilidad de la implementación de la presente norma será del titular de cada entidad.

Artículo 7.- Déjese sin efecto

Deróguese la Resolución Ministerial Nº 129-2012-PCM.

Regístrese, comuníquese y publíquese

PEDRO CATERIANO BELLIDO
Presidente del Consejo de Ministros

Anexo 3. Oficio Múltiple a la MDCH por parte de la Secretaria del Gobierno Digital

PERÚ | Presidencia del Consejo de Ministros | Secretaría General | Secretaría de Gobierno Digital

FIRMA DIGITAL PCM PRESIDENCIA DEL CONSEJO DE MINISTROS

Firmado digitalmente por CHOCOBAR REYES Marushka Victoria Lia FAU 20168999926 hard
Secretaria De Gobierno Digital
Motivo: Soy el autor del documento
Fecha: 19.05.2020 12:27:37 -05:00

"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
Año de la Universalización de la Salud

Lima, 19 de Mayo del 2020

OFICIO MULTIPLE N° D000037-2020-PCM-SEGDI

Señores:
ANTONIO HUAMAN ARIAS
Alcalde Distrital
MUNICIPALIDAD DISTRITAL DE CHAMACA
CALLE 28 DE JULIO S/N

Presente.-

Asunto : Vigilancia y Acompañamiento al Cumplimiento de la Implementación del Sistema de Gestión de Seguridad de la Información en el marco del Resolución Ministerial N° 004-2016-PCM.

De mi consideración:

Es grato dirigirme a usted a fin de saludarle y, hacer de su conocimiento que en el marco del Decreto Legislativo N°1412, el Decreto de Urgencia N°006-2020, el Decreto de Urgencia N°007-2020 y el Decreto Supremo N°118-2020-PCM, la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros ejerce la rectoría en materia de gobierno, transformación y confianza digital y viene liderando el despliegue de tecnologías digitales en el país en favor de un Perú más íntegro, competitivo, innovador, confiable y cercano a los ciudadanos.

En virtud de ello, y con la urgencia que nos exige la emergencia nacional a causa de la pandemia del COVID19, la Secretaría de Gobierno Digital **viene desplegando las acciones correspondientes a la vigilancia y acompañamiento al cumplimiento de la regulación vigente en materia digital a fin de acelerar el logro de los objetivos de transformación digital del país.**

Con ese objetivo, es necesario que su entidad cumpla con lo establecido en el Resolución Ministerial N° 004-2016-PCM que indica:

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

Artículo 3.- De la implementación
Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma.
Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información (…)

En ese sentido, solicitamos remitir el documento correspondiente al acto de administración que aprueba la Implementación del Sistema de Gestión de Seguridad de la Información de su entidad, y, a su vez, subirlo al siguiente vínculo bit.ly/2wqYmSx en el más breve plazo posible, a fin de dar cumplimiento a la referida norma.

Para cualquier coordinación y apoyo en el despliegue de las acciones necesarias para el avance digital de su entidad así como el cumplimiento de la normatividad vigente no dude en comunicarse al correo gobierno.digital@pcm.gob.pe o al teléfono 949076065 con Yan Romero Aranda, Consultor en Transformación Digital para Gobiernos Locales por el Proyecto del Banco Interamericano de Desarrollo y la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno Digital.

Seguros de contar con su compromiso, le expreso mis sentimientos de consideración y estima.

Cordialmente.

Documento firmado digitalmente
MARUSHKA VICTORIA LIA CHOCOBAR REYES
SECRETARIA DE GOBIERNO DIGITAL
PRESIDENCIA DEL CONSEJO DE MINISTROS

Esta es una copia auténtica imprimible de un documento electrónico archivado en la Presidencia del Consejo de *Ministros*, aplicando lo dispuesto por el Art. 25 de D.S. 070-2013-PCM y la Tercera Disposición Complementaria Final del D.S. 026-2016-PCM. Su autenticidad e integridad pueden ser contrastadas a través de la siguiente dirección web:
Url: **https://sgdciudadano.pcm.gob.pe/register/verifica** Clave: **IA7SPSQ**

EL PERÚ PRIMERO

Anexo 4. Resolución de aprobación de la implementación de un SGSI en la MDCH

Municipalidad Distrital de Chamaca

Chumbivilcas - Cusco - Perú

RESOLUCIÓN DE ALCALDÍA N° 271-2020-A-MDCH.

