ESCUELA DE POSGRADO Y ESTUDIOS CONTINUOS

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA PROTEGER LOS ACTIVOS DE INFORMACIÓN DEL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA DE LA ZONA NORTE DEL PERÚ

Tesis para optar el grado de **MAESTRA** en:

Ingeniería de Sistemas con Mención en Gerencia de Sistemas de Información

Autora:

Miryam Liliana Mendez Navarro

Asesor:

Doctor. Alberto Carlos Mendoza De Los Santos

Trujillo – Perú

2021

Resumen

La investigación tuvo como objetivo el diseño de un Sistema de Gestión de Seguridad de la Información para proteger los activos de información del Servicio de Administración Tributaria de la Zona Norte del Perú; dando cumplimiento a la Resolución Ministerial Nº 166-2017-PCM que dispone el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 en todas las entidades integrantes del Sistema Nacional de Informática.

La investigación es de tipo descriptiva debido a que se han observado situaciones ya existentes; así mismo, las técnicas utilizadas para la extracción de datos fueron recopiladas de una manera organizada y estructurada a través de entrevistas y revisión documentaria lo que ha permitido conocer y analizar el estado actual de la Administración Tributaria de acuerdo a los requisitos y objetivos de control y controles que tiene la norma, analizar su contexto organizacional, definir su estructura de seguridad, las políticas de seguridad de la información y los recursos necesarios para realizar el diseño. Adicionalmente, se identificó los activos de información, las vulnerabilidades técnicas y los riesgos de seguridad de información.

El diseño propuesto del Sistema de Gestión de Seguridad de Información proporcionó a la Gerencia General dirección y apoyo para gestionar la seguridad de información del Servicio de Administración Tributaria, debido a que se ha propuesto realizar la gestión de los riesgos de seguridad de información mediante la implementación los controles y políticas preservando con ello la disponibilidad, confidencialidad e integridad de los activos de información.

Finalmente, se han establecidos las conclusiones y recomendaciones que han permitido identificar la importancia de la implementación del modelo propuesto del Sistema de Gestión de Seguridad de la Información para el cumplimiento de los objetivos estratégicos de la Administración Tributaria y la adecuada gestión de los riesgos a los que se encuentran expuestos la institución.

Palabras Clave: Seguridad, riesgos, políticas, controles, información.

Abstract

The objective of the investigation was the design of an Information Security Management System to protect the information assets of the Tax Administration Service of the Northern Zone of Peru; complying with Ministerial Resolution No. 166-2017-PCM, which provides for the mandatory use of the Peruvian Technical Standard "NTP-ISO/IEC 27001:2014 in all entities that are part of the National Information System.

The research is descriptive because existing situations have been observed; Likewise, the techniques used for data extraction were collected in an organized and structured manner through interviews and documentary review, which has allowed knowing and analyzing the current state of the Tax Administration according to the requirements and objectives of control and controls that the standard has, analyze its organizational context, define its security structure, information security policies and the resources necessary to carry out the design. Additionally, information assets, technical vulnerabilities and information security risks were identified.

The proposed design of the Information Security Management System provided the General Management with direction and support to manage the information security of the Tax Administration Service, due to the fact that it has been proposed to manage information security risks through the implementation controls and policies thereby preserving the availability, confidentiality and integrity of information assets.

Finally, the conclusions and recommendations have been established that have made it possible to identify the importance of the implementation of the proposed model of the Information Security Management System for the fulfillment of the strategic objectives of the Tax Administration and the adequate management of the risks to the that are exposed to the institution.

Keywords: Security, risks, policies, controls, information.

Dedicatoria

A Dios y mi Virgen de la Puerta, por permitirme llegar hasta esta etapa de mi vida, por darme salud y las fuerzas que necesito para ir cumpliendo las metas que me proponga.

A mis padres, Grumencio y Miryam, porque ellos saben el esfuerzo que hay detrás de cada meta trazada y cumplida, por su empeño por darme cada día lo mejor en cada momento enseñándome que con esfuerzo todo se puede lograr, por sus sabios consejos y sobre todo por su gran amor.

A mis hermanos, Sandra y Álvaro, porque ellos me enseñan que cada día se puede ser mejor, cada día se vuelve a ser niña y a disfrutar de los pequeños momentos que se harán eternos.

Agradecimientos

A la Universidad Privada del Norte, por brindarme las herramientas necesarias para ampliar mis conocimientos y poder continuar desarrollándome ampliamente en el ámbito laboral.

A mí asesor el Dr. Alberto Mendoza de los Santos, por su paciencia, tiempo y constante asesoría en el desarrollo de la presente investigación, muy agradecida y orgullosa de contar con su ayuda.

A todas las personas que me apoyaron directa e indirectamente en el desarrollo de la presente investigación.

Tabla de Contenidos

Índice de tablas

Índice de figuras

I. INTRODUCCIÓN

I.1. Realidad problemática

Hoy en día la información es considerada como uno de los activos más importantes de las organizaciones y por ello se deben de desarrollar mecanismos que permitan proteger la información de las amenazas a las que se encuentra expuesta como producto de la evolución constante de las tecnologías de información y comunicaciones; esta seguridad se consigue mediante la implementación de controles los que necesitan ser establecidos, implementados, monitoreados y en constante mejora para asegurar el cumplimiento de los objetivos de la seguridad de información además de que se pueda asegurar la continuidad de los procesos de negocio.

A lo anterior se puede agregar que el estado peruano mediante Resolución Ministerial N°004-2016-PCM, modificada por la Resolución Ministerial Nº 166-2017-PCM, 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. 2ª Edición", y dispone la creación del Comité de Gestión de Seguridad de información en todas las entidades integrantes del Sistema Nacional de Informática (El Peruano, 2019); donde establece como "prioridad el uso de herramientas de tecnologías de información para mejorar los procesos que llevan a cabo, con la finalidad de satisfacer las necesidades que la sociedad peruana demanda, buscando la confianza del ciudadano en los sistemas estatales a los cuales accede; como apoyo a las entidades públicas". Así mismo, ha dispuesto que la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI), adscrito a la Presidencia del Consejo de Ministros, coordine de manera permanente con las entidades públicas integrantes del Sistema Nacional de Informática respecto de la aplicación de la normatividad vigente. (CODESI, 2005).

La Administración Tributaria; encargado de organizar y ejecutar la administración, fiscalización y recaudación de todos los ingresos municipales, tributarios y no tributarios que se generan dentro del distrito de su jurisdicción, forma parte del Sistema Nacional de Informática, por lo tanto se encuentra en la obligación de cumplir con los lineamientos dispuestos en la NTP-ISO/IEC 27001:2014. Es preciso señalar que, en cumplimiento con la Resolución Ministerial N° 004-2016-PCM, la gerencia de la institución nombró en el año 2018 mediante Resolución Gerencial la conformación del comité de Seguridad de Información con la finalidad de dar cumplimiento a lo establecido, sin embargo en la actualidad aún no se cuenta con una estructura de gestión para iniciar y controlar la implantación del Sistema de Gestión de Seguridad de Información, todo esto aumentó el riesgo a que se produzcan incidentes de seguridad de información; tales como: filtración de información confidencial, infección con malware (ransomware .SSPQ y virus .ZEPTO), falta de control en la realización de copias de seguridad, antivirus con licencia caducada, inadecuado control de mantenimiento de equipos del Centro de Datos, la institución cuenta con políticas para el control de cuentas de usuario para el acceso en los sistemas informáticos las cuales no son administradas de manera adecuadas motivo por el cual se

logró detectar accesos no autorizados a los sistemas, divulgación de contraseñas, alteraciones intencionadas de los datos de las áreas críticas, el acceso al área restringida donde se realiza el tratamiento de información no es controlado de manera adecuada debido a que todo el personal tiene acceso al mismo; que originaron pérdidas económicas además de la reducción de la productividad de los colaboradores.

Este escenario nos obliga a contar con un Sistema de Gestión de Seguridad de Información, que es un conjunto de políticas y procesos para gestionar eficientemente la información asegurando la confidencialidad, disponibilidad e integridad de los activos de información de la Administración Tributaria cuya finalidad es permitir gestionar los riesgos de manera adecuada y establecer un plan de respuesta mucho más rápido y eficaz frente a incidentes de seguridad de información.

I.2. Pregunta de investigación

I.2.1. Pregunta general

¿Cómo contribuye el diseño de un Sistema de Gestión de Seguridad de Información en los activos de información del Servicio de Administración Tributaria de la Zona Norte del Perú?

I.3. Objetivos de la investigación

I.3.1. Objetivo general

Diseñar un Sistema de Gestión de Seguridad de Información para proteger los activos de información del Servicio de Administración Tributaria de la Zona Norte del Perú.

I.3.2. Objetivos específicos

- Identificar el estado actual de la institución en materia de seguridad de información.
- Realizar la identificación y el análisis de los activos de información de la institución.
- Realizar el análisis de riesgos a los que se encuentra expuestos la institución.
- Seleccionar los controles y objetivos de control de la seguridad de información ajustados a los riesgos detectados.

I.4. Justificación de la investigación

I.4.1. Social

La investigación repercutirá socialmente cambiando el paradigma que tienen actualmente los usuarios de Administración Pública, ya que al aceptar el diseño propuesto se encaminaran a una gestión de riesgos de seguridad de información asegurando el compromiso que deben tener los usuarios con la seguridad de información.

I.4.2. Practica

La investigación brindó los lineamientos realizar la selección de controles que permitirán proteger los activos de información y con ello preservar la confidencialidad, integridad y disponibilidad de los mismos, elementos esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen necesarios para lograr los objetivos institucionales.

I.4.3. Teórica

La investigación servirá de apoyo a otros estudios debido a que se elaboró en cumplimiento con lo establecido en la norma técnica peruana NTP-ISO/IEC 27001:2014; mediante la cuantificación de los riesgos a los que se encuentran expuestos los activos de información en la institución.

I.4.4. Metodológica

La investigación sirve como antecedente de futuras investigaciones debido a que pueden usarse como modelo de investigaciones a entidades miembros del Sistema Nacional de Informática, teniendo en consideración que la investigación se enfocó en el tipo de investigación aplicada; con un nivel de investigación descriptivo; es decir, se permitió detallar eventos producidos en un determinado momento los que permitieron realizar el Diseño del Sistema de Gestión de Seguridad de Información.

I.5. Alcance de la investigación

Mediante la investigación se propuso el diseño de un Sistema de Gestión de Seguridad de Información con la finalidad de proteger los activos de información de la institución, de esta forma se logrará mantener la confidencialidad, integridad y disponibilidad de la información. Es preciso señalar que la investigación no desarrolló las etapas de implementación, revisión y mantenimiento del Sistema de Gestión de Seguridad de Información; únicamente se desarrolló la etapa de planeamiento en donde se realizó el diagnóstico de la situación actual, diseño y generación del SGSI.

La adopción de un SGSI constituye una decisión estratégica mediante la cual se busca preservar la información generando confianza a las partes interesadas debido a que los riesgos son manejados; sin embargo en base a los resultados obtenidos se dispuso que la toma de decisiones sobre la implementación del SGSI quedó a cargo de la Gerencia General de la institución. Los objetivos de control y controles que han sido propuestos de implementación fueron seleccionados mediante la Declaración de Aplicabilidad de la NTP-ISO/IEC 27001:2014 (Tabla N° 25); así también nos muestra si los objetivos de control o controles se encuentran operando, los que fueron excluidos, así como la justificación del porque fueron innecesarios o no requeridos por la institución.

Los controles que fueron seleccionados luego del análisis se muestran en la Tabla N°01;

Tabla N° 01: Controles seleccionados durante el proceso del tratamiento del riesgo

Dominio	Objetivo de Control	Control
A.5. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN	A.5.1. Dirección de la Gerencia para la Seguridad de la Información	A.5.1.1. Políticas para la seguridad de información
		A.5.1.2. Revisión de las políticas para la seguridad de la información
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN	A.6.1. Organización Interna	A.6.1.1. Roles y Responsabilidades para la seguridad de la información
		A.6.1.2. Segregación de Funciones
A.8. GESTIÓN DE ACTIVOS	A.8.1. Responsabilidad de los Activos	A.8.1.1. Inventario de Activos
		A.8.1.2. Propiedad de los Activos
		A.8.1.3. Uso aceptable de los activos
	A.8.2. Clasificación de la Información	A.8.2.1. Clasificación de la Información
		A.8.2.2. Etiquetado de la Información
		A.8.2.3. Manejo de Activos
	A.8.3. Manejo de los Medios	A.8.3.1. Gestión de Medios Removibles
A.9. CONTROL DE ACCESOS	A.9.1. Requisitos de la Empresa para el Control de Accesos	A.9.1.1. Política de Control de Accesos
		A.9.1.2. Accesos a redes y Servicios de red
	A.9.2. Gestión de Accesos de usuario	A.9.2.1. Registro y baja de usuarios
		A.9.2.4. Gestión de información de autenticación secreta de usuario
		A.9.2.5. Revisión de derechos de acceso de usuario
		A.9.2.6. Remoción o ajustes de derechos de acceso
	A.9.3. Responsabilidad de los Usuarios	A.9.3.1. Uso de Información de autenticación secreta
	A.9.4. Control de Acceso a Sistema y aplicación	A.9.4.1. Restricción de acceso a la información
		A.9.4.2. Procedimientos de acceso seguro
		A.9.4.3. Sistema de Gestión de contraseñas
A.11. SEGURIDAD FÍSICA Y DEL AMBIENTE	A.11.1. Áreas Seguras	A.11.1.1. Perímetro de Seguridad física
		A.11.1.2. Controles de acceso físico
		A.11.1.4. Protección contra amenazas externas y ambientales
	A.11.2. Equipos	A.11.2.1. Emplazamiento y protección de equipos
		A.11.2.2. Servicio de suministro
		A.11.2.3. Seguridad en el cableado
		A.11.2.4. Mantenimiento de equipos
		A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones

		A.11.2.7. Disposición o reutilización segura de equipos
A.12. SEGURIDAD DE LAS OPERACIONES	A.12.1. Procedimientos y responsabilidades operativas	A.12.1.1. Procedimientos operativos documentados
		A.12.1.2. Gestión de cambio
		A.12.1.3. Gestión de la capacidad
	A.12.2. Controles contra código malicioso	A.12.2.1. Controles contra código malicioso
	A.12.3. Respaldo	A.12.3.1. Respaldo de la información
	A.12.4. Registro y monitoreo	A.12.4.1. Registro de eventos
	A.12.5. Control de Software en la Producción	A.12.5.1 Instalación de Software en los Sistemas Operativos
	A.12.6. Gestión de vulnerabilidad técnica	A.12.6.2. Restricciones de instalación de software
A.13. SEGURIDAD DE LAS COMUNICACIONES	A.13.1. Gestión de la Seguridad de la Red	A.13.1.2. Seguridad de los servicios de red
		A.13.1.3. Segregación en redes
	A.13.2. Transferencia de información	A.13.2.4. Acuerdos de confidencialidad o no divulgación
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	A.14.1. Requisitos de Seguridad en los Sistemas de Información	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información
A.16. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN	A.16.1. Gestión de incidentes de la Seguridad de la Información y mejoras	A.16.1.1. Responsabilidades y procedimientos
		A.16.1.2. Reporte de eventos de seguridad de la información
		A.16.1.3. Reporte de debilidades de seguridad de la información
		A.16.1.4. Evaluación y decisión sobre eventos de seguridad de la información
		A.16.1.5. Respuesta de incidentes de seguridad de la información
		A.16.1.6. Aprendizaje de los incidentes de la seguridad de información
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO	A.1.7.1. Continuidad de Seguridad de la información	A.17.1.1. Planificación de continuidad de seguridad de la información
		A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información
A.18. CUMPLIMIENTO	A.18.1. Cumplimiento con los Requisitos Legales y Contractuales	A.18.1.1. Identificación de los requisitos contractuales y legislación aplicables

II. MARCO TEÓRICO

II.1. Antecedentes

II.1.1. Antecedentes de la Investigación a nivel Internacional

En la tesis “Diseño de un SGSI (Sistema de Gestión de Seguridad de Información) basado en la ISO27001 para laboratorios de servicios farmacéuticos de Calidad SFC LTDA” (Rodriguez Correa, 2017); el autor concluye que la implementación de un SGSI establece un gran avance en las labores y reputación de la compañía, ya que las organizaciones manejan información de carácter confidencial dentro de las labores diarias siendo así indispensable preservar la seguridad de la información dando cumplimiento a los principios de confidencialidad, integridad y disponibilidad de la información.

Así mismo, en la tesis “Modelo de un Sistema de Gestión de Seguridad de la Información en la organización GEOCONSULT CS” (Fonseca Herrera, 2019); el autor concluye que al aplicar la metodología completa de establecimiento de un SGSI se desarrollan actividades que cumplen con las buenas prácticas para el aseguramiento de calidad, adicionalmente, la implementación de un SGSI resulta ser un primer paso para la continuidad de negocio, en los cuales los procesos vitales puedan contar con el respaldo suficiente en caso de falla, de esta forma las organizaciones podrán seguir siendo un proveedor de servicios confiables.

Por otro lado, el autor de la tesis “Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio” (Guano Zapata, 2020); concluye que la información como activo importante para la continuidad y éxito de cualquier organización; debe ser protegida y mantenerla segura, esto mediante la implantación de un SGSI alineados a las normas internacionales ISO 27000- 27001 y 27002; las cuales van a permitir identificar los riesgos en el entorno de la organización recomendando las medidas necesarias para mitigar dichos riesgos.

II.1.2. Antecedentes de la Investigación a nivel Nacional

En la Tesis, “Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú” (Salinas Rodríguez, 2017); en donde se evaluaron los niveles de riesgos a los que se encuentran expuestos una entidad bancaria y desarrollar la propuesta de implementación del sistema de gestión de seguridad de la información bajo la norma ISO/IEC 27001:2005 y las etapas del modelo Deming (Plan-Do-Check-Act) la cual garantiza que se logren los objetivos de la herramienta de seguridad y beneficiar a la empresa en la protección de sus activos.

Así mismo, “Diseño e Implementación de un Sistema de Gestión de Seguridad de Información para proteger los activos de información de la Clínica MEDCAM PERÚ SAC” (Cruz Dias & Fukusaki Infantas, 2017); los autores concluyen que la implementación de un SGSI garantiza que los riesgos de la seguridad de información

son conocidos, asumidos, gestionados y minimizados; de esta manera se protege la información de un amplio rango de amenazas.

De igual forma, en la tesis "Relación de la NTP ISO/IEC 27001:2008 EDI y la seguridad de la Información en los Ministerios del Estado Peruano al 2015" (Flores Solis & Guerra Farfan, 2017) los autores concluyen que pese a la obligatoriedad de la implementación de la norma en las entidades públicas no se ha logrado un nivel de desarrollo definido de la misma, debido a que existen factores que dificultan el proceso de implementación del SGSI en las instituciones públicas, tales como la capacitación y concientización del capital humano, así mismo, los autores concluyen que se deben aplicar estrategias necesarias para la concientización del personal en seguridad de la información y dar cumplimiento a lo estipulado en la norma.

Por otro en la tesis, en la tesis "Implementación de Controles y Cumplimiento de Requisitos de la ISO/IEC 27001:2013 para la seguridad de información de una PYME Consultora" (Crystobal & Mechan, 2018) ; el autor identifica que la implementación de los controles de la mencionada norma mejoran la seguridad de la información en el proceso CORE y en los procesos involucrados; utiliza la metodología del ciclo de Deming (PDCA) , la cual se divide en cuatro fases: planear, hacer, verificar y actuar; para establecer, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información; finalmente el autor concluye que la implementación de los controles cumple con los requisitos mínimos aceptables relacionados con la norma ISO/IEC 27001:2013, en consecuencia, se mejoró significativamente la seguridad de información.

Así mismo, el autor de la tesis "Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/ IEC 27001:2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones" (Torres León, 2018); concluye que gestionar los riesgos y ejecutar los niveles de aplicabilidad de los controles logra reducir a niveles aceptables de ocurrencia en los riesgos que afecten los activos de información, además el autor establece que el factor humano es crítico para la implementación de cualquier sistema de Gestión es por ello, que se debe formar y concientizar al personal sobre la importancia de su rol para lograr la implementación exitosa.