Chamaca, 26 de agosto de 2020.

EL ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE CHAMACA.

VISTO: El Informe Legal Nº 017-2020-OAL-MDCH/CH-ENH., de fecha 22 de agosto de 2020, Y;

CONSIDERANDO:

Que, de conformidad con lo establecido por el Artículo 194° de la Constitución Política del Perú, modificada por Ley N° 30305, señala que "Las municipalidades provinciales y distritales son Órganos de Gobierno Local. Tienen autonomía política, económica y administrativa en los asuntos de su competencia (...)"; lo que debe ser concordado con lo dispuesto por el Artículo II del Título Preliminar de la Ley N°27972, Ley Orgánica de Municipalidades que especifica que: "Los gobiernos locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia". En ese sentido la autonomía que la Constitución Política del Perú establece para las municipalidades radica en la facultad de ejercer actos de gobierno administrativo y de administración con sujeción al ordenamiento jurídico;

Que, el Artículo VIII del Título Preliminar de la Ley Orgánica de Municipalidades Nº 27972, establece que los gobiernos locales están sujetos a las leyes y disposiciones que, de manera general y de conformidad con la Constitución Política del Perú, regulan las actividades y funcionamiento del Sector Público; así como a las normas técnicas referidas a los servicios y bienes públicos, y a los sistemas administrativos del Estado que por su naturaleza son de observancia y cumplimiento obligatorio;

Que, mediante Decreto Legislativo Nº 1412 se aprueba Ley de Gobierno Digital, que tiene como objetivo establecer el marco de gobernanza del Gobierno Digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, conforme establece el artículo 5º numeral 5.9 del Decreto Legislativo Nº 1412, establece que los disposiciones contenidas en la presente ley, así como su aplicación se rigen por los siguientes principios rectores, que los **Datos Abiertos por Defecto.-** Los datos se encuentran abiertos y disponibles de manera inmediata, sin comprometer el derecho a la protección de los datos personales de los ciudadanos. Ante la duda corresponde a la Autoridad de Transparencia definirlo; concordante con el artículo 6º señala que el gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital; y el numeral 23.2 artículo 23º, del mismo cuerpo de Ley señala que las entidades de la Administración Pública administran sus datos como un activo estratégico, garantizando que estos se recopilen, procesen, publiquen, almacenen y pongan a disposición durante el tiempo que sea necesario y cuando sea apropiado, considerando las necesidades de información, riesgos y la normatividad vigente en materia de gobierno digital, seguridad digital, transparencia, protección de datos personales y cualquier otra vinculante;

Que, mediante el Decreto Supremo Nº 118-2018-pcm, se declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial, asimismo a través del Decreto de Urgencia Nº 006-2020, se crea el Sistema Nacional de Transformación Digital y mediante Decreto DE Urgencia Nº 007-2020, se aprueba el marco de confianza digital y dispone medidas para su fortalecimiento;

Que, el numeral 9.3 del artículo 9º del Decreto de Urgencia Nº 007-2020, establece que "Las entidades de la administración pública deben implementar un Sistema de Gestión de Seguridad de la Información (SGSI), un Equipo de Respuestas ante Incidentes de Seguridad Digital cuando corresponda y cumplir con la regulación emitida por la Secretaría de Gobierno Digital";

Que, mediante Resolucion Ministerial Nº 004-2016-PCM., se aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad.

Un nuevo comienzo para un futuro mejor...!

Municipalidad Distrital de Chamaca
Chumbivilcas - Cusco - Perú

Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática;

Que, conforme al Artículo 3º de la citada Resolucion Ministerial establece que las "Las entidades integrantes del Sistema Nacional de Informática, tendrán un plazo máximo de dos (2) años para la implementación y/o adecuación de la presente norma". Dichas entidades públicas tendrán un plazo de 60 días contados a partir de la fecha de publicación de la presente norma, para la presentación del cronograma de implementación y/o adecuación del sistema de gestión de la Seguridad de la Información, que deberá ser presentado a la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI) de la Presidencia del Consejo de Ministros. Concordante con el articulo 5° de la misma Resolucion Ministerial, señala que, Cada entidad designará un Comité de Gestión de Seguridad de la Información, conformado por: i) El/la titular de la entidad; ii) El/la responsable de administración o quien haga sus veces; iii) El/la responsable de planificación o quien haga sus veces; iv) El/la responsable del área de informática o quien haga sus veces; v) El/la responsable de área legal o quien haga sus veces y vi) El/la oficial de seguridad de la información;

Que, mediante Informe Legal Nº 017-2020- OAL-MDCH/CH-ENH., de fecha 22 de agosto de 2020, el Abg. Elías Ninaquispe Huamani, Asesor Legal de la Municipalidad Distrital de Chamaca, habiendo analizado el contenido del Oficio Múltiple Nº D000037-2020-PCM-SEGDI., de la Secretaria de Gobierno Digital de la Presidencia del Concejo de Ministros, considera legalmente procedente aprobar la implementación del Sistema de Gestión de Seguridad de la Información de la Municipalidad distrital de Chamaca, de conformidad a la Resolucion Ministerial Nº 004-2016-PCM;

Por, las consideraciones expuestas, en uso de las facultades contenidas en el inciso 6), del artículo 20º de la Ley Nº 27972- Ley Orgánica de Municipalidades;

SE RESUELVE:

ARTÍCULO PRIMERO.- APROBAR la implementación del Sistema de Gestión de Seguridad de la Información de la Municipalidad distrital de Chamaca, de conformidad a la Resolucion Ministerial Nº 004-2016-PCM; conforme expuesto en la parte considerativa en la presente resolución, la misma está integrado por lo siguientes funcionarios:

- El Alcalde de la Municipalidad distrital de Chamaca.
- El Gerente Municipal de la Municipalidad distrital de Chamaca.
- El Jefe de Planificación y Presupuesto de la Municipalidad distrital de Chamaca.
- El Responsable de Informática y Sistemas de la Municipalidad distrital de Chamaca.
- El Asesor Legal de la Municipalidad distrital de Chamaca.

ARTÍCULO SEGUNDO.- ENCARGAR a los funcionarios considerados en el articulo primero el cumplimiento estricto de lo dispuesto en el Decreto de Urgencia Nº 007-2020.

ARTICULO TERCERO - ENCARGAR a la Asesoría Legal la implementación de funciones del Comité de Gestión de Seguridad de la Información, de la Municipalidad distrital de Chamaca de conformidad a la Resolucion Ministerial Nº 004-2016-PCM.

ARTÍCULO CUARTO.- REMITIR copia de la presente resolución a la Secretaría de Gobierno Digital de la Presidencia del Consejo de Ministros.

ARTICULO QUINTO.- DISPONER la publicación de la presente Resolución en el Cartel de la Municipalidad distrital de Chamaca.

REGÍSTRESE. COMUNÍQUESE Y PUBLÍQUESE

MUNICIPALIDAD DISTRITAL DE CHAMACA
CHUMBIVILCAS - CUSCO
Antonio Huaman Arias
DNI: 00520431
ALCALDE

Un nuevo comienzo para un futuro mejor...!

Anexo 5. Solicitud presentada a la MDCH para implementar el SGSI

CARGO

MUNICIPALIDAD DISTRITAL CHAMACA
CHUMBIVILCAS CUSCO
MESA DE PARTES
Fecha: 07 DIC. 2022 Hora: 3:34
Exp. Nº 3465 Folios: 36 F

SOLICITO: PERMISO PARA APLICACIÓN DE PROYECTO DE TESIS Y APLICACIÓN DE ENCUESTAS AL PERSONAL QUE LABORA EN LA MUNICIPALIDAD DISTRITAL DE CHAMACA.