II.2. Bases Teóricas

III.2.1. Comisión Multisectorial para el Desarrollo de la Sociedad de la Información – Mesa 5

Creada en el 2003 mediante Resolución Ministerial Nº 181-2003-PCM, tiene como finalidad establecer las herramientas necesarias que permitan el acceso de las personas a las ventajas que derivan del desarrollo de las comunicaciones y expansión de las TI (CODESI, 2005). Esta comisión está organizada en seis mesas de trabajo; siendo la Mesa 5: Gobierno Electrónico, la encargada de formular las estrategias y

recomendaciones para mejorar la eficiencia, transparencia y eficacia de la administración pública al servicio de la comunidad con el desarrollo, implementación y sostenibilidad del gobierno electrónico. (CODESI, 2005)

III.2.2. Oficina Nacional de Gobierno electrónico e Informática ONGEI

Creada en junio del 2003, con el finalidad de liderar los proyectos, la normatividad y las diversas actividades en materia de Gobierno Electrónico que realiza el estado; entre sus actividades permanentes están: (ONGEI, 2017)

- Normatividad Informática
- Seguridad de Información
- Desarrollo de proyectos en Tecnologías de información y comunicación
- Capacitación y difusión en temas de gobierno electrónico
- Modernización y descentralización del estado
- Desarrollo de la sociedad de información en el Perú

III.2.3. Resolución Ministerial N° 004-2016-PCM

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. 2ª Edición”, en todas las entidades integrantes del Sistema Nacional de Informática. (ElPeruano, 2016)

III.2.4. Norma Técnica Peruana NTP-ISO/IEC 27005:2009

Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información; esta norma proporciona directrices para la gestión de riesgos de seguridad de la información. Es compatible con los conceptos generales especificados en la norma técnica peruana NTP-ISO/IEC 27001:2014 y está diseñado para ayudar a la ejecución satisfactoria de seguridad de la información basado en un enfoque de gestión de riesgos (NTP-ISO/IEC27005:2009, 2011).

III.2.5. NTP-ISO/IEC 27001:2014. Tecnología de información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos

Norma técnica peruana elaborada con la finalidad de brindar los requisitos necesarios para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de seguridad de información; así mismo, los requerimientos para la implementación de controles de seguridad para las necesidades de una organización, un sector de la misma, o un proceso, según el alcance del SGSI. De igual forma se establece la documentación exigida para su certificación en el caso del cumplimiento de todos los requisitos. Así mismo, en el Anexo A de la mencionada norma se

establece los controles que deben ser implementados en la organización para garantizar la seguridad de información. (NTP-ISO/IEC27001-2014, 2014)

III.2.6. Norma Internacional ISO/IEC 31000:2018

Gestión del Riesgo – directrices. Esta norma internacional aporta a la organización herramientas para integrar la gestión de riesgos en sus actividades incluyendo la toma de decisiones por parte de las gerencias; ya que requiere una organización implicada con la adecuada gestión de amenazas y riesgos. (ISO31000, 2021)

III.2.7. Norma Internacional ISO/IEC 31010:2019

Gestión de riesgos. Técnicas de evaluación de riesgos Esta norma internacional facilita orientación sobre la selección y aplicación de técnicas para evaluar riesgos en una amplia gama de situaciones. (ISO31010:2019)

III.2.8. Riesgo de Seguridad de Información

Posibilidad que una amenaza determinada explote las vulnerabilidades de los activos y cause daño a la organización; es considerada así como la combinación de la probabilidad de un evento y sus consecuencias. El riesgo indica lo que podría pasarle a los activos si no se protegen adecuadamente. Es importante saber qué características son de interés de cada activo, así como saber en qué medida las características están en peligro, es decir, analizar el sistema. (NTP-ISO/IEC27005:2009, 2011)

III.2.9. Objetivos de Control y Controles de seguridad de información

Los controles de seguridad son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos. El objetivo de control en tecnologías de información se define como una sentencia del resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad de tecnología de información particular. (ISO/IEC27002:2013)

III.2.10. Requisitos de la NTP-ISO/IEC 27001:2014.

Los Requisitos de la NTP-ISO/IEC 27001:2014 se adaptan a las necesidades de las instituciones;

- Contexto de la Organización; la organización debe determinar los aspectos internos y externos relevantes para el cumplimiento del propósito.
- Liderazgo; la alta dirección debe mostrar el liderazgo y compromiso respecto del sistema de Gestión de seguridad de Información.
- Planificación; Se debe determinar los riesgos que deben ser tratados.

- Soporte; La organización debe determinar y otorgar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI
- Operación; la organización debe controlar los procesos necesarios para el cumplimiento de los requisitos de seguridad de información.
- Evaluación de Desempeño; la organización debe evaluar el desempeño de la seguridad de información y la efectividad del SGSI.
- Mejora; la organización debe mejorar continuamente la conveniencia, adecuación y efectividad del SGSI. (NTP-ISO/IEC27001-2014, 2014)

III.2.11. Ciclo de Deming

El ciclo de Deming es llamado también modelo PDCA, es el sistema más utilizado para la implantación de planes de mejora continua.

Está compuesto de 4 etapas de manera que al finalizar la última de ellas se comienza con la primera nuevamente; esto permite que la efectividad sea evaluada de manera continua, incorporando nuevas mejoras. (Deming, 2021)

La norma NTP-ISO/IEC 27001:2014 incluye también el ciclo de Deming en sus cuatro etapas para la implementación y mantenimiento del SGSI:

- Planificar; se establecen los objetivos y procesos necesarios para conseguir los resultados según las especificaciones del cliente.
- Hacer; se implantan los procesos
- Verificar; se revisan y evalúan tanto los servicios como los procesos comparándolos con las políticas, los objetivos y requisitos de información sobre los resultados obtenidos.
- Actuar; comienzan a emprender acciones para mejorar el rendimiento del SGSI. (Deming I. 2., 2021)

III.2.12. Confidencialidad

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados; es decir, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. (Firma-e, 2014)

III.2.13. Integridad

Para la seguridad de información, integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas; es decir, que los datos sean exactamente fueron creados sin alteraciones ni manipulaciones por parte de terceros. (NTP-ISO/IEC27001-2014, 2014)

III.2.14. Disponibilidad

La información puede ser accedida en el momento que sea requerida a través de canales adecuados siguiendo los procesos correctos. (Firma-e, 2014)

III.2.15. Amenazas

Suceso desfavorable que puede ocurrir teniendo consecuencias negativas sobre los activos informáticos provocando su indisponibilidad, funcionamiento incorrecto o pérdida de valor. (CiberSeguridad, 2014)

III.2.16. Vulnerabilidades

Debilidad que se presenta en los activos que puede ser aprovechado por alguna fuente de amenaza para atentar contra las políticas de seguridad. (NIST800, 2014)

II.3. Marco conceptual

II.3.1. Seguridad de Información

Se entiende por seguridad de información a todas aquellas medidas preventivas y reactivas que permitan resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de la misma (Carralli, 2004). De lo dicho anteriormente se reafirma que la información es un activo clave para las organizaciones y como tal está expuesta a amenazas que ponen en riesgo su valor, que es necesario preservar incorporando para ello los principios del Gobierno de la Seguridad de la Información como parte integral de las estrategias, procesos, personal en el marco de Gobierno de las Tecnologías de Información. (ISO/IEC-27002, 2013) (NTP-ISO/IEC17799:2007, 2007)

II.3.2. Activos Informáticos

Un activo es algo que tiene valor para la organización, sus operaciones comerciales y continuidad. Por esta razón se necesitan protegerse para asegurar la correcta operación del negocio y continuidad de sus operaciones. (Alexander, 2007)

Se deben tener en cuenta los siguientes criterios sobre los activos informáticos de las organizaciones:

- Es importante llevar un control sobre los activos de informática, tanto para control interno como externo,
- Se deben implementar políticas claras para la asignación y control de accesos a los activos. (Informáticos, 2013)

II.3.3. Sistema de Gestión de Seguridad de Información

El sistema de gestión de seguridad de información - SGSI - tiene como finalidad preservar la confidencialidad, integridad y disponibilidad de la información mediante el

proceso de gestión de riesgos (NTP-ISO/IEC27001-2014, 2014); con un enfoque sistemático para gestionar y proteger los activos informáticos con la aplicación de controles que son necesarios para establecer las reglas de seguridad de la información. (ISOTools-ISO27001, 2019)

El SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, de tal manera que va permitir la toma de decisiones sobre las estrategias a seguir con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir; es decir, la organización conoce los riesgos a los que se encuentran sometidos sus activos informáticos y los asume, minimiza, transfiere o controla mediante un sistema definido, revisado y mejorado constantemente. (SGSI-ISO27000.ES)

La documentación necesaria que implique que el SGSI garantice la confidencialidad, integridad y disponibilidad de la información son:

- Alcance del SGSI: declaración de hasta que ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas.
- Política y objetivos de seguridad: Documento que establece el compromiso de la organización en la gestión de la seguridad de la información.
- Metodología para la evaluación del riesgo, se trata de cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado.
- Informe de evaluación de riesgos: Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- Plan de tratamiento de riesgos: Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- Procedimientos para el control de la documentación: son los procedimientos que aseguran la planificación, operación y control de los procesos de seguridad de la información.
- Registros: Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- Declaración de aplicabilidad: documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

III. HIPÓTESIS

III.1. Operacionalización de variables

Debido a que el presente trabajo de investigación según su alcance tiene un nivel descriptivo, se ha tenido a bien considerar la variable independiente que sustenta la presente investigación, la cual se define como “Diseño de un Sistema de Gestión de Seguridad de Información para proteger los activos de información del Servicio de Administración Tributaria de la Zona Norte del Perú” (Tabla N° 02).

III.2.1. Variable Independiente:

Diseño de un Sistema de Gestión de Seguridad de Información para proteger los activos de información del Servicio de Administración Tributaria de la Zona Norte del Perú.

Tabla N° 02: Operacionalización de Variables

Variable	Tipo de Variable	Operacionalización	Categorías o Dimensiones	Definición	Indicador	Nivel de Medición	Unidad de Medida	Índice	Valor
Diseño de un Sistema de Gestión de Seguridad de Información para proteger los activos de Información	Variable Independiente	Esta variable será medida a través de tres dimensiones: Controles de seguridad existentes en la institución, Nivel de Riesgo y los activos con los que cuenta la institución.	Controles de seguridad	Son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar que los objetivos del negocio serán alcanzados. (ISO/IEC27002:2013)	Cantidad de controles existentes	Escala de Razón	Unidad	Índice de controles existentes	17 Controles
			Riesgos	Posibilidad que una amenaza específica explote las vulnerabilidades de los activos y cause daño a la organización; es considerada así como la combinación de la probabilidad de un evento y sus consecuencias. (NTP-ISO/IEC27005:2009, 2011)	Nivel de Riesgo	Ordinal	Puntaje	Índice de Riesgos identificados	NR=I x P Riesgo alto (12-16) Riesgo medio (8-9) Riesgo bajo (1-6)
			Activos	Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y continuidad. (Alexander, 2007)	Valoración de activos	Ordinal	Puntaje	Índice de activos evaluados	1: Insignificante 2: Bajo 3: Mediano 4: Alto 5: Muy Alto

Fuente: Elaboración Propia

III.2. Propuesta de solución

Mediante la presente investigación, se propone el diseño de un Sistema de Gestión de Seguridad de Información para proteger activos de información de la Administración Tributaria como parte del cumplimiento de la Resolución Ministerial Nº 166-2017-PCM, que dispone 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"; cuya finalidad es proteger la información de la institución y los activos de información utilizados para el procesamiento de la misma, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información, teniendo en consideración el anexo A de la NTP-ISO/IEC 27001:2014, controles que han sido seleccionados previa evaluación siendo un total de 39 controles que servirán de base para el desarrollo del Sistema de Gestión de Seguridad de Información que han sido seleccionado según la Declaración de Aplicabilidad descritos en la Tabla N° 25 .

Los recursos y costos asociados al proyecto se encuentran en la Tabla N° 10, los mismos que ascienden de 2, 241,855.75 soles, sin embargo, se evidenció que en la actualidad existe un proyecto de Renovación del Centro de Datos que esta valorizado en 2, 221,936.94 soles los cuales se reducen del costo de la implementación del SGSI quedando a evaluación por parte de la Gerencia el monto total de 19,918.81 soles.

Es compromiso de los Gerentes y responsables de oficina establecer de manera clara el apoyo de la dirección, funcionamiento y cumplimiento de los controles aplicados para la Seguridad de Información; debido a que, los objetivos que se desean alcanzar luego de implementación del Sistema de Gestión de Seguridad de Información son los siguientes:

Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de la institución en la administración del riesgo.

Compromiso de todos los colaboradores de la institución en todo el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.

Mantener las Políticas de Seguridad de Información de la Administración Tributaria actualizada con la finalidad de asegurar su vigencia y nivel de eficacia.

IV. DESCRIPCIÓN DE MÉTODOS Y ANÁLISIS

IV.1. Tipo de investigación

Según el propósito el tipo de investigación es aplicada; debido a que los estudios aplicados se caracterizan por resolver un problema mediante la aplicación o utilización de los conocimientos adquiridos. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014, pág. 42) .

IV.2. Nivel de investigación

Según el alcance el nivel de investigación es Descriptivo; debido a que los estudios descriptivos permiten detallar situaciones o eventos, es decir, como es y cómo se manifiesta determinado fenómeno. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014, pág. 90) .

IV.3. Diseño de investigación

El diseño de investigación es no Experimental de tipo Transaccional o transversal, ya que los datos recolectados serán en un determinado momento. El propósito de este diseño de investigación es observar y analizar la variable en un determinado momento sin manipularla. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014, pág. 152)

IV.4. Método de investigación

Según el esquema del enfoque el método de la investigación es deductivo, debido a que se van a extraer conclusiones lógicas en base a los resultados. (Hernandez Sampieri, Fernandez Collado, & Baptista Lucio, 2014, pág. 92)

IV.5. Población

La población está constituida por 4 colaboradores del Servicio de Administración Tributaria de la Zona Norte del Perú, quienes ocupan los cargos de: Responsable de la oficina de Tecnología de Información, Responsable de la Oficina de Calidad, Responsable de la Oficina de Planeamiento y Oficial de Seguridad.

IV.6. Muestra

El grupo experimental fue tomado de la población de 4 colaboradores del Servicio de Administración Tributaria de la Zona Norte del Perú, quienes ocupan los cargos de: Responsable de la oficina de Tecnología de Información, Responsable de la Oficina de Calidad, Responsable de la Oficina de Planeamiento y Oficial de Seguridad.

IV.7. Unidad de estudio

La Unidad de Estudio comprende a los 4 colaboradores del Servicio de Administración Tributaria de la Zona Norte del Perú, quienes ocupan los cargos de: Responsable de la

oficina de Tecnología de Información, Responsable de la Oficina de Calidad, Responsable de la Oficina de Planeamiento y Oficial de Seguridad.

IV.8. Técnicas de recolección de datos

Durante la investigación se usaron diversas técnicas de recopilación de información necesaria para realizar el diagnostico situacional y el proceso de selección de controles con la finalidad de dar cumplimiento a los objetivos propuestos, las cuales se detallan a continuación:

IV.8.1. Técnica

- Entrevista; Permite extraer información sobre el conocimiento de los usuarios sobre la seguridad de información
- Revisión Documentaria; Permite la revisión de los documentos con respecto a políticas de seguridad, inventarios de usuarios y controles de acceso.

IV.8.2. Instrumento

- Guías de entrevista basado en los requisitos del SGSI
- Guías de entrevista basado en el cumplimiento de controles del anexo A de la NTP-ISO/IEC 27001:2014
- Documentación del Servicio de Administración Tributaria de la Zona Norte del Perú

Tabla N° 03: Técnicas e Instrumentos

TECNICA	JUSTIFICACION	INSTRUMENTOS	APLICACION
Entrevista	Permite extraer información sobre el conocimiento de los usuarios sobre la seguridad de información	Guías de entrevista	Oficial de Seguridad Responsable de la Oficina de Tecnologías de Información
Revisión documentaria	Permite la revisión de los documentos con respecto a políticas de seguridad, inventarios de usuarios y controles de acceso	Documentación del Servicio de Administración Tributaria de la Zona Norte del Perú	Responsable de la Oficina de Tecnologías de Información; Responsable de Calidad

Fuente: Elaboración Propia

V. RESULTADOS

Esta propuesta de diseño del Sistema de Gestión de Seguridad de Información se desarrolló dentro del marco de referencia de la NTP-ISO/IEC 27001:2014, que tiene un enfoque basado en procesos basado en el ciclo de Deming que consta de 4 etapas necesarias para el desarrollo del SGSI, Plan-Hacer-Verificar-Actuar; el presente estudio se encuentra dentro de la primera fase "Plan"; esta fase únicamente aplica a la etapa de diagnóstico, diseño y generación del modelo del SGSI

V.1. Diagnóstico Inicial

De la información obtenida mediante las entrevistas (Anexo N° 02, Anexo N° 03) y revisión documentaria (Anexo N° 04), cuyo contenido son preguntas relacionadas a los requisitos de cumplimiento de la NTP-ISO/IEC 27001:2014 (Tabla N° 04) y controles referidos en el anexo A de la misma (Tabla N° 05); y revisión documentaria se realizó el análisis GAP o análisis de brechas con la finalidad de identificar la situación actual de la Administración Tributaria con respecto a la seguridad de la información. Este análisis determina el nivel de madurez por cada requisito de cumplimiento y controles de la mencionada norma; para ellos se estableció que el nivel mínimo acordado es de 3 (Anexo N° 01) que indica que se tienen procesos que están definidos y documentados mediante políticas, procedimientos documentados, formalizados, aprobados y difundidos a todos los colaboradores de la institución.

Tabla N° 04: Requisitos de cumplimiento NTP-ISO/IEC 27001:2014

Numeral	Clausula
4	Contexto de la Organización
5	Liderazgo
6	Planificación
7	Soporte
8	Operación
9	Evaluación del Desempeño
10	Mejora

Tabla N° 05: Controles Anexo A NTP-ISO/IEC 27001:2014

Objetivo de Control	Anexo A NTP-ISO/IEC 27001:2014
Objetivo de Control A.5.	Políticas de Seguridad de Información
Objetivo de Control A.6.	Organización de la Seguridad de Información
Objetivo de Control A.7.	Seguridad de los Recursos Humanos
Objetivo de Control A.8.	Gestión de Activos
Objetivo de Control A.9.	Control de Accesos
Objetivo de Control A.10.	Criptografía
Objetivo de Control A.11.	Seguridad Física y del Ambiente
Objetivo de Control A.12.	Seguridad de las Operaciones
Objetivo de Control A.13.	Seguridad de las Comunicaciones
Objetivo de Control A.14.	Adquisición, Desarrollo y Mantenimiento de Sistemas

Objetivo de Control A.15.	Relaciones con los Proveedores
Objetivo de Control A.16.	Gestión de Incidentes de la Seguridad de Información
Objetivo de Control A.17.	Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio
Objetivo de Control A.18.	Cumplimiento

Para la evaluación del Servicio de Administración Tributaria de la Zona Norte del Perú se tomó de referencia el modelo de madurez que propone COBIT, que establece que se pueda evaluación desde un nivel de no existente (0) hasta un nivel de optimizado (5) tal como se muestra en la Tabla N° 8. Con este modelo se puede evaluar tanto la existencia como el grado de implantación de los requisitos de cumplimiento como los 11 controles referidos en el anexo A de la NTP-ISO/IEC 27001:2014; debido a que se podrá ubicar en la escala de medición y evaluar qué acciones deben tomarse para desarrollar mejoras.

Tabla N° 06: Nivel de Capacidad - MODELO DE MADUREZ COBIT

Nivel de Madurez	Descripción	Valor
Inexistente	El control es inexistente. La empresa no reconoce la existencia de un problema a resolver.	0
Inicial	El control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe.	1
Repetible	El control esta implementado y se han desarrollado procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento y comunicación formal de los procedimientos estándar, y se deja a la responsabilidad del individuo	2
Definida	Los procedimientos se han estandarizado y documentado, y se han difundido a través del entrenamiento.	3
Administrada	Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas.	4
Optimizada	En este nivel se encuentran las entidades en las cuales se mide la efectividad de los controles con el fin de mejorarlos y optimizarlos.	5

Para la hallar el nivel de cumplimiento se tiene en consideración la puntuación según los niveles de capacidad por cada control (Tabla N° 06), que será determinado por el siguiente cálculo:

Nivel Medio Cumplimiento = Puntuación total de cada control / Nro. Controles totales

Considerando:

Tabla N° 07: Nivel de Cumplimiento - MODELO DE MADUREZ COBIT

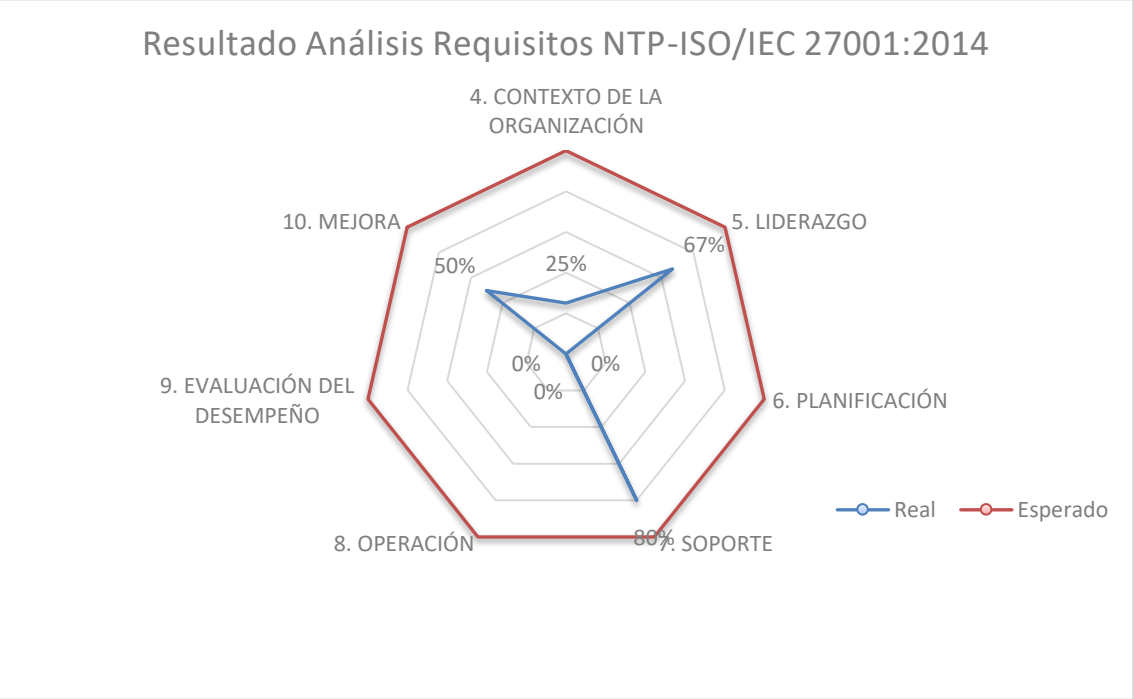
Nivel de Cumplimiento	Detalle
No Cumple	Menor a 1.65
Cumple Parcialmente	Entre 1.66 y 3.25
Cumplimiento con Requisitos de la Norma	Mayor a 3.26

V.1.1. Evaluación de los Requisitos de la NTP-ISO/IEC 27001:2014. Como resultado de la entrevista basado en los requisitos del SGSI (Anexo N° 05) se logró determinar que el nivel de cumplimiento en el que se encuentra la administración es del 32% es decir, no se cumplen con los requisitos necesarios para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de Información mientras que el 68% restante corresponde a incumplimiento de requisitos, procesos existentes que no se encuentran documentados (Tabla N° 08).

Tabla N° 08: Nivel de Cumplimiento de los Requisito de la NTP-ISO/IEC 27001:2014.

Criterio NTP-ISO/IEC 27001:2014	Nivel de Madurez	Nivel de Cumplimiento		
		Real	Esperado	Brecha
4. CONTEXTO DE LA ORGANIZACIÓN	0.75	25%	100%	75%
5. LIDERAZGO	2.00	67%	100%	33%
6. PLANIFICACIÓN	0.00	0%	100%	100%
7. SOPORTE	2.40	80%	100%	20%
8. OPERACIÓN	0.00	0%	100%	100%
9. EVALUACIÓN DEL DESEMPEÑO	0.00	0%	100%	100%
10. MEJORA	1.50	50%	100%	50%
Nivel de Cumplimiento		32%	100%	68%

Figura N° 01: Resultado Análisis Requisitos NTP-ISO/IEC 27001:2014



El diagrama radial de la Figura N° 01, representa el estado actual en cuanto al nivel de cumplimiento de los requisitos para la implementación de la NTP-ISO/IEC 27001:2014, en este se puede verificar que el requisito 4. Conocer el contexto de la organización tiene un nivel de cumplimiento del 25% debido a que la administración

no cuenta con la documentación y aprobación del SGSI; sin embargo, se puede identificar que en el año 2018 mediante Resolución Gerencial se determinó la conformación del comité de Seguridad de la Información en la administración en la que se establecen las partes interesadas para la elaboración y asegurar el cumplimiento del SGSI.

El requisito 5. Liderazgo refiere al compromiso de las Gerencias durante el proceso de implantación del SGSI, se puede evidenciar que el nivel de cumplimiento de este requisito es del 67% teniendo así que reforzar la cultura de seguridad de la información dentro de la administración para garantizar el compromiso de la gerencia con la aportación de recursos tanto humanos como materiales para el desarrollo de los objetivos de la seguridad de información.

El requisito 7. Soporte indica determinar los recursos necesarios para la implantación del SGSI; se puede evidenciar que la administración tiene un nivel de cumplimiento del 80%, es decir se cumple parcialmente con el requisito debido a que la administración cuenta con personal idóneo a nivel técnico, capaz de resolver los problemas que se encuentran, y evaluar y gestionar los riesgos asociados.

El requisito 10. Mejora el nivel de cumplimiento refiere al tratamiento de las no conformidades de tal forma que se van a tener los datos necesarios para evaluar las causas de problemas y el impacto en el sistema; para este requisito se puede evidencias que el nivel de cumplimiento es del 50%, es decir no se cumple con este requisito debido a que los documentos encontrados que respaldan los procedimientos de no conformidades no se encuentran actualizados.

Es preciso señalar que para los requisitos 6. Planificación y 8. Operación es nulo, debido a que no se han establecido tiempos ni asignaciones de responsabilidades en los procesos y controles del SGSI y no se cuentan con planes de auditoria interna en la relación con la seguridad de información. Esto conlleva que el requisito 9. Evaluación de desempeño se encuentre en un estado inexistente, mostrando la necesidad de implementar procesos que formulen la mejora.

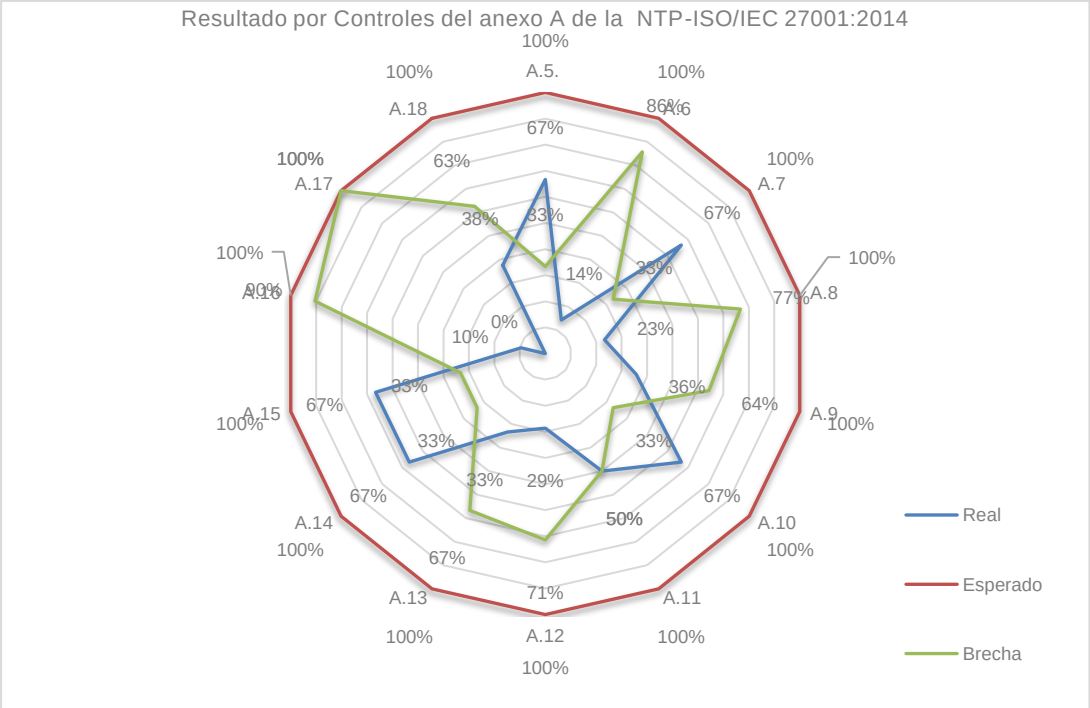
Sin embargo, la norma no nos condiciona a cumplir al 100% con los requisitos establecidos, por el contrario estos se pueden adaptar a las necesidades particulares de la administración.

V.1.2. Resultado por los Controles del anexo A de la NTP-ISO/IEC 27001:2014. Como resultado de la entrevista basada en el cumplimiento de controles del anexo A de la NTP-ISO/IEC 27001:2014 (Anexo N° 06) se logró determinar que el nivel de cumplimiento en el que se encuentra la administración es del 40%, es decir en el Servicio de Administración Tributaria de la Zona Norte del Perú existen controles que se están ejecutando sin embargo no están documentados o no se soportan en una política documentada, aprobada y de conocimiento a los colaboradores de la institución. (Tabla N° 09)

Tabla N° 09: Nivel de Cumplimiento - Resultado por los Controles del anexo A de la NTP-ISO/IEC 27001:2014.

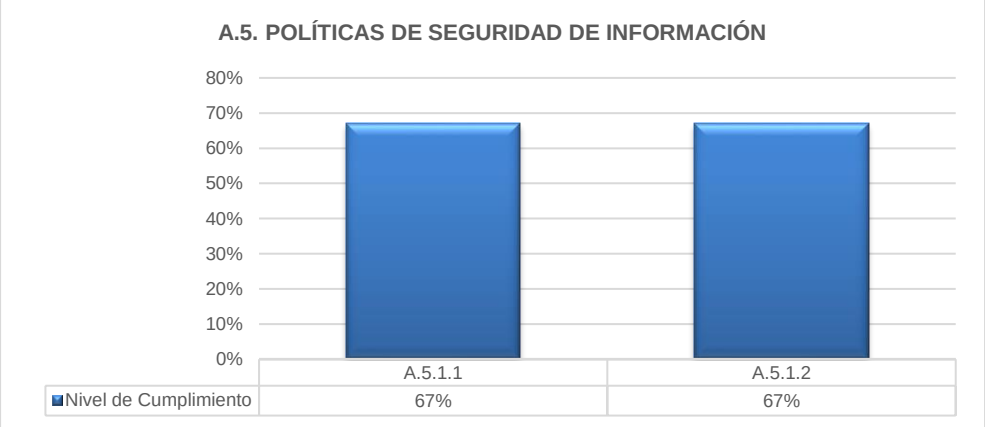
Anexo A NTP-ISO/IEC 27001:2014		Nivel de Madurez	Nivel de Cumplimiento		
			Real	Esperado	Brecha
A.5.	Políticas de Seguridad de Información	2.00	67%	100%	33%
A.6	Organización de la Seguridad de Información	0.43	14%	100%	86%
A.7	Seguridad de los Recursos Humanos	2.00	67%	100%	33%
A.8	Gestión de Activos	0.70	23%	100%	77%
A.9	Control de Accesos	1.07	36%	100%	64%
A.10	Criptografía	2.00	67%	100%	33%
A.11	Seguridad Física y del Ambiente	1.50	50%	100%	50%
A.12	Seguridad de las Operaciones	0.86	29%	100%	71%
A.13	Seguridad de las Comunicaciones	1.00	33%	100%	67%
A.14	Adquisición, Desarrollo y Mantenimiento de Sistemas	2.00	67%	100%	33%
A.15	Relaciones con los proveedores	2.00	67%	100%	33%
A.16	Gestión de incidentes de la seguridad de información	0.29	10%	100%	90%
A.17	Aspectos de seguridad de la información en la gestión de continuidad del negocio	0.00	0%	100%	100%
A.18	Cumplimiento	1.13	38%	100%	63%
Nivel de Cumplimiento			40%	100%	60%

Figura N° 02: Resultado por Controles del anexo A de la NTP-ISO/IEC 27001:2014



V.1.2.1. A.5. Políticas de Seguridad de Información

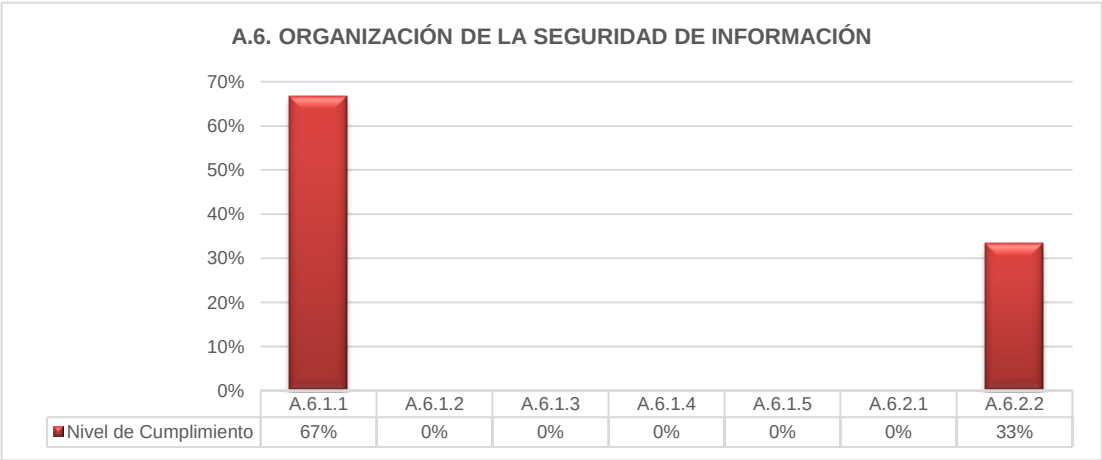
Figura N° 03: A.5. Políticas de Seguridad de Información



La Figura N° 03 nos muestra que el dominio A.5 presenta un nivel de cumplimiento del 67% con respecto al resultado esperado, dejando una brecha del 33% indicando que la institución cumple parcialmente este dominio, es decir el control se encuentra implementado y soportado mediante una política o documento de comunicación, sin embargo estos documentos no se encuentran actualizados.

V.1.2.2. A.6. Organización de la Seguridad de Información

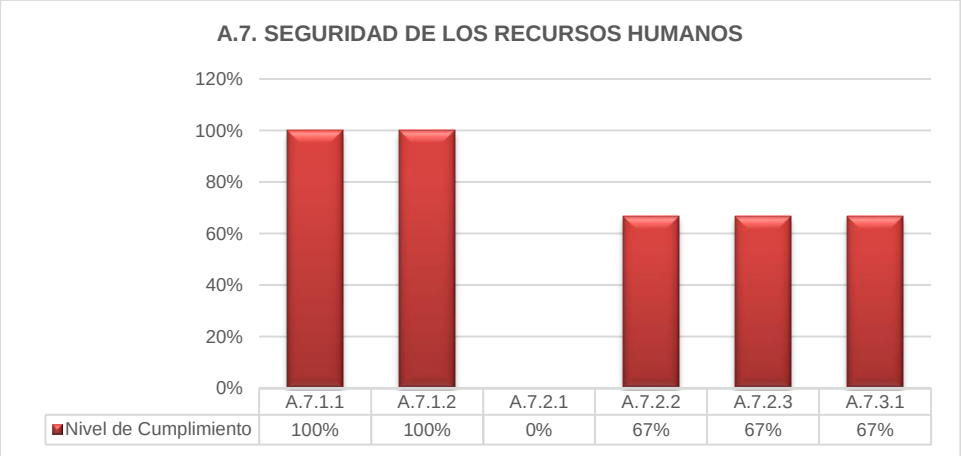
Figura N° 04: A.6. Organización de la Seguridad de Información



La Figura N° 04 nos muestra que el dominio A.6 presenta un nivel de cumplimiento del 14% con respecto al resultado esperado, dejando una brecha del 86%, es decir la institución no cumple en la mayoría de los controles de este dominio debido a que no se cuenta con el área de seguridad de información encargada de llevar a cabo la implementación del SGSI, sin embargo es preciso señalar que se evidenció que en el año 2018 mediante Resolución Gerencial se determinó la conformación del comité de Seguridad de la Información en la institución.

V.1.2.3. A.7. Seguridad de los Recursos Humanos

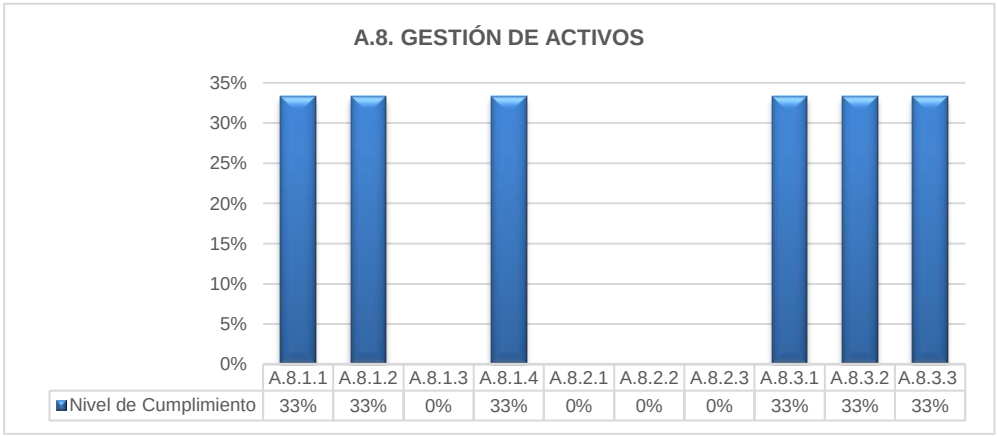
Figura N° 05: A.7. Seguridad de los Recursos Humanos



La Figura N° 05 nos muestra que el dominio A.7 presenta un nivel de cumplimiento del 67% con respecto al resultado esperado, dejando una brecha del 33%, es decir la institución cumple parcialmente debido a que los controles se encuentran implementados y documentados, sin embargo es preciso señalar que no se han definido procedimientos que garanticen la seguridad de la información al finalizar el vínculo laboral.

V.1.2.4. A.8. Gestión de Activos

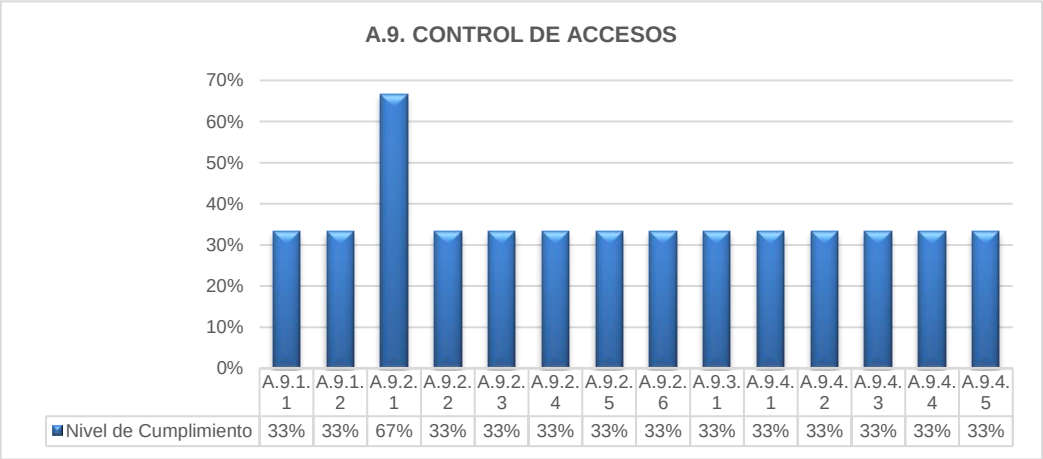
Figura N° 06: A.8. Gestión de Activos



La Figura N° 06 nos muestra que el dominio A.8 presenta un nivel de cumplimiento del 20% con respecto al resultado esperado, dejando una brecha del 80%, es decir la institución no cumple con todos los controles de este dominio debido a que se cuenta con un inventario de los activos de información, sin embargo este no se encuentra actualizado ni estandarizado de tal forma que permita dar cumplimiento a lo estipulado en el anexo A de la norma evaluada.

V.1.2.5. A.9. Control de Accesos

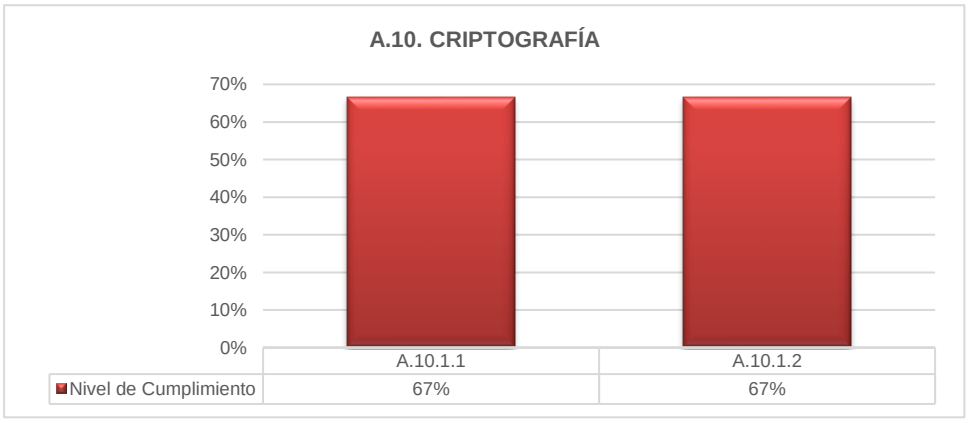
Figura N° 07: A.9. Control de Accesos



La Figura N° 07 nos muestra que el dominio A.9 presenta un nivel de cumplimiento del 36% con respecto al resultado esperado, dejando una brecha del 64%, es decir la institución cumple parcialmente con la implementación de los controles de este dominio, sin embargo estos no se encuentran documentados mediante un modelo de política.