SR. ANTONIO HUAMAN ARIAS
ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE CHAMACA

Yo: **ALCIDES LAROTA CUITO**, identificada con **DNI N° 46621444**. Bachiller de la Escuela profesional de Ing. Informática y de Sistemas de la Universidad Nacional de San Antonio Abad del Cusco, Domiciliado Urb. UVIMA 7, del distrito de San Sebastián, provincia y departamento de Cusco. Ante Ud. Respetuosamente me presento y expongo.

Que teniendo el agrado de saludarle y a la vez expresarle mis saludos cordiales y a la vez solicitarle permiso para la aplicación del proyecto de tesis y en ingreso a la Municipalidad, principalmente su tiempo de cada trabajador de todas las áreas para realizar una encuesta del proyecto titulado: **"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON NTP ISO/IEC 27001: 2014, PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE CHAMACA, CHUMBIVILCAS, CUSCO 2020-2021"**, el cual está aprobado con **RESOLUCIÓN Nro. D-2525-2022-FIEEIM-UNSAAC**, por la Universidad Nacional de San Antonio Abad del Cusco. Para tal proyecto le solicito realizar una encuesta a los trabajadores que laboran en las diferentes áreas de la municipalidad, dicha encuesta será de vital importancia para el interesado y el principal beneficiado con este proyecto será la Municipalidad Distrital de Chamaca, los resultados ayudarán de manera eficiente a la alta gerencia en la toma de decisiones respecto a la seguridad de información dentro de la Municipalidad.

Adjunto:

- ✓ Resolución de aprobación del proyecto de tesis de la Universidad Nacional de San Antonio Abad del Cusco.
- ✓ Plan de tesis.
- ✓ Formato de encuestas

Por lo expuesto:

Estaré atento a su respuesta y le agradezco de antemano su atención prestada.

Chamaca 05 de diciembre del 2022

Bc. ALCIDES LAROTA CUITO
DNI: 46621444

Anexo 6. ISO/IEC 27002:2013

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

Anexo 7. Encuesta realizada a los trabajadores de la MDCH..

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMA
ENCUESTA SOBRE EL PROYECTO DE TESIS

ENCUESTA RESPECTO A LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE CHAMACA.

Estoy realizando un estudio sobre el Proyecto denominado:
Por tal motivo, me gustaría realizar algunas preguntas respecto a su terminal tecnológico. La información que es recopilada será estrictamente confidencial y permanecerá **"IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN CON NTP ISO/IEC 27001: 2014, PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE CHAMACA, CHUMBIVILCAS, CUSCO 2020-2021"**. Que es de absoluta reserva. Según Ley Nº 29733 (Ley de Protección de Datos Personales). Presentado por Br. Alcides Larota Cuito Bachiller de la escuela profesional Ing. Informática y de Sistemas- UNSAAC.

La siguiente encuesta tiene por finalidad saber si el personal administrativo que labora en el área de _____ ,conoce utiliza y salvaguarda la información de manera óptima y adecuada.

Instrucciones:

PROTECCION DE LOS ACTIVOS DE INFORMACION

Para desarrollar la encuesta, usted debe leer cada pregunta y escoger una las alternativas propuestas con un "**X**" dentro de los paréntesis.

1) ¿Ud. tiene conocimiento si en la Municipalidad Distrital de Chamaca existe un sistema de gestión de seguridad de la información (SGSI)?
   Si ( ) Parcialmente ( ) No ( )
2) Ud tiene conocimiento sobre un Sistema de Gestión de Seguridad de Información
   Si ( ) Parcialmente ( ) No (
3) ¿Cree usted que implementado un SGSI mejorara la seguridad de información de su área de trabajo?
   Si ( ) Parcialmente ( ) No ( )
4) ¿Aprobaría usted la implementación del SGSI en el área de su trabajo?
   Si ( ) Parcialmente ( ) No ( )
5) ¿Cree Ud. que en su área de trabajo se lograra un cambio positivo con la aplicación de este SGSI?
   Si ( ) Parcialmente ( ) No ( )
6) ¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?
   Si ( ) Parcialmente ( ) No ( )
7) ¿Cuenta Ud. con un computador para realizar sus funciones?
   Si ( ) Parcialmente ( ) No ( )
8) Usted apaga los equipos informáticos debidamente después de utilizarlos
   Si ( ) Parcialmente ( ) No ( )
9) Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro del área de su trabajo
   Si ( ) Parcialmente ( ) No ( )
10) Existe algún extintor cerca de los equipos informáticos de su área de trabajo.
    Si ( ) Parcialmente ( ) No ( )