V.1.2.6. A.10. Criptografía

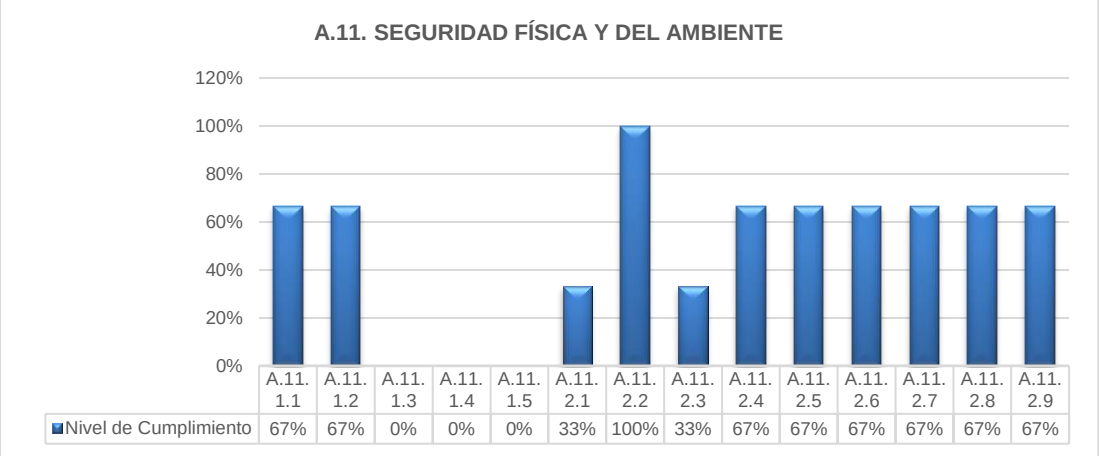
Figura N° 08: A.10. Criptografía



La Figura N° 08 nos muestra que el dominio A.10 presenta un nivel de cumplimiento del 67% con respecto al resultado esperado, dejando una brecha del 33%, es decir la institución cumple parcialmente con la implementación de los controles de este dominio debido a que a pesar de contar con procedimientos sobre el uso de criptografía, esta no se encuentra documentada en una política.

V.1.2.7. A.11. Seguridad Física y del Ambiente

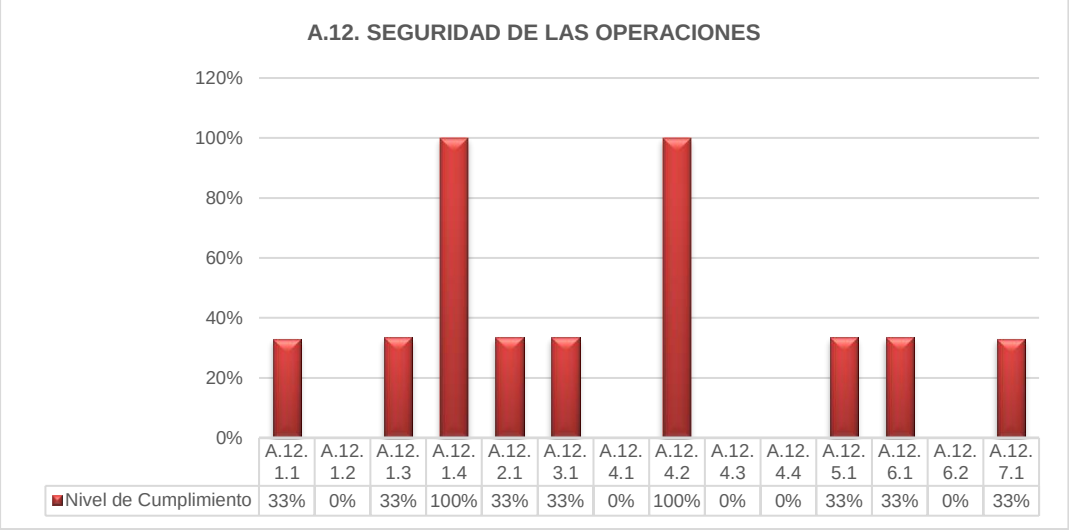
Figura N° 09: A.11. Seguridad Física y del Ambiente



La Figura N° 09 nos muestra que el dominio A.11 presenta un nivel de cumplimiento del 50% con respecto al resultado esperado, dejando una brecha del 50%, es decir la institución no cumple con la implementación de los controles de este dominio debido a que no se cuenta con un Plan de recuperación ante desastres, de igual forma se evidenció que la administración cuenta con un plan de mantenimiento preventivo realizado de manera semestral sin embargo, no se cuenta con un plan de mantenimiento correctivo de los equipos principalmente del centro de datos y centrales eléctricas.

V.1.2.8. A.12. Seguridad de las Operaciones

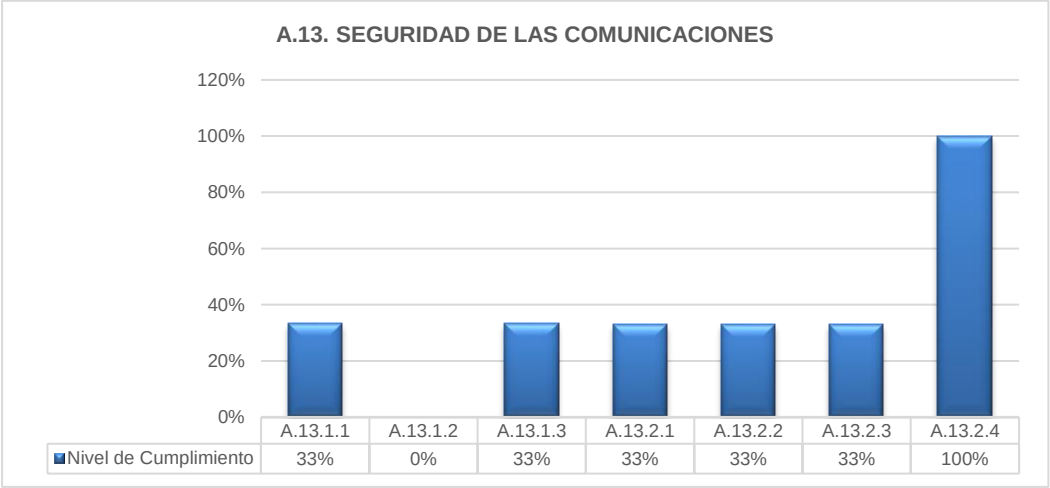
Figura N° 10: A.12. Seguridad de las Operaciones



La Figura N° 10 nos muestra que el dominio A.12 presenta un nivel de cumplimiento del 29% con respecto al resultado esperado, dejando una brecha del 71%, es decir la institución no cumple con la implementación de los controles de este dominio debido a que no se han establecido procedimientos que permitan asegurar la seguridad de las operaciones en el tratamiento de información.

V.1.2.9. A.13. Seguridad de las Comunicaciones

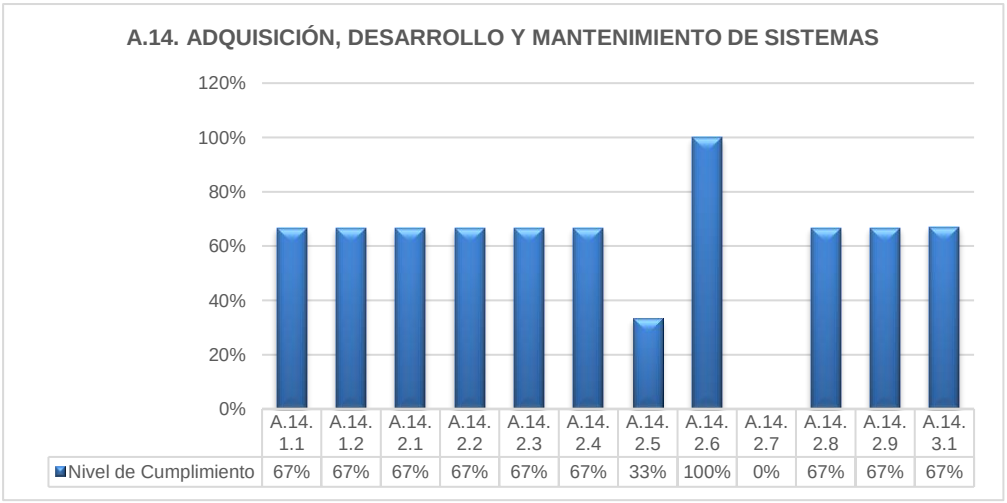
Figura N° 11: A.13. Seguridad de las Comunicaciones



La Figura N° 11 nos muestra que el dominio A.13 presenta un nivel de cumplimiento del 33% con respecto al resultado esperado, dejando una brecha del 67%, es decir la institución no cumple con la implementación de los controles de este dominio debido a que, no se cuenta con procedimiento o políticas documentadas que respalden la existencia del control.

V.1.2.10. A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas

Figura N° 12: A.14. Adquisición, Desarrollo y Mantenimiento de Sistemas



La Figura N° 12 nos muestra que el dominio A.14 presenta un nivel de cumplimiento del 67% con respecto al resultado esperado, dejando una brecha del 33%, es decir la institución cumple parcialmente con la implementación de los controles de este dominio debido a que existen los procedimientos para la implementación de seguridad de la información en el proceso de desarrollo sin embargo estos no se encuentran documentados.

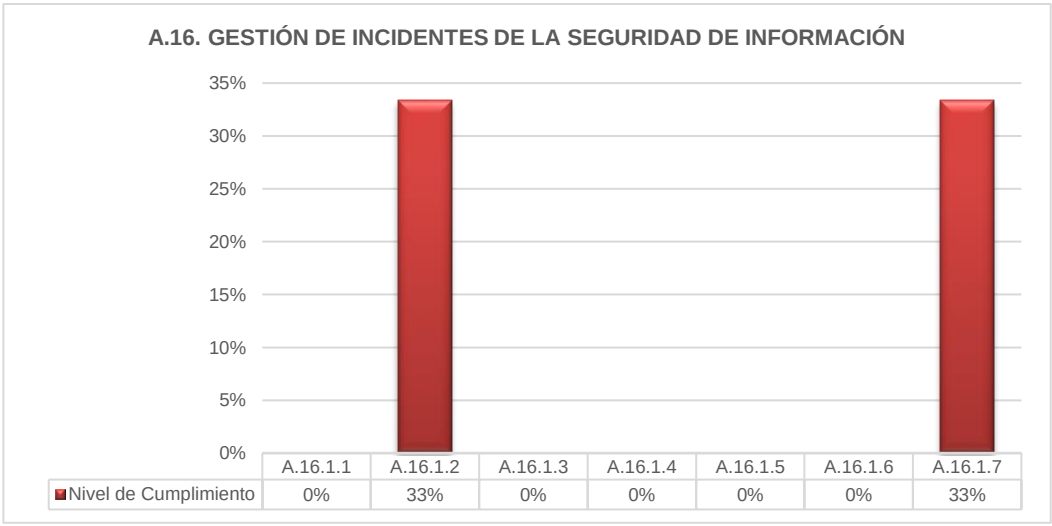
V.1.2.11. A.15. Relaciones con los Proveedores

Figura N° 13: A.15. Relaciones con los Proveedores

La Figura N° 13 nos muestra que el dominio A.15 presenta un nivel de cumplimiento del 67% con respecto al resultado esperado, dejando una brecha del 33%, es decir la institución cumple parcialmente con la implementación de controles de este dominio sin embargo, los mismos no se encuentran documentados mediante una política que los respalde.

V.1.2.12. A.16. Gestión de Incidentes de la Seguridad de Información

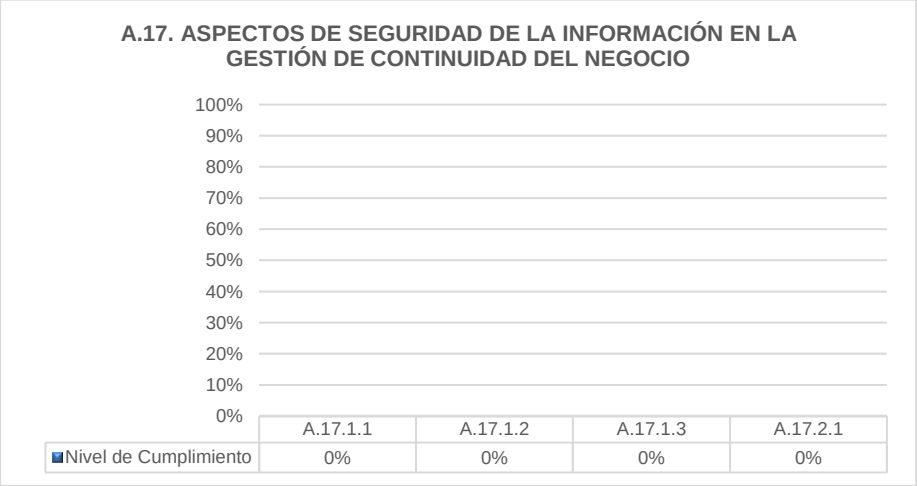
Figura N° 14: A.16. Gestión de Incidentes de Seguridad de Información



La Figura N° 14 nos muestra que el dominio A.16 presenta un nivel de cumplimiento del 10% con respecto al resultado esperado, dejando una brecha del 90%, es decir la institución no cumple con la implementación de los controles de este dominio debido a que no se ha realizado la evaluación de riesgos a los que se encuentra expuesta la administración.

V.1.2.13. A.17. Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio

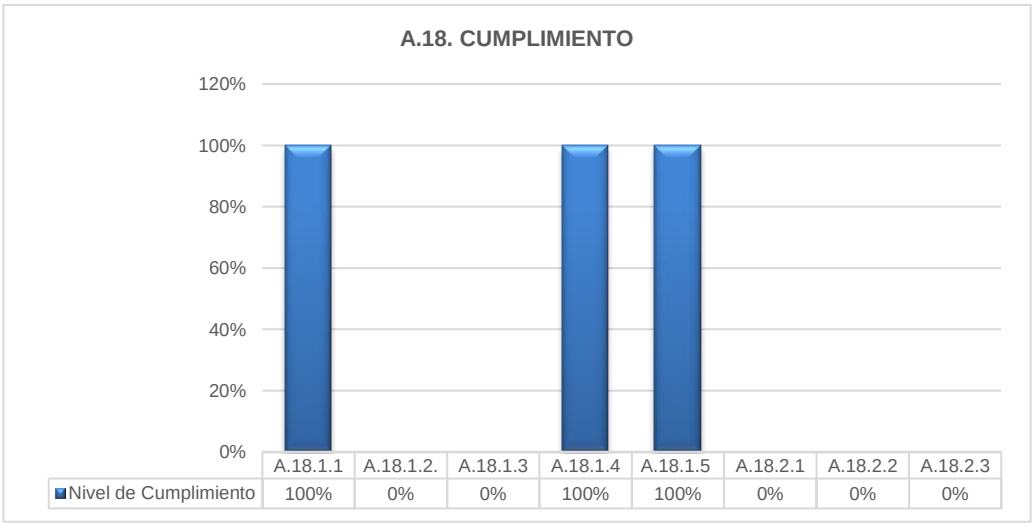
Figura N° 15: A.17. Aspectos de Seguridad de la Información en la Gestión de Continuidad del Negocio



La Figura N° 15 nos muestra que el dominio A.17 presenta un nivel de cumplimiento del 0% con respecto al resultado esperado, es decir la institución no ha implementado ningún control de este dominio debido a que no se ha elaborado el plan de continuidad de negocio frente a incidentes de seguridad de la información.

V.1.2.14. A.18. Cumplimiento

Figura N° 16: A.18. Cumplimiento



La Figura N° 16 nos muestra que el dominio A.18 presenta un nivel de cumplimiento del 38% con respecto al resultado esperado, dejando una brecha del 63%, es decir la institución no cumple con la implementación de controles de este dominio debido a no se cuenta con un SGSI documentado e implementado.

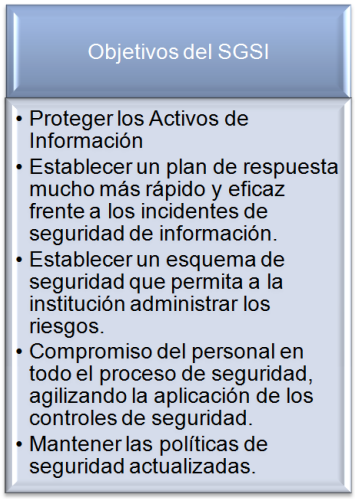
V.2. Propuesta de Diseño del Sistema de Gestión de Seguridad de Información

Como resultado del análisis realizado en base a la recopilación de información mediante el uso de las técnicas e instrumentos desarrollados en la presente investigación, se identifica a la seguridad de la información como una necesidad inmediata de implementación, basado en el diseño propuesto, el Sistema de Gestión de Seguridad de Información cuyas políticas estarán definidas y así proteger los activos de información y dar cumplimiento a la normativa vigente.

V.2.1. Análisis del Contexto Organizacional

En base a la misión, visión y objetivos estratégicos de la institución; se han determinado los objetivos bajo los cuales se deberá desarrollar el Sistema de Gestión de Seguridad de Información.

Figura N° 17: Objetivos del Sistema de Gestión de Seguridad de Información



V.2.1.1. Alcance del Sistema de Gestión de Seguridad de Información

El Sistema de Gestión de Seguridad de Información, involucra a todos los sistemas y colaboradores que tratan información, sin embargo es conveniente indicar que la implementación de políticas está a cargo de la Oficina de Tecnología de Información, por ser uno de los principales responsables del tratamiento y conservación de la información. (Anexo N° 07)

Los objetivos de control y controles propuestos de implementación han sido seleccionados mediante la declaración de aplicabilidad del Anexo A de la NTP-ISO/IEC 27001:2014 como se muestra en la tabla N° 25: Declaración de Aplicabilidad de la NTP-ISO/IEC 27001:2014; así también nos muestra si los objetivos de control o controles se encuentran operando, los que serán excluidos, así como la justificación del porque son innecesarios o no son requeridos por la institución.

V.2.1.2. Política General del SGSI

En la presente investigación se desarrolló la propuesta de definir las políticas de seguridad de la institución; estas políticas son parte de la herramienta del Sistema de Gestión de Seguridad de Información (Anexo N° 07)

V.2.2. Estructura Organizacional en función de la Seguridad de Información

Los roles y responsabilidades para la seguridad de información estarán definidos según la segregación de funciones para los miembros del comité de seguridad de información, nombrados mediante Resolución Gerencial en el año 2018. (Anexo N° 08)

V.2.3. Definición de Recursos

Para llevar a cabo cada actividades relacionadas a la implementación de los controles del anexo A de la NTP-ISO/IEC 27001:2014; donde se detalla la cantidad de días que va tomar la implementación de cada actividad.

En la Tabla N° 10 se muestra el monto total de la implementación del SGSI sería de 2, 241,855.75 soles, sin embargo, se evidenció que en la actualidad existe un proyecto de Renovación del Centro de Datos que esta valorizado en 2, 221,936.94 soles los cuales se reducen del costo de la implementación del SGSI quedando a evaluación por parte de la Gerencia General el monto total de 19,918.81 soles, a fin de determinar la viabilidad económica de la misma.

Tabla N° 10: Costos Asociados a la implementación de Controles

Propuesta de proyecto de Implementación del SGSI						
Código de Proyecto	Descripción del Proyecto	Tiempo de Ejecución (Días)	Avance	Cant.	Costo	Total
PP_SGSI_001	Configuraciones del Firewall con los roles para el control de acceso lógico	1	80%	1	-	-
PP_SGSI_002	Actualizaciones de licencias a los equipos del data center	3	0%	1	147782.74	147,782.74
PP_SGSI_003	Actualización de antivirus en las computadoras	3	20%	160	73.2	11,712.00
PP_SGSI_004	Actualización de antivirus en los servidores	3	20%	15	73.2	1,098.00
PP_SGSI_005	Configuración de Biométrico de acceso a personal	1	0%	1	-	-
PP_SGSI_006	Implementación de cableado horizontal sótano, Piso1,Piso2 y Piso3	4	10%	1	151564.19	151,564.19
PP_SGSI_007	Optimización de procedimientos de la base de datos	5	30%	1	-	-
PP_SGSI_008	Renovación cámaras de seguridad en los ambientes de trabajo					
	Servidor de Video Vigilancia	3	0%	1	5360	5,360.00

	Cámara Tipo I	3	0%	35	1063.63	37,227.05
	Cámara Tipo II	3	0%	3	9350	28,050.00
PP_SGSI_009	Software para el registro de visitas	10	0%	1	-	-
PP_SGSI_010	Software para el registro de inventario de activos	10	0%	1	-	-
PP_SGSI_011	Software para el registro de incidentes de seguridad de información	10	0%	1	-	-
PP_SGSI_012	Implementación de Tablas bitácoras	4	10%	1	-	-
PP_SGSI_013	Kit Herramientas nuevas (para el técnico de soporte)	4	0%	6	329	1,974.00
PP_SGSI_014	Mantenimiento de hardware de ordenadores	2	0%	1	5,000.00	5,000.00
PP_SGSI_015	Renovación del Centro de Datos	145	20%	1	1,758,170.95	1,758,170.95
PP_SGSI_016	Mantenimiento del Grupo Electrógeno	2	80%	1	9,000.00	9,000.00
PP_SGSI_017	Capacitación sobre seguridad de la información	2	0%	1	-	-
PP_SGSI_018	Segregación de la red interna	5	50%	1	1,000.00	1,000.00
PP_SGSI_019	Implementación de Políticas de Seguridad de Información	2	15%	1	-	-
PP_SGSI_020	Software para el control de contraseñas	3	0%	1	-	-
PP_SGSI_021	Implementación de documentos para el retiro de equipos	3	0%	1	-	-
PP_SGSI_022	Implementación de aire acondicionado de precisión	1	0%	1	80,972.01	80,972.01
PP_SGSI_023	Contratar personal DBA	1	0%	1	2,200.00	2,200.00
PP_SGSI_024	Actualización del Plan de Continuidad del Negocio	4	0%	1	-	-
PP_SGSI_025	Implementación del Sistema de Gestión de Seguridad de Información	4	0%	1	-	-
PP_SGSI_026	Implementación del Plan de Restauración de Copias de Seguridad	4	10%	1	744.81	744.81
PP_SGSI_027	Definir los Roles, Responsabilidades y funciones del Comité se Seguridad de Información	4	0%	1	-	-
PP_SGSI_028	Revisión de los roles de usuario	4	0%	1	-	-

Con la ejecución de los proyectos se logrará llevar a cabo la implementación del Sistema de Gestión de Seguridad de Información cuya finalidad será proteger los activos de información del Servicio de Administración Tributaria de la zona Norte del Perú, debido a que se implementaran controles efectivos mediante los cuales se podrán gestionar y minimizar la materialización de los riesgo originado ante la ocurrencia de un evento de seguridad de información. Es preciso señalar que

realizado el análisis GAP (Anexo N° 05 y Anexo N° 06) se evidencio la existencia de controles de seguridad aplicados a procedimientos sin embargo, estos no se encuentran documentados en una política que permita el seguimiento continuo del cumplimiento; así mismo, del resultado obtenido del análisis de riesgos de la institución se han encontrado situaciones de riesgo (Tabla N° 20) que ameritan tomar medidas correctivas y preventivas.

De igual forma, la implementación del Sistema de Gestión de Seguridad de Información conlleva a dar cumplimiento a la Resolución Ministerial N° 004-2016-PCM, mediante la cual se aprueba de uso obligatorio la Norma Técnica Peruana "ISO NTP/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.

V.3. Planificación del Sistema de Gestión de Seguridad de Información

V.3.1. Identificación y Clasificación de los activos

La NTP-ISO/IEC 27001:2014 establece que la identificación de los activos es un elemento principal para el análisis de riesgo debido a que provee información necesaria para realizar dicho análisis.

Para la identificación de los activos se tomó como referencia a la NTP-ISO/IEC 27005 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información, que proporciona una lista de activos de información que serán considerados en esta actividad; así mismo, se han identificado las vulnerabilidades a las que se encuentran los activos de información las podrían ser explotadas por las amenazas (Tabla N° 11).

Tabla N° 11: Vulnerabilidades y amenazas de los activos de información

Tipo de Activo de Información		Activo de Información	Vulnerabilidad	Amenaza	Cód.
Activos Primarios	Procesos de Negocio	- Proceso de generación deuda Tributaria - Proceso de generación deuda No Tributaria - Proceso de Cobranza de Impuestos	Falta de revisiones regulares de gestión	Falla de la aplicaciones críticas	AM1
				Pérdida de servicios esenciales	AM2
	Información	- Datos Contribuyentes - Base de Datos	Copiado no controlado de la información	Robo de información	AM3
			Mal uso de aplicativos	Divulgación de la información	AM4
			Manipulación no autorizada de información	Alteración de información	AM5
			Falta de definición de perfil, privilegios y restricciones del personal	Copia fraudulenta de información	AM6
		- Documentos Institucionales	Falta de etiquetado de activos	Indisponibilidad de información física	AM7
		- Documentos de Gestión - Planes	Documentos no actualizados	Falta de normas y reglas claras	AM8
		- Copias de Respaldo	Falta de copias de respaldo	Indisponibilidad general de la sede	AM9
		- Código Fuente de Sistemas	Falta de control de cambios efectivo	Mal Funcionamiento de Software	AM10
Activos de Apoyo	Hardware	- Firewall	Inseguridad en la arquitectura de la red	Espionaje Remoto	AM11
		- Servidores	UPS de baja potencia	Pérdida de suministro de energía	AM12
			Susceptibilidad a variaciones de voltaje		
			Falta de mantenimiento	Falla de aire acondicionado	AM13
		- Computadoras	Almacenamiento no protegido	Robo de equipos	AM14
		- Unidad de disco extraíble	Antivirus no actualizado o sin licencia	Infección de sistemas a través de unidades portables sin escaneo (Virus, Malware)	AM15
		- Impresoras	Mantenimiento insuficiente	Daño de Equipos	AM16

	Software	- Sistema Integrado de Administración Tributaria SIAT - Sistema de Gestión Operativa - Sistema Integrado de Gestión Administrativa - Sistema Integrado de Administración Financiera	Falta o insuficiente prueba de software	Fallas en la operación	AM17
		- Correo Electrónico	Falta de Política del uso de correos	Filtración de información	AM18
		- Motor de Base de Datos	Falta de Mantenimiento correctivo y preventivo de equipos	Indisponibilidad de la base de datos	AM19
		- Paquete de Office - Lenguaje de programación - Sistema Operativo	Falta de procedimientos de estipulación de cumplimiento con derechos de propiedad intelectual	Uso de software falso o copiado	AM20
	Red	- Switch - Router - VPN - Red Telefónica - Ethernet	Mantenimiento insuficiente	Daño físico en infraestructura	AM21
				Indisponibilidad de las computadoras	AM22
	Personal	- Personal de la Administración Tributaria	Brecha de disponibilidad de personal	Ausencia de personal que cumpla con los Roles establecidos para dar cumplimiento a la normativa vigente	AM23
			Falta de Segmentación de funciones	Manejo inadecuado de los datos	AM24
			Falta de políticas de confidencialidad de información.		
		- Personal de Limpieza - Personal de Seguridad - Personal de Mantenimiento externo - Personal de Mensajería Externa	Falta de definición de perfil, privilegios y restricciones del personal	Acceso no autorizados	AM25

Luego de realizar la identificación de los activos de información, se debe estimar el valor que tienen para la administración y cuál es su importancia.

La NTP-ISO/IEC 27001:2014 indica que seguido de la identificación de los activos de información se deben establecer los criterios de clasificación de la información según el carácter confidencial de la misma.

Tabla N° 12: Niveles de Clasificación de los Activos

Tipo	Glosa	Descripción
C	Confidencial	Información de gran relevancia para la administración, se restringe el acceso a la misma.
R	Restringido	Accesible para determinados colaboradores según el desempeño de las funciones.
UI	Uso Interno	Accesible para todo los colaboradores de la administración.
P	Público	Información de dominio público como la publicada en la página web.

A pesar que la norma no establece como requisito la evaluación del activo según la dimensión, se ha visto conveniente realizarla debido a que se va cuantificar la importancia del activo a través de las dimensiones CID (Confidencialidad, Integridad y disponibilidad); teniendo en consideración el nivel de evaluación establecido en la NTP-ISO/IEC 27005 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información.

Tabla N° 13: Leyenda Criterio de clasificación CID

Valor	Nivel	Criterio de Clasificación
5	Muy Alto	Conocimiento y divulgación de la información Reservada, impacta negativamente tanto las finanzas y la reputación de la entidad.
4	Alto	Conocimiento y divulgación de la información Sensible, impacta negativamente la reputación de la entidad.
3	Medio	Conocimiento y divulgación de la información Interna, impacta negativamente las finanzas de la entidad.
2	Bajo	Conocimiento y divulgación de información Pública, impacta negativamente a nivel operacional la entidad.
1	Muy Bajo	Conocimiento y divulgación de la información no clasificada, no genera impacto alguno para la entidad.

El valor total del activo se calcula en base al promedio de los valores obtenidos en el proceso de evaluación del activo según la dimensión

VALOR DEL ACTIVO = PROMEDIO (CID)

El resultado se evaluara según el criterio en la tabla

Tabla N° 14: Leyenda de Valor de los Activos

Valor	Descripción	
5	Muy Alto	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente tanto las finanzas y la reputación de la entidad.
4	Alto	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente la reputación de la entidad.
3	Medio	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente las finanzas de la entidad.
2	Bajo	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, impacta negativamente a nivel operacional la entidad.
1	Muy Bajo	La pérdida de Integridad, Disponibilidad y Confidencialidad del activo, no genera impacto alguno para la entidad.

Se evalúa el impacto que genera en la administración en caso de pérdida o robo del activo de información.

Tabla N° 15: Leyenda Magnitud de Daño

Tipo	Descripción	Información
1	Insignificante	No causa ningún tipo de impacto o daño a la organización
2	Bajo	Causa daño aislado, que no perjudica a ningún componente de la organización.
3	Mediano	Provoca la desarticulación de un componente de la organización. Si no se atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
4	Alto	En el corto plazo desmoviliza o desarticula a la organización

Según los criterios de evaluación se tienen como resultado la Tabla N° 16 sobre la valorización de los activos de información.

Tabla N° 16: Valoración de los activos de información

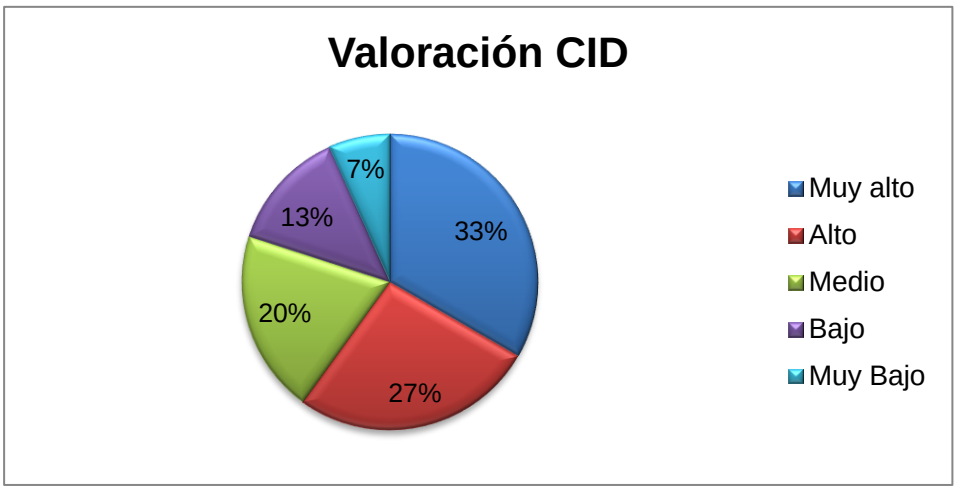
Identificación del Activo de información				**Valoración de los activos de información**									
Tipo de Activo de Información		**Cod. Activo**	**Activo de Información**	**Criterio de Clas.**	**Dim. del activo**			**Valor del activo**	**Magnitud de Daño**	**Propiedad del activo**		**Valor**	**Mag.**
					C	**I**	**D**			**Propietario del activo**	**custodio del activo**		
Activos Primarios	Procesos de Negocio	A1	Proceso de generación deuda Tributaria	R	5	5	5	5	4	OTIC	OTIC	5	4
		A2	Proceso de generación deuda No Tributaria	R	5	5	5	5	4	OTIC	OTIC		
		A3	Proceso de Cobranza de Impuestos	R	5	5	5	5	4	OTIC	OTIC		
	Información	A4	Datos Contribuyentes	C	5	5	5	5	4	OTIC	OTIC	4	4
		A5	Base de Datos	R	5	5	5	5	4	OTIC	OTIC		
		A6	Documentos Institucionales	R	3	4	4	4	4	Planeamiento	Planeamiento		
		A7	Documentos de Gestión – Planes	P	3	4	3	3	4	Planeamiento	Planeamiento		
		A8	Copias de Respaldo	R	5	5	4	5	4	OTIC	OTIC		
		A9	Código Fuente de Sistemas	R	3	5	4	4	3	OTIC	OTIC		
Activos de Apoyo	Hardware	A10	Firewall	UI	3	3	4	3	4	OTIC	OTIC	3	3
		A11	Servidores	UI	5	5	5	5	4	OTIC	OTIC		
		A12	Computadoras	UI	2	2	4	3	3	OTIC	OTIC		
		A13	Impresoras	UI	2	2	3	2	2	OTIC	OTIC		
		A14	Unidad de disco extraíble	UI	2	2	3	2	2	OTIC	OTIC		
	Software	A15	Sistema	UI	2	3	4	3	4	OTIC	OTIC	3	3

			Integrado de Administración Tributaria									
		A16	Sistema de Gestión Operativa	UI	2	3	4	3	4	OTIC	OTIC	
		A17	Sistema Integrado de Gestión Administrativa	UI	2	3	4	3	2	OTIC	OTIC	
		A18	Sistema Integrado de Administración Financiera	UI	2	3	4	3	2	OTIC	OTIC	
		A19	Correo Electrónico	UI	3	3	3	3	2	OTIC	OTIC	
		A20	Sistema Operativo	UI	2	2	3	2	3	OTIC	OTIC	
		A21	Motor de Base de Datos	R	2	2	2	2	2	OTIC	OTIC	
		A22	Paquete de Office	UI	2	2	2	2	2	OTIC	OTIC	
		A23	Lenguaje de programación	R	2	2	2	2	2	OTIC	OTIC	
	Red	A24	Switch	UI	2	3	3	3	4	OTIC	OTIC	2	3
		A25	Router	UI	2	3	3	3	4	OTIC	OTIC		
		A26	VPN	UI	2	2	3	2	2	OTIC	OTIC		
		A27	Red Telefónica	UI	2	2	2	2	2	OTIC	OTIC		
		A28	Ethernet	UI	2	2	2	2	2	OTIC	OTIC		
	Personal	A29	Personal de la Administración Tributaria	UI	2	2	2	2	2	Talento Humano	Talento Humano	1	2
		A30	Personal de Limpieza	UI	1	1	2	1	2	Abastecimiento	Abastecimiento		
		A31	Personal de	UI	1	1	2	1	2	Abastecimiento	Abastecimiento		

			Seguridad										
		A32	Personal de Mantenimiento externo	UI	1	1	2	1	2	Abastecimiento	Abastecimiento		
		A33	Personal de Mensajería Externa	UI	1	1	2	1	2	Abastecimiento	Abastecimiento		

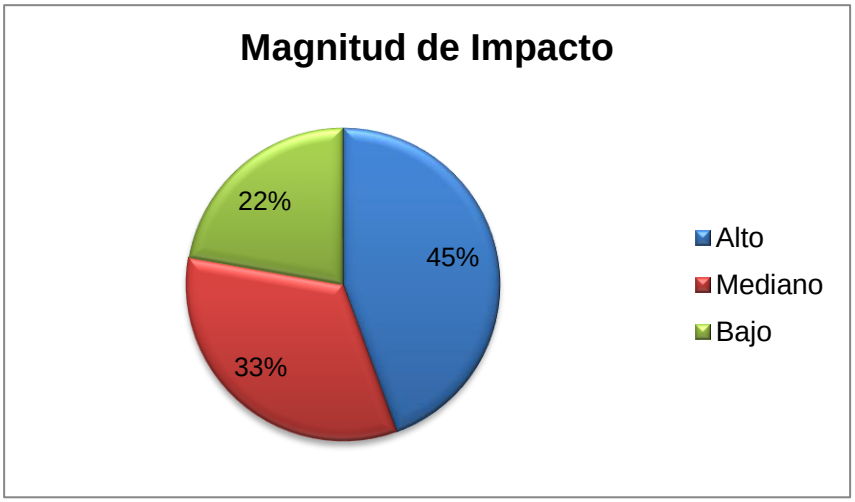
De acuerdo a los resultados obtenidos, se observa en la Figura N° 18 que los activos de información según su valoración, se concentran en la clasificación de muy alto correspondiente al 33%, alto correspondiente al 27%, seguido del 20% y 13% para medio y bajo correspondiente; finalmente existe una valoración baja del 7%.

Figura N° 18: Valoración CID



Los valores resultantes de la evaluación del impacto que genera en la institución en caso de pérdida de confidencialidad, integridad y disponibilidad para cada activo, se pueden observar en la figura N° 19; donde se produce un impacto alto del 45%, así mismo se obtiene el 33% de impacto mediano y el 22% para impacto bajo.

Figura N° 19: Magnitud de Impacto



V.3.2. Gestionar los riesgos y crear un plan de tratamiento de riesgos

V.3.2.1. Evaluación de Riesgos

La evaluación de riesgo es el proceso en donde se va a realizar la identificación del riesgo, análisis y la valorización del riesgo; para ello se toma como referencia la NTP-ISO/IEC 27005 Tecnología de la información. Técnicas de seguridad. Gestión de riesgos de la seguridad de la información y la Norma Internacional ISO 31000:2018 Gestión del Riesgo – Directrices, que proporciona una serie de amenazas típicas que deben ser utilizadas durante el proceso de evaluación, estas han sido tomadas como referencia para encontrar, reconocer y describir los riesgos a los que se encuentra expuesta la administración y que podrían impedir al cumplimiento de los objetivos.

Mediante este análisis se va a decidir que riesgos serán tratados mediante la aplicación de controles para el tratamiento de los mismos; para ello es necesario establecer probabilidades de ocurrencia de los mismos:

Tabla N° 17: Leyenda de Probabilidad de Ocurrencia

Medición	**Probabilidad**		
	Criterio de medición		**Frecuencia**
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en cualquier momento	Al menos una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años
4	Probable	El evento ocurre probablemente en la mayoría de circunstancias	Al menos una vez en el último año
5	Casi Seguro	Se espera que el evento ocurra en la mayoría de circunstancias	Más de una vez al año

De igual forma se debe considerar el valor de impacto que se tendría de ocurrir el riesgo identificado.

Tabla N° 18: Leyenda de Valor de Impacto

Medición	**Valor Impacto**	
	Criterio de medición	
1	Insignificante	Si el hecho llega a presentarse, tendría efecto mínimo en la administración
2	Menor	Si el hecho llega a presentarse, tendría bajo impacto
3	Moderado	Si el hecho llega a presentarse, tendría medianas consecuencias
4	Alto	Si el hecho llega a presentarse, tendría altas consecuencias
5	Catastrófico	Si el hecho llega a presentarse, tendría desastrosas consecuencias

El valor del riesgo se calcula de la siguiente fórmula:

Riesgo = Probabilidad de Ocurrencia de Amenaza* Valor del Activo

Cuyos valores se pueden interpretar de la siguiente manera:

Tabla N° 19: Leyenda de Valorización del Riesgo

Nivel de Riesgo	**Valorización del Riesgo**	
	Descripción	
Extremo	(13-25)	Si una situación se evalúa como de extremo riesgo, hay una necesidad inminente y urgente de tomar medidas correctivas en el corto plazo.
Alto	(8-12)	Si una situación se evalúa como de alto riesgo, hay una necesidad inminente de tomar medidas correctivas en el corto o mediano plazo.
Moderado	(4-6)	Si una situación se clasifica como de riesgo moderado, las acciones correctivas son necesarias en un período de tiempo razonable.
Bajo	(1-3)	Si una situación se clasifica como de riesgo bajo, debe decidirse si las acciones correctivas son requeridas o se acepta el riesgo.

Una vez valorizado el riesgo se observa el nivel de riesgo para cada escenario.