RIESGSOS DE ACCESO A LOS ACTIVOS DE INFORMACION

11) ¿Las contraseñas de acceso de usuario a las computadoras donde se tiene información vital son descifradas o combinados con caracteres?
    Si ( ) Parcialmente ( ) No ( )
12) ¿La información está protegida contra posibles alteraciones?
    Si ( ) Parcialmente ( ) No ( )
13) ¿Se restringen la instalación de otras aplicaciones o software que no sea de su trabajo?
    Si ( ) Parcialmente ( ) No ( )
14) ¿La municipalidad Distrital de Chamaca cuenta con controles de acceso al personal de la institución y público en general?
    Si ( ) Parcialmente ( ) No ( )
15) ¿La puerta y las ventanas de las áreas de trabajo se encuentran seguras?
    Si ( ) Parcialmente ( ) No ( )

UNIVERSIDAD NACIONAL DE SAN ANTONIO ABAD DEL CUSCO
ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMA
ENCUESTA SOBRE EL PROYECTO DE TESIS

16) En caso que su computadora presente averias, es asistido por un personal especializado?
Si ( ) Parcialmente ( ) No ( )
17) ¿El área de trabajo está bien ubicado y seguro contra amenazas externas? Ejemplo inundaciones
Si ( ) Parcialmente ( ) No ( )
18) ¿En caso de alguna falla del internet en su computadora y/o dispositivo móvil Ud. conoce donde ir para su pronta verificación?
Si ( ) Parcialmente ( ) No ( )
19) ¿Se realiza mantenimiento periódico del hardware y software en la institución?
Si ( ) Parcialmente ( ) No ( )
20) ¿Se realiza copias de sus activos de información que maneja en el equipo tecnológico de trabajo?
Si ( ) Parcialmente ( ) No ( )

Instrucciones: En cada tabla marque (**x**) con los activos que se cuentan.

CUESTIONARIO DE ACTIVOS DE INFORMACION
¿Qué activos de tipo servicio son fundamentales para el área de su trabajo?
Marque con (**x**) los activos que cuenta el área de la oficina a donde pertenece. ( ) Internet ( ) Intranet ( ) Acceso remoto ( ) Correo electrónico ( ) Almacenamiento de ficheros (File Server) ( ) Intercambio electrónico de datos
CUESTIONARIO DE TIPO SOFTWARE / APLICACIONES UTILIZADAS
¿Qué activos de tipo software son fundamentales para el área de su trabajo?
Marque con (**x**) los activos que cuenta el área de la oficina a donde pertenece. ( ) Páginas Web ( ) Intranet ( ) Servidor de correo electrónico ( ) Sistema de gestión de bases de datos ( ) Anti-Virus, Autocad, Office, Adobe pdf, ( ) Sistema Operativo, Windows.
CUESTIONARIO DE TIPO EQUIPOS INFORMÁTICOS
¿Qué tipo de hardware son fundamentales para el área de su trabajo?
Marque con (**x**) los activos que cuenta el área de la oficina a donde pertenece. ( ) Impresoras ( ) Escáneres ( ) Módems ( ) Conmutadores (Switch) ( ) Encaminadores (Router) ( ) Cortafuegos (Firewall) ( ) Punto de acceso inalámbrico (WIFE)
CUESTIONARIO DE TIPO EQUIPAMIENTO
Marque con (**x**) los activos que cuenta el área de la oficina a donde pertenece. ( ) Fuentes de alimentación ( ) Generadores eléctricos ( ) Equipos de climatización ( ) Cable eléctrico ( ) Red de Internet ( ) Mobiliario: armarios, gabinetes, escritorios, etc.