Figura N° 20: Leyenda de Nivel de Impacto del Riesgo

Probabilidad de Ocurrencia

Probabilidad de Ocurrencia	Valor Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Alto (4)	Catastrófico (5)
Casi Seguro (5)	5	10	15	20	25
Probable (4)	4	8	12	16	20
Posible (3)	3	6	9	12	15
Improbable (2)	2	4	6	8	10
Raro (1)	1	2	3	4	5

Impacto

Tabla N° 20: Análisis de Riesgo

Riesgos	Amenaza	Tipo de Riesgo	Probabilidad	Valorización de riesgo	Nivel de Riesgo
Pérdida de la información de la entidad	Falla de la aplicaciones críticas	Seguridad de Información	4	12	Alto
	Pérdida de servicios esenciales		4	12	Alto
	Robo de información		2	6	Moderado
	Divulgación de la información		5	15	Extremo
	Alteración de información		5	15	Extremo
	Copia fraudulenta de información		5	15	Extremo
	Indisponibilidad de información física		2	6	Moderado
	Falta de normas y reglas claras		2	6	Moderado
Indisponibilidad de la información	Indisponibilidad general de la sede		4	12	Alto
	Mal Funcionamiento de Software		4	12	Alto
	Espionaje Remoto		5	15	Extremo
	Pérdida de suministro de energía		5	15	Extremo
	Falla de aire acondicionado		4	12	Alto
	Robo de equipos		4	12	Alto
	Infección de sistemas a través de unidades portables sin escaneo		4	12	Alto
	Daño de Equipos		4	12	Alto
	Fallas en la operación		4	12	Alto
	Filtración de información		2	6	Moderado
Fallas de seguridad por recurso humano	Indisponibilidad de la base de datos		4	12	Alto
	Uso de software falso o copiado		4	12	Alto
	Daño físico en infraestructura		4	12	Alto
	Indisponibilidad de las computadoras		2	6	Moderado
	Ausencia de personal que cumpla con los Roles establecidos para dar cumplimiento a la normativa vigente		3	9	Alto
	Manejo inadecuado de los datos		3	9	Alto
	Acceso no autorizados		4	12	Alto

Tabla N° 21: Resumen de Análisis de Riesgo

	Activos de Información					
Riesgos	**Procesos de Negocio**	**Información**	**Hardware**	**Software**	**Red**	**Personal**
Pérdida de la información	18	16	11	9	9	4
Indisponibilidad de la información	20	17	12	10	10	5
Fallas de seguridad por recurso humano	17	15	10	9	8	4

La herramienta usada para el análisis de los riesgos, fue la Matriz de Riesgos o Matriz de probabilidad e impacto, que consiste en una matriz de doble entrada (Activo / Amenaza) cuya finalidad es informar sobre la evaluación del riesgo. Esta herramienta es sugerida por la ISO/IEC 31010 Gestión de riesgos. Técnicas de evaluación de riesgos, que consiste en la recopilación de los escenarios que deben considerarse durante el proceso de la evaluación del riesgo, esta herramienta evalúa el nivel de probabilidad y el impacto de las consecuencias de cada riesgo realizando el cálculo de cada nivel de riesgo que posteriormente ayudaran a priorizar para actuar con el tratamiento de los mismos a fin de evitar que estos afecten a la continuidad del cumplimiento de los objetivos de la administración (Ver Anexo N° 09).

El análisis realizado es Cualitativo, debido a que se realizaron estimaciones de pérdidas potenciales en cuanto al nivel de probabilidad e impacto en el activo, de ocurrida la amenaza; las mismas que determinaran un nivel de riesgo en la matriz de probabilidad e impacto dividida en zonas que corresponden el nivel obtenido por cada riesgo cuya finalidad es determinar la aceptabilidad de los riesgos analizados y priorizar la intervención y el plan de tratamiento a realizar. Así mismo, del resultado obtenido durante la evaluación de los riesgos de la institución se puede evidenciar que se encontraron 15 situaciones que se encuentran en el nivel de riesgo alto, es decir existe la necesidad de tomar medidas correctivas en corto o mediano plazo; 5 situaciones que se encuentran en el nivel de riesgo extremo, es decir, existe la necesidad urgente de tomar medidas preventivas en corto plazo; así mismo, 5 situaciones que se encuentran en nivel de riesgo moderado es decir se pueden tomar medidas en un tiempo razonable o por el contrario se puede aceptar el nivel de riesgo.

Tabla N° 22: Resumen Cantidad de Riesgos por Nivel

Nivel de Riesgo	**Riesgos**
Extremo	5
Moderado	5
Alto	15

Se identificaron los escenarios relevantes considerados como nivel de riesgo extremo y alto, ya que estos impactan en el cumplimiento de los requisitos de seguridad de la información.

Es necesario tener en cuenta que para este proceso se ha determinado la causa del riesgo.

Tabla N° 23: Identificación de los escenarios relevantes

Riesgos	Amenaza	Tipo de Riesgo	Nivel de Riesgo
Pérdida de la información de la entidad	Falla de la aplicaciones críticas	Seguridad de Información	Alto
	Pérdida de servicios esenciales		Alto
	Divulgación de la información		Extremo
	Alteración de información		Extremo
	Copia fraudulenta de información		Extremo
Indisponibilidad de la información	Indisponibilidad general de la sede		Alto
	Mal Funcionamiento de Software		Alto
	Espionaje Remoto		Extremo
	Pérdida de suministro de energía		Extremo
	Falla de aire acondicionado		Alto
	Robo de equipos		Alto
	Infección de sistemas a través de unidades portables sin escaneo (Virus, Malware)		Alto
	Daño de Equipos		Alto
	Fallas en la operación		Alto
Fallas de seguridad por recurso humano	Indisponibilidad de la base de datos		Alto
	Uso de software falso o copiado		Alto
	Daño físico en infraestructura		Alto
	Ausencia de personal que cumpla con los Roles establecidos para dar cumplimiento a la normativa vigente		Alto
	Manejo inadecuado de los datos		Alto
	Acceso no autorizados		Alto

V.3.2.2. Plan de Tratamiento de Riesgos

Una vez identificados los riesgos se debe identificar controles que se deben aplicar para mitigar, evitar o transferir los riesgos a los que se encuentran expuestos la institución para ello es necesario realizar el plan de tratamiento de riesgos.

El Plan de Tratamiento de riesgos como se muestra en la tabla N° 24 contempla las actividades que se deben realizar para el cumplimiento de cada control, se han identificado los responsables como los recursos asociados para llevar a cabo el cumplimiento de las mismas.

Tabla N° 24: Plan de Tratamiento de Riesgos

Riesgos	Amenaza	Activo Relacionado	Nivel de Riesgo	Tratamiento	Referencia Anexo A ISO 27001:2014	Actividades	Proyecto Asociado	Recurso	Responsable
Pérdida de la información de la entidad	Falla de la aplicaciones críticas	Información Hardware Software Personal	Alto	Mitigar el Riesgo	A.17.1.1. Planificación de continuidad de seguridad de la información	Diseñar el "Plan de continuidad del negocio"	PP_SGSI_024 PP_SGSI_025	Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
						Integrar los requisitos de seguridad de información al "Plan de Continuidad del Negocio"			
	Pérdida de servicios esenciales	Información Red Software Personal	Alto	Mitigar el Riesgo	A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	Mantener actualizado el Sistema de Gestión de Seguridad de Información, mediante la revisión periódica del cumplimiento de los controles de seguridad de información.		Propio	Resp. De Tecnología de Información Of. De Seguridad de Información
	Divulgación de la información	Información Software Personal	Extremo	Mitigar el Riesgo	A.11.1.2. Controles de acceso físico	Establecer una política que restringa el uso de cámaras fotográficas o video en las áreas de tratamiento de información.	PP_SGSI_001 PP_SGSI_019	Firewall FG-300E - Fortinet	Administrador de Red Resp. De Tecnología de Información
					A.8.3.1. Gestión de Medios Removibles	Definir una política que restrinja el uso de dispositivos de almacenamiento			
						Bloque a lectura y escritura de medios extraíbles y magnéticos			
					A.9.1.2. Accesos a redes y Servicios de red	Realizar las configuraciones al Firewall con los roles para el control de acceso lógico		Propio	Resp. De Tecnología de Información Of. De Seguridad de Información
					A.11.2.7. Disposición o reutilización segura	Establecer una política que determine que los equipos deben ser formateados			

					de equipos	antes de ser reutilizados.			
					A.13.2.4. Acuerdos de confidencialidad o no divulgación	Establecer acuerdos de confidencialidad de información que deben abarcar a cada nivel de los colaboradores, los mismos que deben ser entregados como parte de las funciones a realizar.			
	Alteración de información	Información Software Personal	Extremo	Mitigar el Riesgo	A.9.4.1. Restricción de acceso a la información	Establecer una política de acceso a la información que se determine por roles de usuario	PP_SGSI_010 PP_SGSI_012 PP_SGSI_017	Propio	Resp. De Tecnología de Información Analistas Programadores
						Identificar los niveles de acceso según el perfil del puesto			
					A.12.4.1. Registro de eventos	Implementar tablas bitácoras para los cambios realizados en los datos de contribuyentes, predios, cuentas corrientes.		Propio	Resp. De Tecnología de Información Analistas Programadores
					A.8.2.1. Clasificación de la Información	Realizar la clasificación de información según el valor para la institución			
						Realizar los procedimientos de seguridad de información según cada grupo de clasificación		Especialista	Resp. De Tecnología de Información Of. De Seguridad de Información
					A.8.2.2. Etiquetado de la Información	Realizar los procedimientos para realizar el etiquetado de la información			
	Copia fraudulenta de información	Información Software Personal	Extremo	Mitigar el Riesgo	A.8.1.3. Uso aceptable de los activos	Documentar el uso adecuado de los activos	PP_SGSI_017 PP_SGSI_019 PP_SGSI_021	Especialista	Resp. de Planeamiento Resp. De Calidad

									Resp. De Tecnología de Información
						Comunicar a los colaboradores sobre el uso de los activos		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad
					A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	Mantener un registro de custodia de equipos cuando salen de la institución		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
Indisponibilidad de la información	Indisponibilidad general de la sede	Información Red Software Personal	Alto	Mitigar el Riesgo	A.17.1.1. Planificación de continuidad de seguridad de la información	Diseñar el "Plan de continuidad del negocio"	PP_SGSI_024 PP_SGSI_025	Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
						Integrar los requisitos de seguridad de información al "Plan de Continuidad del Negocio"			
					A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	Mantener actualizado el Sistema de Gestión de Seguridad de Información, mediante la revisión periódica del cumplimiento de los controles de seguridad de información.		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad

	Mal Funcionamiento de Software	Información Software Personal	Alto	Mitigar el Riesgo	A.12.1.1. Procedimientos operativos documentados	Definir los procedimientos y documentarlos para las actividades de operaciones de tal forma que garanticen la seguridad.	PP_SGSI_007 PP_SGSI_023 PP_SGSI_015	Propio	Resp. De Tecnología de Información Administrador de Red Administrador de BD
					A.12.1.2. Gestión de cambio	Mantener documentados los cambios ocurridos en los sistemas de información.			
					A.12.1.3. Gestión de la capacidad	Optimizar los procedimientos de la base de datos que generan carga masiva de información.		Contrato Personal DBA	Resp. De Tecnología de Información Administrador de Red Administrador de BD
					A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	Definir una política donde se especifique que se debe seguir las etapas del desarrollo de manera adecuada.		Proyecto IOAR	Gerencia General Gerencia de Administración Resp. De Tecnología de Información Soporte Técnico
	Espionaje Remoto	Información Red Software Personal	Extremo	Mitigar el Riesgo	A.9.1.1. Política de Control de Accesos	Establecer una política de control de acceso	PP_SGSI_001 PP_SGSI_018 PP_SGSI_019	Firewall FG-300E - Fortinet	Administrador de Red Resp. De Tecnología de Información
					A.9.1.2. Accesos a redes y Servicios de red	Realizar las configuraciones al Firewall con los roles para el control de acceso lógico			
					A.13.1.2. Seguridad de los servicios de red	Realizar las configuraciones al Firewall para gestionar los servicios de red		Especialista	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de

									Información
					A.13.1.3. Segregación en redes	Segregar la red de la institución, por pisos y mantener un red aislada para servidores y para la oficina de tecnología de información		Especialista	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
	Pérdida de suministro de energía	Información Red Software Personal	Extremo	Mitigar el Riesgo	A.11.1.1. Perímetro de Seguridad física	Implementar sensores de humedad en el Centro de Datos	PP_SGSI_006 PP_SGSI_015 PP_SGSI_016	Canaletas	Resp. De Tecnología de Información Soporte Técnico
						Implementar Detectores de humo o fuego			
					A.11.2.2. Servicio de suministro	Establecer oficinas a entrar en carga critica del respaldo eléctrico		Proyecto IOAR	Gerencia General Gerencia de Administración Resp. De Tecnología de Información Soporte Técnico
	Falla de aire acondicionado	Información Red Software Personal	Alto	Mitigar el Riesgo		Implementar servicios redundantes de suministros de fluido eléctrico			
						Realizar mantenimiento del Grupo Electrógeno		Soporte Técnico especialista en mant. de Centro de Datos	Resp. De Tecnología de Información Soporte Técnico
					A.11.2.3. Seguridad en el cableado	Separar el cableado eléctrico según demanda, Pc's, Impresoras y servidores			
						Implementar estabilizadores de corriente al fluido eléctrico			
	Robo de equipos	Información Hardware Software Personal	Alto	Mitigar el Riesgo	A.8.1.1. Inventario de Activos	Identificar los activos que dan soporte a la institución	PP_SGSI_005 PP_SGSI_008 PP_SGSI_019 PP_SGSI_021	Propio	Resp. De Tecnología de Información
						Clasificar los activos según su importancia			

					A.8.1.2. Propiedad de los Activos	Asignar a los propietarios de los activos		Propio	Resp. De Tecnología de Información Of. De Seguridad de Información Soporte Técnico
					A.11.1.1. Perímetro de Seguridad física	Contratar un personal para monitorear por video vigilancia			
						Segmentar el área de atención al público y el ingreso de los colaboradores a las oficinas administrativas.		Especialista	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
					A.11.1.2. Controles de acceso físico	Implementar medidas de identificación para el registro de visitantes		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
					A.11.2.1. Emplazamiento y protección de equipos	Control de acceso al centro de datos, por biométrico o tarjetas rf			
	Infección de sistemas a través de unidades portables sin escaneo (Virus, Malware)	Información Hardware Software Personal	Alto	Evitar el Riesgo	A.12.2.1. Controles contra código malicioso	Realizar compra de antivirus para todos los equipos de la institución	PP_SGSI_001 PP_SGSI_003 PP_SGSI_004 PP_SGSI_019	Firewall FG-300E - Fortinet	Administrador de Red Resp. De Tecnología de Información
						Establecer controles de navegación por páginas web		Antivirus Licenciado para ordenadores	Resp. De Tecnología de Información Soporte Técnico
						Mantener actualizados los antivirus			
					A.12.5.1 Instalación de Software en los Sistemas Operativos	Establecer una política para que las instalaciones de software sean bajo aprobación de jefes inmediatos.		Antivirus Licenciado para servidores	Resp. De Tecnología de Información Soporte Técnico

					A.12.6.2. Restricciones de instalación de software	Bloquear permisos desde el directorio activos para que los usuarios no puedan realizar instalaciones.		Especialista	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
	Daño de Equipos	Información Hardware Software Personal	Alto	Mitigar el Riesgo	A.11.1.1. Perímetro de Seguridad física	Establecer niveles de acceso a la oficina de Tecnología de información	PP_SGSI_002 PP_SGSI_013 PP_SGSI_014	Licencias de Servidores	Administrador de Red Resp. De Tecnología de Información Soporte Técnico
						Segmentar el área de atención al público y el ingreso de los colaboradores a las oficinas administrativas.		Kit de herramientas para soporte	Resp. De Abastecimiento
					A.11.2.4. Mantenimiento de equipos	Establecer el plan de mantenimiento físico y lógico de los equipos informáticos de manera semestral o anual			
					A.11.1.4. Protección contra amenazas externas y ambientales	Desarrollar e implementar "plan de continuidad de negocio" o "disaster recovery"		Soporte Técnico	Resp. De Tecnología de Información Soporte Técnico
	Fallas en la operación	Información Red Software Personal	Alto	Mitigar el Riesgo	A.12.3.1. Respaldo de la información	Establecer una política de copias de seguridad o de respaldo de la información que tenga en cuenta la periodicidad con la que se hacen las copias.	PP_SGSI_019 PP_SGSI_026	Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad

						Realizar la revisión diaria de las copias de seguridad		Especialista	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad
Fallas de seguridad por recurso humano	Indisponibilidad de la base de datos	Información Red Software Personal	Alto	Mitigar el Riesgo	A.11.2.4. Mantenimiento de equipos	Establecer el plan de mantenimiento físico y lógico de los equipos informáticos de manera semestral o anual	PP_SGSI_014	Propio	Soporte Técnico Resp. De Tecnología de Información
	Uso de software falso o copiado	Información Red Software Personal	Alto	Evitar el Riesgo	A.12.6.2. Restricciones de instalación de software	Bloquear permisos desde el directorio activos para que los usuarios no puedan realizar instalaciones.	PP_SGSI_002 PP_SGSI_001	Licencias de Servidores	Administrador de Red Resp. De Tecnología de Información Soporte Técnico
								Firewall FG-300E - Fortinet	Administrador de Red Resp. De Tecnología de Información
	Daño físico en infraestructura	Información Hardware Software Personal	Alto	Mitigar el Riesgo	A.11.2.1. Emplazamiento y protección de equipos	Control de acceso al centro de datos, por biométrico o tarjetas rf	PP_SGSI_008 PP_SGSI_009 PP_SGSI_006 PP_SGSI_014 PP_SGSI_021	Cámaras de Seguridad	Administrador de Red Resp. De Tecnología de Información Resp. De Abastecimiento Gerencia de Administración
					A.11.2.2. Servicio de suministro	Establecer oficinas a entrar en carga critica del respaldo eléctrico			
						Implementar servicios redundantes de suministros de fluido		Propio	Resp. De Tecnología de Información

						eléctrico			Analistas Programadores
						Realizar mantenimiento del Grupo Electrógeno			
					A.11.2.3. Seguridad en el cableado	Separar el cableado eléctrico según demanda, Pc's, Impresoras y servidores			
						Implementar estabilizadores de corriente al fluido eléctrico		Canaletas	Resp. De Tecnología de Información Soporte Técnico
						Implementación de cableado de datos inteligente para monitoreo constante de la red			
						Realizar la canalización de red de datos con canaletas resistentes y auto extinguibles en caso de siniestro		Soporte Técnico	Resp. De Tecnología de Información Soporte Técnico
					A.11.2.4. Mantenimiento de equipos	Establecer el plan de mantenimiento físico y lógico de los equipos informáticos de manera semestral o anual			
					A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	Mantener un registro de custodia de equipos cuando salen de la institución		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información
					A.11.2.7. Disposición o reutilización segura de equipos	Establecer una política que determine que los equipos deben ser formateados antes de ser reutilizados.			
	Ausencia de personal que cumpla con los Roles	Información Software Personal	Alto	Evitar el Riesgo	A.6.1.1. Roles y Responsabilidades para la seguridad de la información	Definir los perfiles y funciones de cada integrante del comité de seguridad	PP_SGSI_011 PP_SGSI_017 PP_SGSI_019 PP_SGSI_027	Propio	Resp. De Tecnología de Información Analistas

	establecidos para dar cumplimiento a la normativa vigente					Comunicar a cada integrante del comité de seguridad sus roles y responsabilidades			Programadores
					A.6.1.2. Segregación de Funciones	Definir los perfiles y funciones de cada integrante del comité de seguridad			
					A.16.1.1. Responsabilidades y procedimientos	Definir responsables para la gestión de incidentes de seguridad de información		Especialista	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad
						Establecer los procedimientos para la detección, análisis y elaboración de informes de incidentes de la seguridad de información			
						Hacer de conocimiento a los colaboradores de la institución sobre los procedimientos establecidos para la gestión de incidentes.			
					A.16.1.2. Reporte de eventos de seguridad de la información	Establecer una política donde se especifique los canales de comunicación para todos los eventos o incidentes		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad
						Desarrollar e implementar un sistema que permita realizar el registro de los eventos de seguridad de información			

					A.16.1.3. Reporte de debilidades de seguridad de la información	Diseñar los parámetros que debe contener el reporte de incidentes.			
					A.16.1.4. Evaluación y decisión sobre eventos de seguridad de la información	Identificar el nivel de impacto de los riesgos según la clasificación realizada por el responsable de la gestión de incidentes.		Propio	Resp. De Tecnología de Información Oficial de Seguridad
					A.16.1.5. Respuesta de incidentes de seguridad de la información	Definir los tiempos de respuesta aceptables por cada incidente de seguridad			
					A.16.1.6. Aprendizaje de los incidentes de la seguridad de información	Diseñar una base de conocimiento que permita tener un repositorio de los incidentes en seguridad que ha ocurrido en la institución, con la finalidad de gestionarlos.			
	Manejo inadecuado de los datos	Información Software Personal	Alto	Mitigar el Riesgo	A.8.2.1. Clasificación de la Información	Realizar la clasificación de información según el valor para la institución	PP_SGSI_001 PP_SGSI_028	Firewall FG-300E - Fortinet	Administrador de Red Resp. De Tecnología de Información
						Realizar los procedimientos de seguridad de información según cada grupo de clasificación			
					A.8.2.2. Etiquetado de la Información	Realizar los procedimientos para realizar el etiquetado de la información		Propio	Resp. De Tecnología de Información Oficial de Seguridad
					A.8.2.3. Manejo de Activos	Realizar los procedimientos para el óptimo manejo de activos			

	Acceso no autorizados	Información Software Personal	Alto	Mitigar el Riesgo	A.9.2.1. Registro y baja de usuarios	Establecer una política para el proceso de alta y bajas de usuario	PP_SGSI_001 PP_SGSI_019 PP_SGSI_028	Firewall FG-300E - Fortinet	Administrador de Red Resp. De Tecnología de Información
						Identificar los tiempo de conexión al acceso remoto			
					A.9.2.4. Gestión de información de autenticación secreta de usuario	Establecer una política de gestión de contraseñas			
						Establecer una clausula en el contrato sobre las condiciones de puesto de trabajo sobre contraseñas seguras, según corresponda			
					A.9.2.5. Revisión de derechos de acceso de usuario	Establecer un procedimiento que determine que las cuentas de usuarios deben ser validadas continuamente			
					A.9.2.6. Remoción o ajustes de derechos de acceso	Establecer un procedimiento que determine que las cuentas de usuarios estén acorde a las funciones que realiza.			
					A.9.3.1. Uso de Información de autenticación secreta	Establecer una política para mantener la confidencialidad de las contraseñas de acceso a sistemas		Propio	Resp. de Planeamiento Resp. De Calidad Resp. De Tecnología de Información Oficial de Seguridad
					A.9.4.1. Restricción de acceso a la información	Definir los niveles de acceso a la información según los roles de cada usuario.			
					A.9.4.2. Procedimientos de acceso seguro	Establecer una política para el inicio de sesión seguro en los sistemas de información			

						Configurar los sistemas de información para que permitan el inicio de sesión mediante usuario y contraseña			
						Elaborar procedimientos almacenados que permitan que la contraseña se almacene encriptada.			
						Configurar los sistemas de información para que luego de un tiempo determinado las sesiones se encuentren inactivas.		Propio	Resp. De Tecnología de Información Oficial de Seguridad
					A.9.4.3. Sistema de Gestión de contraseñas	Establecer una política de contraseñas en la que se indique que las contraseñas deben contener caracteres alfa numéricos.			
						Configurar los sistemas de información a fin que permita realizar el cambio de contraseña al primer inicio de sesión			
						Establecer el periodo que debe pasar para realizar los cambios de contraseña			

V.3.3. Establecer políticas y procedimientos para controlar los riesgos

V.3.3.1. Políticas de Seguridad de Información

Las políticas específicas de seguridad de la información deben estar alineadas y soportadas bajo la política general del Sistema de Gestión de seguridad de Información (Anexo N° 10), las cuales son las siguientes:

- Política para la asignación y baja de usuarios
- Política para el control de accesos
- Política para la seguridad entre comunicaciones.
- Política para la seguridad de información involucrando al colaborador
- Política para las seguridad física y ambiental
- Política para el desarrollo y mantenimiento de sistemas
- Política para la Administración de la continuidad de las actividades de la institución

V.3.3.2. Declaración de Aplicabilidad

Le declaración de aplicabilidad de la NTP-ISO/IEC 27001:2014 como se muestra en la tabla N° 25, contempla los objetivos de control y controles que han sido seleccionados, además de las razones por las cuales se realiza la acción de selección y las medidas de seguridad adicionales que se debe de implementar.

También nos muestra si los objetivos de control o controles se encuentran operando, los que serán excluidos, así como la justificación del porque son innecesarios o no son requeridos por la institución.

Los controles indicados en la declaración de aplicabilidad son seleccionados como resultado de la identificación de los riesgos, además de realizar el cumplimiento de la Resolución Ministerial N° 004-2016-PCM.

Tabla N° 25: Declaración de Aplicabilidad de la NTP-ISO/IEC 27001:2014

CONTROL APLICADO			CONTROL IMPLEMENTADO	EXCLUSIÓN DE CONTROL	JUSTIFICACIÓN
Dominio	**A.5. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN**				
Objetivo de Control	**A.5.1. Dirección de la Gerencia para la Seguridad de la Información**				
1	A.5.1.1. Políticas para la seguridad de información	La institución cuenta con políticas documentadas sobre uso de internet, alta y baja de usuarios,	SI	NO	Se establece dar cumplimiento a lo estipulado en la Resolución Ministerial N° 004-2016-PCM y asegurar la integridad de la información de la institución.
2	A.5.1.2. Revisión de las políticas para la seguridad de la información	No se realiza la revisión de las políticas existentes en la administración.	SI	NO	Para hacer el adecuado control y seguimiento de cumplimiento de las políticas que serán implementadas.
Dominio	**A.6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN**				
Objetivo de Control	**A.6.1. Organización Interna**				
1	A.6.1.1. Roles y Responsabilidades para la seguridad de la información	Mediante Resolución Gerencial en el año 2018 se determinó la conformación del comité de Seguridad de la Información en la administración.	SI	NO	Dar cumplimiento a la normativa vigente y mediante la cual la institución se encuentra obligada de cumplir.
2	A.6.1.2. Segregación de Funciones	No se evidencia la segregación de funciones para el comité de Seguridad de la información	SI	NO	Dar cumplimiento a la normativa vigente y mediante la cual la institución se encuentra obligada de cumplir.
3	A.6.1.3. Contacto con autoridades	No se evidencia la existencia de un proceso definido.	NO	SI	La institución considera que este control se debe excluir, debido a que las comunicaciones de incidentes se deben dar a nivel gerencial.
4	A.6.1.4. Contacto con grupos especiales de interés	No se evidencia la existencia de comunicaciones con grupos de interés con respecto a temas relacionados con seguridad de la información	NO	SI	La institución considera que este control se debe excluir, debido a que todo evento de seguridad de información será comunicado al comité de seguridad de información; mediante los canales que se establezcan.

5	A.6.1.5. Seguridad de la información en la gestión de proyectos	Se evidencia que no existen controles que incluyan temas de seguridad de la información en la gestión de proyectos.	NO	SI	La institución no ha establecido las disposiciones necesarias para el cumplimiento de este control, debido a que no se generan proyectos..
Objetivo de Control	**A.6.2. Dispositivos Móviles y teletrabajo**				
1	A.6.2.1. Política de dispositivos móviles.	No se encontraron políticas para la utilización de dispositivos móviles	NO	SI	La institución no asigna dispositivos móviles para la ejecución de funciones
2	A.6.2.2. Teletrabajo	Se han identificado medidas que evitan accesos no autorizados mediante la conexión remota.	SI	SI	Se han establecidos los medios necesarios para el teletrabajo
Dominio	**A.7. SEGURIDAD DE LOS RECURSOS HUMANOS**				
Objetivo de Control	**A.7.1. Antes del Empleo**				
1	A.7.1.1. Selección	Se realiza la revisión de la documentación presentada por los colaboradores durante el proceso de selección.	SI	SI	Se excluye este control debido a que la institución realiza la revisión de la documentación presentada por los colaboradores durante el proceso de selección
2	A.7.1.2. Términos y condiciones del empleo	Existen clausulas sobre seguridad de la información en los contratos	SI	SI	Se excluye este control debido a que las cláusulas de confidencialidad están estipuladas en los contratos.
Objetivo de Control	**A.7.2. Durante del Empleo**				
1	A.7.2.1. Responsabilidades de la Gerencia	No existe un procedimiento de formación continua para mantener las habilidades en el desarrollo de las acciones antes y durante al acceso a los activos de información.	NO	SI	La institución considera que este control debe estar como parte de la segregación de las funciones del comité de seguridad, en la evaluación del cumplimiento de las políticas
2	A.7.2.2. Conciencia, educación y capacitación sobre la seguridad de la información	El reglamento interno de trabajo regula los temas relacionados a la confidencialidad de información por parte de los colaboradores.	SI	SI	La institución considera que este control debe ser excluido, debido a que el reglamento interno de trabajo regula los temas relacionados a seguridad de información; el mismo documento que es de conocimiento a todos los colaboradores.

3	A.7.2.3. Proceso disciplinario	El reglamento interno de trabajo indica las sanciones disciplinarias para los colaboradores que infrinjan la confidencialidad de la información.	SI	SI	La institución considera que este control debe ser excluido, debido a que en el reglamento interno de trabajo se encuentran indicadas las sanciones disciplinarias ante incumplimiento, las mismas que son de conocimiento a todos los colaboradores.
Objetivo de Control	**A.7.3. Terminación y cambio de empleo**				
1	A.7.3.1. Terminación o cambio de responsabilidades del empleo	No se han definido procedimientos que garanticen la seguridad de la información al término de vínculo laboral.	NO	SI	La institución considera que este control debe estar como parte de la segregación de las funciones del comité de seguridad, en la evaluación del cumplimiento de las políticas
Dominio	**A.8. GESTIÓN DE ACTIVOS**				
Objetivo de Control	**A.8.1. Responsabilidad de los Activos**				
1	A.8.1.1. Inventario de Activos	La administración cuenta con inventario de activos, pero dicho inventario no está estandarizado además de no contar con las actualizaciones pertinentes.	SI	NO	Realizar el inventario de activos según lo estipulado en la NTP ISO 27001:2014, a fin de dar cumplimiento con la normativa vigente.
2	A.8.1.2. Propiedad de los Activos	El responsable de cada oficina es el responsable del activo informático que se encuentra dentro de su ámbito laboral.	SI	NO	Establecen propietarios de los activos a fin de mantener las responsabilidades del uso aceptable de los activos
3	A.8.1.3. Uso aceptable de los activos	La administración no cuenta con la documentación necesaria para el uso aceptable de los activos.	SI	SI	La institución considera que este control debe excluirse debido a que se cuenta con la documentación necesaria para el uso de los activos, así mismo establece que mediante los párrafos precedentes se dará cumplimiento.
4	A.8.1.4. Retorno de Activos	Se ha definido un procedimiento, sin embargo no se encuentra documentado.	SI	SI	La institución considera que este control debe excluirse, debido a que los activos salen de las instalaciones toda vez que se realizan campañas Tributarias; para ellos el procedimiento de traslado y retorno se cumple con responsabilidad.
Objetivo de Control	**A.8.2. Clasificación de la Información**				

1	A.8.2.1. Clasificación de la Información	La administración no cuenta con la clasificación de los activos, la documentos son almacenados sin contar con los rótulos respectivos	NO	NO	Realizar la clasificación y etiquetado de activos conforme a la importancia de los mismos, a fin de dar cumplimiento con la normativa vigente.
2	A.8.2.2. Etiquetado de la Información	La administración no cuenta con un control de etiquetado de información.	NO	NO	
3	A.8.2.3. Manejo de Activos	La administración no cuenta con procedimientos de manipulación de la información	NO	NO	Se requiere garantizar la protección y el manejo optimo del activo a través del procedimiento de gestión de activos
Objetivo de Control	**A.8.3. Manejo de los Medios**				
1	A.8.3.1. Gestión de Medios Removibles	La administración cuenta con el control de medios removibles, sin embargo, no ha sido documentado.	SI	NO	Este control debe ser documentado y hacerse de conocimiento a fin de evitar la propagación de virus informáticos y fuga de información
2	A.8.3.2. Disposición de Medios	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	SI	La institución considera que este control debe ser excluido, debido a que los procedimientos de disposición de medios se realizan con responsabilidad.
3	A.8.3.3. Transferencia de los medios	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	SI	La institución considera que este control debe ser excluido, debido a que los procedimientos de transferencia de medios se realizan con responsabilidad.
Dominio	**A.9. CONTROL DE ACCESOS**				
Objetivo de Control	**A.9.1. Requisitos de la Empresa para el Control de Accesos**				
1	A.9.1.1. Política de Control de Accesos	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	NO	La institución debe establecer roles y perfiles de acceso de acuerdo a las funciones del cargo dando cumplimiento a los acuerdos de confidencialidad,
2	A.9.1.2. Accesos a redes y Servicios de red	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	NO	Es necesario que solo los usuarios de la red y servicios de red tengan permisos de acceso específicos a las conexiones de la institución
Objetivo de Control	**A.9.2. Gestión de Accesos de usuario**				

1	A.9.2.1. Registro y baja de usuarios	La administración cuenta con el control de procesos formales para el registro y baja de usuarios.	SI	NO	Se debe documentar el proceso que permita asignar y revocar los derechos de acceso, cuando el colaborador inicie o finalice su vinculación laboral
2	A.9.2.2. Aprovisionamiento de acceso de usuario	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	SI	La institución establece que este control debe ser excluido, debido a que se da cumplimiento mediante el control A9.2.1.
3	A.9.2.3. Gestión de derechos de acceso privilegiado	El control de accesos es definido por el perfil del puesto del colaborador	SI	SI	La institución establece que este control debe ser excluido, debido a que se da cumplimiento mediante el control A9.2.1.
4	A.9.2.4. Gestión de información de autenticación secreta de usuario	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	NO	Se requiere verificar la identidad de los usuarios que hacen uso de los sistemas de la institución por medio de autenticación de usuario
5	A.9.2.5. Revisión de derechos de acceso de usuario	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	NO	Los responsables de los activos de información deben validar que los permisos estén acordes con las funciones del cargo, para asegurar que no hayan obtenido privilegios no autorizados
6	A.9.2.6. Remoción o ajustes de derechos de acceso	La administración cuenta con el control, sin embargo, no ha sido documentado.	SI	NO	Los responsables de los activos de información deben validar que los permisos estén acordes con las funciones del cargo, para asegurar que no hayan obtenido privilegios no autorizados. En caso de finalización de contrato se deben revocar los permisos
Objetivo de Control	**A.9.3. Responsabilidad de los Usuarios**				
1	A.9.3.1. Uso de Información de autenticación secreta	Existe el control pero no se encuentra documentado, sin embargo, se detectó que las contraseñas son compartidas por los colaboradores de la administración	SI	NO	Los colaboradores deben cumplir con las directrices establecidas en la política para salvaguardar la información a través de la autenticación.
Objetivo de Control	**A.9.4. Control de Acceso a Sistema y aplicación**				
1	A.9.4.1. Restricción de acceso a la información	El control se encuentra implementado, sin embargo, no se ha documentado.	SI	NO	Los responsables de los activos de información deben validar que los derechos de acceso de los

2	A.9.4.2. Procedimientos de acceso seguro	El control se encuentra implementado mediante los roles de acceso a los sistemas de información.	SI	NO	usuarios estén acordes con las funciones del cargo.
3	A.9.4.3. Sistema de Gestión de contraseñas	El control se encuentra implementado mediante el procedimiento de cambio de contraseñas.	SI	NO	Se requiere asegurar la calidad de las contraseñas para el ingreso confiable a los sistemas.
4	A.9.4.4. Uso de programas utilitarios privilegiados	El control se encuentra implementado mediante los roles de acceso a los sistemas de información.	SI	SI	La institución considera que este control debe ser excluido, debido a que se encuentra implementado mediante los roles de acceso a los sistemas de información.
5	A.9.4.5. Control de acceso al código fuente de los programas	El control se encuentra implementado mediante la gestión de cambios de los sistemas de información.	SI	SI	La institución considera que este control debe ser excluido, debido a que se encuentra implementado mediante la gestión de cambios de los sistemas de información.
Dominio	**A.10. CRIPTOGRAFÍA**				
Objetivo de Control	**A.10. Controles Criptográficos**				
1	A.10.1.1. Política sobre el uso de controles criptográficos	La administración cuenta con la política sobre el uso de controles criptográficos.	SI	SI	La institución considera que este control debe ser excluido, debido a que la utilización de la criptografía y el tráfico de la información garantizan la protección de la misma.
2	A.10.1.2. Gestión de claves	La administración no cuenta con el control	SI	SI	
Dominio	**A.11. SEGURIDAD FÍSICA Y DEL AMBIENTE**				
Objetivo de Control	**A.11.1. Áreas Seguras**				
1	A.11.1.1. Perímetro de Seguridad física	El área e tratamiento de información cuenta con las medidas de control establecidas, puertas con entrada por recepción.	SI	NO	Se debe establecer los perímetros de seguridad necesarios para proteger la información y controlar el acceso en aquellas oficinas de tratamiento de información sensible.
2	A.11.1.2. Controles de acceso físico	La administración cuenta con el control de acceso a áreas restringidas, sin embargo, se pudo evidenciar que los colaboradores ingresan constantemente al área de tratamiento de información	SI	NO	Las áreas de información sensible deberán estar protegidas por un sistema de control físico

3	A.11.1.3. Asegurar oficinas, áreas e instalaciones	La administración cuenta con el control de aseguramiento de oficinas	NO	SI	La institución considera que este control debe ser excluido, debido a que las oficinas de tratamiento de información sensible se encuentran con controles de acceso físico.
4	A.11.1.4. Protección contra amenazas externas y ambientales	La administración no cuenta con un Plan de Recuperación ante desastres.	NO	NO	Para proteger a la institución se debe contar con el conocimiento adecuado del manejo de daños naturales o causados por el hombre
5	A.11.1.5. Trabajo en áreas seguras	La administración no cuenta con un control de supervisión a los colaboradores o visitantes.	NO	SI	La institución considera que este control debe ser excluido, debido a que las oficinas de tratamiento de información sensible se encuentran con controles de acceso físico.
Objetivo de Control	**A.11.2. Equipos**				
1	A.11.2.1. Emplazamiento y protección de equipos	La administración cuenta con el control de protección de equipos.	SI	NO	Se debe establecer un área segura para la ubicación de los equipos y minimizar la exposición a peligro ambiental y la intrusión no autorizada.
2	A.11.2.2. Servicio de suministro	Los ups no cuentan con mantenimiento adecuado generando cortes de energía lo que ha ocasionado paralización de las actividades.	SI	NO	Se deben garantizar el servicio de potencia para los equipos de la institución.
3	A.11.2.3. Seguridad en el cableado	Los cables de red y energía no cuentan con la protección adecuada, se encuentran expuestos.	SI	NO	El cableado de red y energía debe estar debidamente identificado e implementado mediante una opción segura.
4	A.11.2.4. Mantenimiento de equipos	La falta del plan de mantenimiento correctivo de equipos informáticos, ha ocasionado fallas en las unidades de almacenamiento de los servidores del centro de datos, ocasionando pérdidas económicas.	SI	NO	Se deben implementar directrices de mantenimiento correctivo de equipos que garanticen su disponibilidad. Estas directrices deben establecer los intervalos y las especificaciones del servicio y deben ser registradas en bitácoras detallando las fallas y los mantenimientos efectuados
5	A.11.2.5. Renovación de activos	La administración cuenta con el control de salida de equipos.	SI	SI	La institución considera que este control debe ser excluido, debido a que no se cuenta con presupuesto para realizar la renovación de los activos de información.