Anexo 8. Formato 1 para mantenimiento preventivo de equipos de cómputo

MUNICIPALIDAD DISTRITAL DE CHAMACA

PERÚ Presidencia del Consejo de Ministros Secretaría de Gobierno Digital

MANTENIMIENTO PREVENTIVO DE EQUIPOS DE CÓMPUTO

FORMATO 1

FICHA N°

FECHA:

PERSONAL DE SISTEMAS

NOMBRES Y APELLIDOS :

CARGO:

DATOS DEL EQUIPO

CÓDIGO DEL EQUIPO:

USUARIO:

DESCRIPCION:

AREA:

ACTIVIDADES REALIZADAS

HORA INICIO:

HORA FIN:

N°	DESCRIPCION	ESTADO	OBSERVACIONES
1	ASPIRAR POLVO DE EQUIPO	☐	
2	LIMPIEZA DE LA FUENTE DE PODER	☐	
3	LIMPIEZA DE VENTILADORES	☐	
4	LIMPIEZA DE LECTOR OPTICO	☐	
5	APLICAR LIMPIAR CONTACTO	☐	
6	APLICAR REFIGERANTE AL PROCESADOR	☐	
7	LIMPIEZA DEL MONITOR	☐	
8	LIMPIEZA DEL TECLADO Y MOUSE	☐	
9	ENSERADO DEL EQUIPO	☐	
10	OTROS	☐	
	RECOMENDACIONES		

FIRMA DE JEFE DEL AREA DE INFORMATICA	FIRMA DE USUARIO

Fuente: Elaboración propia

Anexo 9. Formato 2 para mantenimiento correctivo de equipos cómputo

MUNICIPALIDAD DISTRITAL DE CHAMACA

PERÚ Presidencia del Consejo de Ministros Secretaría de Gobierno Digital

MANTENIMIENTO CORRECTIVO DE EQUIPOS DE COMPUTO

FORMATO 2

FICHA N°

FECHA:

DATOS DEL USUARIO

NOMBRES Y APELLIDOS : CARGO:

CORREO ELECTRÓNICO: AREA:

PERSONAL DE SISTEMAS

NOMBRES Y APELLIDOS: CARGO:

DETALLE DEL PROBLEMA

ACTIVIDADES REALIZADAS

HORA INICIO: HORA FIN:

SOLUCIÓN:

ENCUESTA AL USUARIO:

MARQUE CON X LA OPCION SELECCIONADA	*COMENTARIOS Y SUGERENCIAS:*
1. ¿LA ACTITUD DE LA PERSONA QUE LO ATENDIO FUE?	
☐ EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA	
2. ¿EL TIEMPO PARA ATENDER SU REQUERIMIENTO FUE?	
☐ EXCELENTE ☑ BUENA ☐ REGULAR ☐ MALA	
3. ¿LA EXPLICACION DE LA SOLUCIÓN FUE?	
☐ EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA	
4.¿LA CALIDAD DEL SERVICIO PROPORCIONADO POR EL SOPORTE TECNICO FUE?	
☐ EXCELENTE ☐ BUENA ☐ REGULAR ☐ MALA	

FIRMA DE JEFE DEL AREA DE INFORMATICA	FIRMA DE USUARIO

Fuente: Elaboración propia

Anexo 10. Formato 3 seguridad operativa

MUNICIPALIDAD DISTRITAL DE CHAMACA

PERÚ Presidencia del Consejo de Ministros Secretaría de Gobierno Digital

SEGURIDAD OPERATIVA PARA ACTIVOS DE INFORMACIÓN

FORMATO 3

FICHA N°

FECHA:

PERSONAL DE SISTEMAS

NOMBRES Y APELLIDOS :

CARGO:

DATOS DEL EQUIPO

CÓDIGO DEL EQUIPO:

USUARIO:

DESCRIPCIÓN:

ÁREA:

ACTIVIDADES REALIZADAS

HORA INICIO:

HORA FIN:

N°	DESCRIPCION	ESTADO	OBSERVACIONES
1	PROCEDIMIENTOS DE OPERACIÓN	☐	
2	PROTECCIÓN CONTRA CÓDIGO MALICIOSO	☐	
3	COPIAS DE SEGURIDAD	☐	
4	REGISTRO DE ACTIVIDAD	☐	
5	CONTROL DEL SOFTWARE	☐	
6	GESTIÓN DE VULNERABILIDAD	☐	
7	AUDITORIAS DE SISTEMAS DE INFORMACIÓN	☐	
	RECOMENDACIONES		

FIRMA DE RESPONSABLE AREA DE INFORMATICA	FIRMA DE USUARIO

Fuente: Elaboración propia

Anexo 11. Formato 4 gestión de activos e inventario de equipos informáticos

MUNICIPALIDAD DISTRITAL DE CHAMACA

PERÚ Presidencia del Consejo de Ministros Secretaría de Gobierno Digital

INVENTARIO DE RECURSOS INFORMATICOS

FORMATO 4

FECHA :

DESCRIPCIÓN DE LOS BIENES INFORMÁTICOS

ÁREA:

RESPONSABLE: CARGO:

N°	CODIGO	DESCRIPCION	TIPO	DETALLE	FECHA ADQ	GUIA REMISIÓN	ESTADO			REPORTE
							BUENO	MALO	REGULAR	
1							☐	☐	☐	
2							☐	☐	☐	
3							☐	☐	☐	
4							☐	☐	☐	
5							☐	☐	☐	
6							☐	☐	☐	
7							☐	☐	☐	
8							☐	☐	☐	
9							☐	☐	☐	
10							☐	☐	☐	
11							☐	☐	☐	
12							☐	☐	☐	
13							☐	☐	☐	

FIRMA DE JEFE DEL AREA DE INFORMATICA	FIRMA DE USUARIO

Fuente: Elaboración propia

Anexo 12. Formato 5 control de acceso

MUNICIPALIDAD DISTRITAL DE CHAMACA

PERÚ Presidencia del Consejo de Ministros Secretaría de Gobierno Digital

GESTIÓN DE CUENTAS DE USUARIO

FORMATO 5

FICHA N° ____

1. DATOS DEL USUARIO (llenado por RR.HH)

DNI: ____

NOMBRES: ____ APELLIDOS: ____

ÁREA: ____ CARGO: ____

FECHA INGRESO ____

2. CARPETAS COMPARTIDAS EN RED (Llenado por gerencia del área)

2.1 ACCESO A CARPETAS COMPARTIDAS ☐ SI ☐ NO

3. EMAIL COORPORATIVO (llenado por la gerencia del área)

3.1 PERMITIR ENVIO A CORREO EXTERNOS ☐ SI ☐ NO

3.2 PERMITIR ENVIO A CORREO WEB (https://munichamaca.gob.pe) ☐ SI ☐ NO

4. ACCESO A INTERNET(llenado por gerencia de área)

4.1 PERMITIR ACCESO A INTERNET ☐ SI ☐ NO

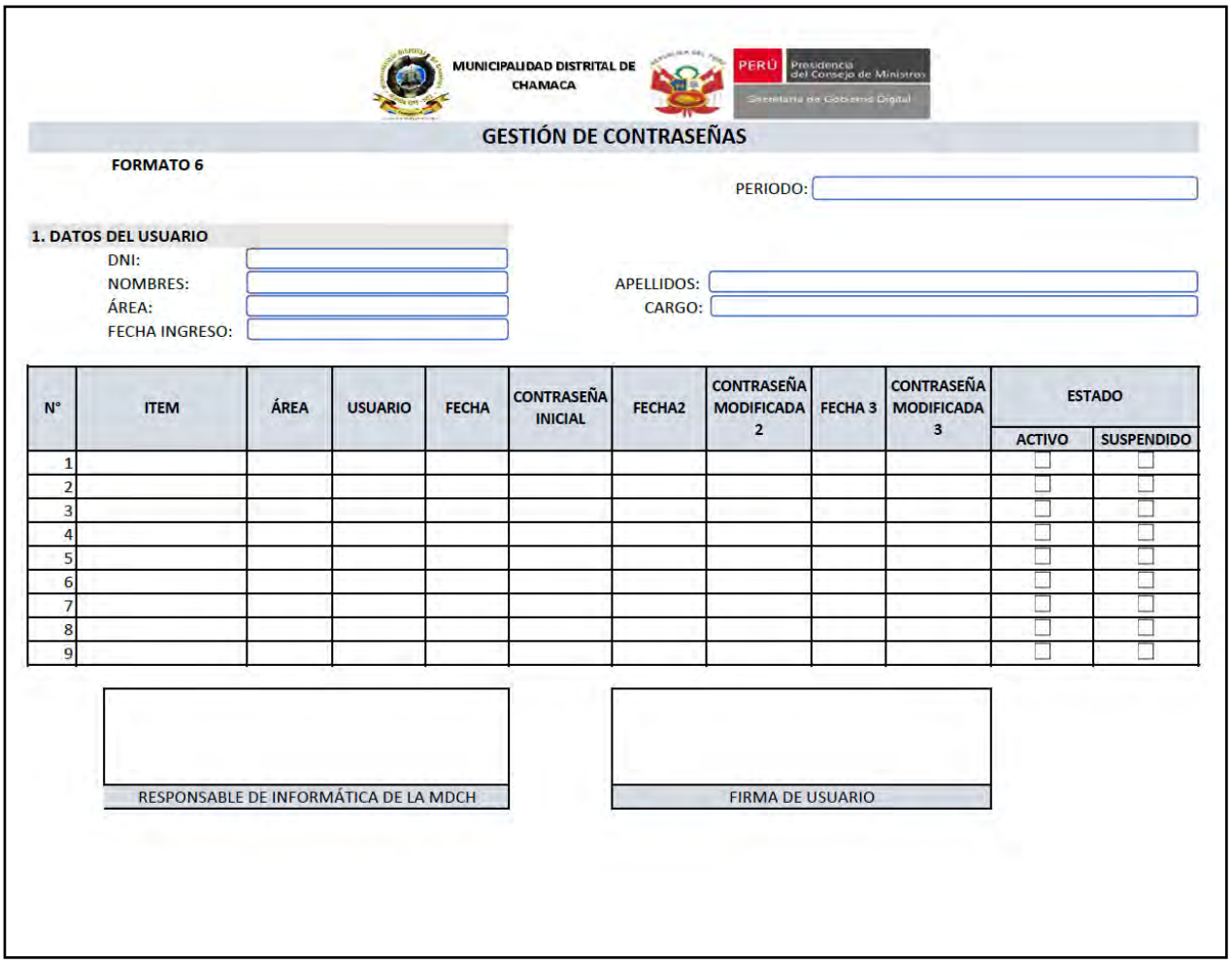
NOTA: En caso de seleccionar SI, tendrá que especificar las paginas que desea ingresar

N°	PAGINA WEB	TIPOS/ CONTENIDO	SUSTENTO
1			
2			
3			

FIRMA DEL RESPONSABLE DE INFORMÁTICA	FIRMA DEL USUARIO

Fuente: Elaboración propia

Anexo 13. Formato 6 gestión de contraseñas



MUNICIPALIDAD DISTRITAL DE CHAMACA

PERÚ Presidencia del Consejo de Ministros Secretaría de Gobierno Digital

GESTIÓN DE CONTRASEÑAS

FORMATO 6

PERIODO:

1. DATOS DEL USUARIO

DNI:
NOMBRES:
ÁREA:
FECHA INGRESO:
APELLIDOS:
CARGO:

N°	ITEM	ÁREA	USUARIO	FECHA	CONTRASEÑA INICIAL	FECHA2	CONTRASEÑA MODIFICADA 2	FECHA 3	CONTRASEÑA MODIFICADA 3	ESTADO	
										ACTIVO	SUSPENDIDO
1										☐	☐
2										☐	☐
3										☐	☐
4										☐	☐
5										☐	☐
6										☐	☐
7										☐	☐
8										☐	☐
9										☐	☐

RESPONSABLE DE INFORMÁTICA DE LA MDCH

FIRMA DE USUARIO

Fuente: Elaboración propia