6	A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	La administración mantiene el registro de custodia de los equipos que se encuentran fuera de las instalaciones.	SI	NO	Para proteger los activos fuera de la instalación de la institución se deben generar directrices que estén enfocadas a la seguridad de los mismos durante las campañas tributarias que se realizan.
7	A.11.2.7. Disposición o reutilización segura de equipos	Los equipos son formateados en las unidades de almacenamiento, toda vez que sea coordinado con cada responsable de oficina.	SI	NO	Se debe disponer de procedimientos para la disposición y reutilización de los equipos, los cuales garantizarán la eliminación de la información ya sea por destrucción o sobre escritura, de tal forma que esta información no sea recuperable.
8	A.11.2.8. Equipos de usuarios desatendidos	Los equipos se encuentran dentro del directorio activo y se cuentan con políticas de escritorio limpio.	SI	SI	La institución considera que este control debe ser excluido, debido a que los usuarios tienen en claro los procedimientos de uso de los equipos, la confidencialidad de la información, el uso de las contraseñas y manejo de las sesiones
9	A.11.2.9. Política de escritorio limpio y pantalla limpia	Los equipos se encuentran dentro del directorio activo y se cuentan con políticas de escritorio limpio.	SI	SI	
Dominio	**A.12. SEGURIDAD DE LAS OPERACIONES**				
Objetivo de Control	**A.12.1. Procedimientos y responsabilidades operativas**				
1	A.12.1.1. Procedimientos operativos documentados	Los procedimientos en los que están involucrados actividades de procesamiento de información no se encuentran definidos y documentados.	SI	NO	Se deben actualizar los procedimientos y documentarlos para las actividades de operaciones de tal forma que garanticen la seguridad.
2	A.12.1.2. Gestión de cambio	La administración no cuenta controles para la gestión de cambios.	NO	NO	Los cambios en los procesos deben documentarse. La documentación debe contener aspectos como: identificación, planificación, valoración del impacto etc.
3	A.12.1.3. Gestión de la capacidad	Se realizan pruebas sobre rendimientos de sistemas, optimización de procedimientos a fin de evitar cuellos de botellas; sin embargo no se encuentran documentados.	SI	NO	Se deben crear los procedimientos y documentarlos para asegurar que las pruebas de rendimiento de sistemas sean realizadas; a fin de evitar demoras en los procesos que se realizan en los sistemas de información
4	A.12.1.4. Separación de los entornos de desarrollo, pruebas y	Debido a la falta de segregación de funciones a los programadores de OTIC, la administración no cuenta con entornos de	SI	SI	La institución considera que este control debe ser excluido, debido a cuenta con entornos de desarrollo y pruebas por separados.

	operaciones	desarrollo y pruebas por separados.			
Objetivo de Control	**A.12.2. Controles contra código malicioso**				
1	A.12.2.1. Controles contra código malicioso	La administración cuenta con antivirus con licencias vencidas, motivo por el cual sufrieron un ataque por Ransomware.	SI	NO	Se debe garantizar la seguridad de la información creando políticas y controles que prohíban el uso de software no autorizado, hacer la detección de software no autorizado, restringir el acceso a sitios web que se sospecha son malicioso.
Objetivo de Control	**A.12.3. Respaldo**				
1	A.12.3.1. Respaldo de la información	La administración cuenta con la actividad de realizar copias de seguridad de base de datos, sin embargo no se realizan la verificación de validez.	SI	NO	La política de respaldo de datos debe contener los requisitos necesarios para realizar la copia de información tanto de hardware como de software a fin de preservar la disponibilidad de la información.
Objetivo de Control	**A.12.4. Registro y monitoreo**				
1	A.12.4.1. Registro de eventos	La administración no cuenta con un registro de eventos para los cambios que se hagan manualmente a la base de datos.	NO	NO	Para dar un correcto manejo a los eventos se deben establecer los procedimientos y directivas necesarias para el registro, almacenamiento y consultas de los eventos log
2	A.12.4.2. Protección de información de registro	No se ha establecido un sistema de protección para los registros, así mismo, no se cuenta con la segregación de funciones dentro del entorno de desarrollo.	SI	SI	La institución considera que este control se debe excluir, debido a que se se ha establecido un sistema de protección para los registros.
3	A.12.4.3 Registro del administrador y del operador	La administración no cuenta con un registro de eventos para los cambios que se hagan manualmente a la base de datos.	NO	SI	La institución considera que este control se debe excluir, debido a que se daría cumplimiento mediante el control A.12.4.1.
4	A.12.4.4. Sincronización de reloj	La administración no cuenta con un procedimiento para el registro de eventos.	SI	SI	La institución considera que este control se debe excluir, debido a que los relojes de los sistemas de información se encuentran sincronizados a los servidores.
Objetivo de	**A.12.5. Control de Software en la Producción**				

Control					
1	A.12.5.1. Instalaciones de Software en sistemas operacionales	Existen permisos de usuario para instalación de software, sin embargo, estos no son monitoreados o controlados llevando así a la instalación de software no autorizados.	SI	NO	Solo el personal autorizado dentro de la institución puede hacer la instalación o desinstalación de software en los equipos de la misma, a fin de llevar un control.
Objetivo de Control	**A.12.6. Gestión de vulnerabilidad técnica**				
1	A.12.6.1. Gestión de Vulnerabilidades técnicas	No se han establecido métodos para identificar las posibles vulnerabilidades técnicas a las que podrían estar expuestas los activos de información.	SI	SI	La institución considera que este control se debe excluir, debido a que este análisis formará parte del SGSI.
2	A.12.6.2. Restricciones de instalación de software	No se han establecido medidas restrictivas para la instalación de software, un usuario con perfil de administrador en el AD puede realizar descarga e instalaciones de aplicativos.	NO	NO	Solo el personal autorizado dentro de la institución puede hacer la instalación o desinstalación de software en los equipos de la misma, a fin de llevar un control.
Objetivo de Control	**A.12.7. Consideraciones para la auditoria de los sistemas de información**				
1	A.12.7.1. Controles de auditoria de Sistemas de Información	Se realizan auditorías a nivel institucional, sin embargo no se ha tenido hasta el momento una auditoria a los sistemas de información	SI	SI	La institución considera que este control se debe excluir, debido a que no se han considerado las auditorías a los sistemas de información; así mismo, las auditorías realizadas a nivel institucional son documentadas y se realiza el seguimiento oportuno.
Dominio	**A.13. SEGURIDAD DE LAS COMUNICACIONES**				
Objetivo de Control	**A.13.1. Gestión de la Seguridad de la Red**				
1	A.13.1.1. Controles de la red	Se han gestionado los elementos físicos que dan soporte a la red.	SI	NO	La institución considera que este control se debe excluir, debido a que se tienen establecidos los procedimientos para la configuración segura de los dispositivos de red.

2	A.13.1.2. Seguridad de los servicios de red	No se han establecido los requisitos de disponibilidad de la red, así mismo no se ha realizado la evaluación de riesgos a los que se encuentra expuesta la red.	NO	NO	La institución considera que este control se debe excluir, debido a que cuenta con los mecanismos de control para gestionar los servicios de red
3	A.13.1.3. Segregación en redes	La administración implantó hace un mes la segregación de la red, como medida de prevención ante el ataque de Ransomware.	SI	NO	Para una mejor gestión y control de red se deben segmentar los dominios creando separación de red.
Objetivo de Control	**A.13.2. Transferencia de información**				
1	A.13.2.1. Políticas o procedimientos para la transferencia de información	No se han establecidos procedimientos que regulen la transferencia de información.	SI	SI	La institución considera que este control se debe excluir, debido a que la información solo es transferida por correo institucional y considera que a nivel gerencial se tienen las pautas para realizar el envío de la misma.
2	A.13.2.2. Acuerdos de transferencia de información	No se han establecido acuerdos para el intercambio de información.	SI	SI	
3	A.13.2.3. Mensajes Electrónicos	No se han establecido criterios de envió de mensajería electrónica.	SI	SI	
4	A.13.2.4. Acuerdos de confidencialidad o no divulgación	Se han establecido acuerdos de confidencialidad para el intercambio de información.	SI	NO	Los criterios de confidencialidad y no divulgación de información se consideran en los contratos de los colaboradores, además el reglamento interno de trabajo.
Dominio	**A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**				
Objetivo de Control	**A.14.1. Requisitos de Seguridad en los Sistemas de Información**				
1	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	Los requisitos de sistemas no son documentados.	SI	NO	La documentación del análisis de requerimientos de los sistemas deben ser incluidos en la etapa de desarrollo de nuevos sistemas o actualizaciones de los existentes, a fin de evitar retrasos en la aprobación de los mismos.
2	A.14.1.2. Aseguramiento de servicios de aplicaciones sobre redes públicas	Se cuenta con la seguridad a nivel WAF (Firewall de aplicaciones web)	SI	SI	La institución considera que este control se debe excluir, debido a que se cuenta con la seguridad a nivel WAF (Firewall de aplicaciones web)
Objetivo de	**A.14.2. Seguridad en los procesos de desarrollo y soporte**				

Control					
1	A.14.2.1. Política de desarrollo seguro		SI	SI	La institución considera que este control se debe excluir, debido a que esta política será considerada en el control A.5.1.1.
2	A.14.2.2. Procedimientos de control de cambios del sistema	Se Mantiene un control de cambios de sistemas, mediante un repositorio.	SI	SI	La institución considera que este control se debe excluir, debido a que se cuenta con el repositorio Tortoise mediante el cual se mantiene un control de los cambios.
3	A.14.2.3. Revisión Técnica de aplicaciones después de cambios a la plataforma operativa	Se mantiene un procedimiento establecido para realizar pruebas del sistema antes del pase a producción	SI	SI	La institución considera que este control se debe excluir, debido a que se mantiene un procedimiento establecido para realizar pruebas del sistema antes del pase a producción
4	A.14.2.4. Restricciones sobre cambios a los paquetes de software	se mantiene un control para las versiones generadas en los sistemas	SI	SI	La institución considera que este control se debe excluir, debido a que se cuenta con el repositorio Tortoise mediante el cual se mantiene un control de las versiones generadas de los sistemas, así mismo se tiene una copia de respaldo de las mismas.
5	A.14.2.5. Principios de ingeniería de sistemas seguros	No existe documentación de procedimientos sobre la implementación de seguridad de la información en el proceso de desarrollo.	NO	SI	La institución considera que este control se debe excluir, debido a que los procesos actuales cumplen con la finalidad de implementación de los sistemas de información.
6	A.14.2.6. Ambiente de desarrollo seguro	La administración no cuenta con un entorno de desarrollo de acceso restringido.	SI	SI	La institución considera que este control debe ser excluido, debido a que cuenta con un entorno de desarrollo de acceso restringido..
7	A.14.2.7. Desarrollo de contratado externamente	No se realizan desarrollos externos.	NO	SI	La institución considera que este control se debe excluir, debido a que no se realizan desarrollos de software por parte de terceros.
8	A.14.2.8. Pruebas de Seguridad del sistema	Se mantiene un procedimiento establecido para realizar pruebas funcionales en cuanto a seguridad de información antes del pase a producción.	SI	SI	La institución considera que este control se debe excluir, debido a que se mantiene un procedimiento establecido para realizar pruebas funcionales en cuanto a seguridad de información antes del pase a producción.

9	A.14.2.9. Pruebas de aceptación del sistema	Se mantiene un procedimiento establecido para realizar pruebas del sistema antes del pase a producción	SI	SI	La institución considera que este control se debe excluir, debido a que se mantiene un procedimiento establecido para realizar pruebas del sistema.
Objetivo de Control	**A.14.3. Datos de Prueba**				
1	A.14.3.1. Protección de datos de prueba	Se mantiene un entorno de pruebas con una base de datos copia del original cuyos datos pueden ser usados para las pruebas funcionales del sistema.	SI	SI	La institución considera que este control se debe excluir, debido a que se mantiene un entorno de pruebas con una base de datos copia del original cuyos datos pueden ser usados para las pruebas funcionales del sistema.
Dominio	**A.15. RELACIONES CON LOS PROVEEDORES**				
Objetivo de Control	**A.15.1. Seguridad de la Información en las relaciones con los proveedores**				
1	A.15.1.1. Política de seguridad de la información para las relaciones con los proveedores	Existe un política de confidencialidad de información con el proveedor de servicios en la nube	SI	SI	La institución considera que este control se debe excluir, debido a que existe un política de confidencialidad de información con el proveedor de servicios en la nube
2	A.15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores	Se han establecido los requisitos de seguridad de la información con el proveedor de servicios en la nube.	SI	SI	La institución considera que este control se debe excluir, debido a que se han establecido los requisitos de seguridad de la información con el proveedor de servicios en la nube.
Dominio	**A.16. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN**				
Objetivo de Control	**A.16.1. Gestión de incidentes de la Seguridad de la Información y mejoras**				
1	A.16.1.1. Responsabilidades y procedimientos	No existen procedimientos que dirijan el proceso de gestión de incidentes de la seguridad de información.	NO	NO	Se deben establecer responsabilidades y procedimientos para la gestión de los incidentes de seguridad de la información, que permitan asegurar una respuesta oportuna y eficaz.
2	A.16.1.2. Reporte de eventos de seguridad de la información	Se han establecido canales de comunicación para informar sobre algún incidente de seguridad de la información.	SI	NO	Todos los colaboradores deben conocer el procedimiento para reportar eventos de seguridad de la información a través de los canales establecidos para tal fin.

3	A.16.1.3. Reporte de debilidades de seguridad de la información	No se ha definido un formato de reporte de debilidades de los sistemas en cuanto a seguridad de la información.	NO	NO	Se debe definir la información necesaria que debe contener el reporte de eventos de seguridad de información, a fin de mantener una base de conocimiento.
4	A.16.1.4. Evaluación y decisión sobre eventos de seguridad de la información	No se ha realizado la evaluación de riesgos en seguridad de la información dentro de la administración.	NO	NO	Es necesario evaluar cada evento de seguridad teniendo en cuenta la clasificación, priorización e impacto para determinar si corresponde a un incidente de seguridad de la información
5	A.16.1.5. Respuesta de incidentes de seguridad de la información	No se ha determinado un proceso para la resolución de incidentes de seguridad de la información.	NO	NO	Es necesario determinar el tiempo de respuesta de cada evento, a fin de evitar retraso en los procesos core de la institución
5	A.16.1.6. Aprendizaje de los incidentes de la seguridad de información	No se ha establecido una base de conocimiento sobre los incidentes de seguridad de la información	NO	NO	Se generará una base de conocimiento sobre los eventos de seguridad ocurridos en la institución, a fin de obtener los procedimientos necesarios que serán ejecutados toda vez que el evento vuelva a repetirse.
7	A.16.1.7. Recolección de evidencias	La evidencia ante un incidente de seguridad de la información queda al resguardo de OTIC.	SI	SI	La institución considera que este control se debe excluir, debido a que se considerará como parte de las responsabilidades del oficial de seguridad la recopilación de evidencias.
Dominio	**A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO**				
Objetivo de Control	**A.1.7.1. Continuidad de Seguridad de la información**				
1	A.17.1.1. Planificación de continuidad de seguridad de la información	La administración no cuenta con un Plan de Continuidad de negocio o Plan de contingencia frente a incidentes de seguridad de la información.	NO	NO	Es necesario que la institución cuente con el Plan de continuidad del Negocio documentado y actualizado.
2	A.17.1.2. Implementación de continuidad de seguridad de la información	La administración no cuenta con un Plan de Continuidad de negocio o Plan de contingencia frente a incidentes de seguridad de la información.	NO	SI	La institución considera que este control se debe excluir, debido a que se dará cumplimiento mediante el control A.17.1.1
3	A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	La administración no cuenta con un Plan de Continuidad de negocio o Plan de contingencia frente a incidentes de seguridad de la información.	NO	NO	El cableado de red y energía debe estar debidamente identificado e implementado mediante una opción segura.

Objetivo de Control	**A.17.2. Redundancias**				
1	A.17.2.1. Instalaciones de procesamiento de la información	No se ha determinado que activos de información requieren ser redundados.	NO	SI	La institución considera que este control se debe excluir, debido a que se dará cumplimiento mediante el control A.17.1.1
Dominio	**A.18. CUMPLIMIENTO**				
Objetivo de Control	**A.18.1. Cumplimiento con los Requisitos Legales y Contractuales**				
1	A.18.1.1. Identificación de los requisitos contractuales y legislación aplicables	Si, el estado Peruano mediante Resolución Ministerial N°004-2016-PCM, modificada por la Resolución Ministerial Nº 166-2017-PCM, el uso obligatorio de la Norma Técnica Peruana “NTP-ISO/IEC 27001:2014"	SI	NO	Se deben dar cumplimiento a los requisitos legales pertinentes a fin de mantener la seguridad de la información
2	A.18.1.2. Derechos de propiedad intelectual	No se ha definido un procedimiento sobre la propiedad intelectual de los productos de software.	NO	SI	La institución considera que este control se debe excluir, debido a que se considera que cada desarrollo realizado en las instalaciones, es de propiedad de la misma, toda vez que ningún colaborador puede extraer el código fuente de los sistemas.
3	A.18.1.3. Protección de Registros	No se han definido las políticas para la protección de información.	NO	SI	La institución considera que este control se debe excluir, debido a que por ser entidad Tributaria, la institución se encuentra obligada al cumplimiento de la Reserva Tributaria recogida en el artículo 2° inciso 5) de la Constitución.
4	A.18.1.4. Privacidad y protección de datos personales	Si, el estado Peruano cuenta con una ley de protección de datos personales Ley N° 29733, la cual se rige la administración debido a tratamiento de información confidencial de contribuyentes.	SI	SI	La institución considera que este control se debe excluir, debido a que el estado Peruano cuenta con una ley de protección de datos personales Ley N° 29733, la cual se rige la administración debido a tratamiento de información confidencial de contribuyentes.
5	A.18.1.5. Regulación de controles criptográficos		SI	SI	La institución considera que este control se debe excluir, debido a que se cuenta con la seguridad a nivel WAF (Firewall de aplicaciones web)
Objetivo de	**A.18.1. Cumplimiento con los Requisitos Legales y Contractuales**				

Control					
1	A.18.2.1. Revisión independiente de la Seguridad de la Información	La administración no cuenta con un SGSI documentado e implementado	NO	NO	Es necesario que se implemente el Sistema de Seguridad de Información en la institución, teniendo en consideración los incidentes de seguridad ocurridos; de esta forma se podrá mantener la disponibilidad, confidencialidad e integridad de la información
2	A.18.2.2. Cumplimiento de políticas y normas de seguridad	No se realiza el cumplimiento de las políticas y controles de seguridad de la información con las que cuenta la administración.	NO	NO	Es necesario establecer controles que aseguren la correcta implementación y operación de la gestión de seguridad de la información en la institución
3	A.18.2.3. Revisión de Cumplimiento Técnico.	No se realiza la evaluación si los sistemas de información se encuentran configurados de acuerdo a las políticas existentes en la administración.	NO	NO	Se requiere evaluar el cumplimiento de las políticas, procedimientos y demás requisitos de seguridad de la información realizando pruebas a través de herramientas que permitan la interpretación y valoración de vulnerabilidades que puedan comprometer la seguridad de los sistemas.

VI. DISCUSIÓN, CONCLUSIONES y RECOMENDACIONES

VI.1. Discusión

Del análisis realizado en la presente investigación, se ha obtenido un análisis de resultados por cada objetivo planteado:

VI.1.1. Del estado actual de la institución en materia de seguridad de información.

Del análisis realizado a la situación actual de la institución mediante el análisis de brechas o análisis GAP en cuanto a los 7 requisitos de la NTP-ISO/IEC 27001:2014 (numerales 4 al 10) se ha obtenido el nivel de cumplimiento de 1 que corresponde al nivel inicial en donde el control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe; es decir solo se cumple con el 25% de los requisitos mínimos necesarios para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de Información, mientras que la brecha existente del 75% correspondes a procesos inexistentes o aquellos procesos que no se encuentran documentados.

Así mismo, se realizó el análisis para los 14 dominios, 35 objetivos de control y 114 controles establecidos en el anexo A de la misma norma se ha obtenido el nivel de cumplimiento del 0.9 que corresponde al nivel inicial en donde el control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe; es decir solo el 35% de los controles se están ejecutando sin embargo no se encuentran documentados o no se soportan en una política documentada, aprobada y de conocimiento a los colaboradores de la institución; mientras que la brecha existente del 65% corresponden a aquellos controles que no se evidencian en la institución además de, aquellos que por la naturaleza de la misma no se aplican.

El análisis de brechas ha logrado determinar que la situación actual de la institución en cuanto a los temas de seguridad de la información se encuentra en nivel inicial en donde el control esta implementado no obstante el modelo de seguridad de políticas, procedimientos y estándares de configuración, no existe; con respecto al nivel mínimo aceptable el 3 definido, en donde los procedimientos se han estandarizado y documentado, y se han difundido a través del entrenamiento. Por lo expuesto, se identifica a la seguridad de la información como una necesidad inmediata de aplicación por ello se considera una necesidad la implementación, basado en el diseño propuesto, del Sistema de Gestión de Seguridad de Información cuyas políticas estarán definidas y así proteger los activos de información y dar cumplimiento a la normativa vigente.

La conclusión descrita puede compararse con las investigaciones descritas en el punto II (II.1. Antecedentes), en donde el autor de la tesis “Relación de la NTP ISO/IEC 27001:2008 EDI y la seguridad de la Información en los Ministerios del Estado Peruano al 2015” (Flores Solis & Guerra Farfan, 2017) establece que el

SGSI no es solo el tratamiento de riesgos, si no es un conjunto de políticas e implementación de controles preventivos, defectivos y correctivos que pueden minimizar las brechas y mejorar drásticamente el porcentaje de cumplimiento al nivel establecido por la institución.

VI.1.2. Del análisis de riesgos a los que se encuentra expuestos la institución.

Con la información obtenida del análisis GAP se procedió a realizar la identificación y valoración de los activos de información dentro de la institución, obteniendo que los activos de información según su valoración, se concentran en la clasificación de muy alto correspondiente al 33%, alto correspondiente al 27%, seguido del 20% y 13% para medio y bajo correspondiente; finalmente existe una valoración baja del 7%. Y según evaluación del impacto que genera en la administración en caso de pérdida o robo del activo de información, se pueden observar en la figura N° 21; donde se produce un impacto alto del 45%, así mismo se obtiene el 33% de impacto mediano y el 22% para impacto bajo. Así mismo, se identificaron las vulnerabilidades y amenazas a los que se encuentran expuestos dichos activos; esta información fue necesaria para realizar la evaluación de riesgos, del resultado obtenido durante la evaluación de los riesgos de la institución se puede evidenciar que se encontraron 15 situaciones que se encuentran en el nivel de riesgo alto, es decir existe la necesidad de tomar medidas correctivas en corto o mediano plazo; 5 situaciones que se encuentran en el nivel de riesgo extremo, es decir, existe la necesidad urgente de tomar medidas preventivas en corto plazo; así mismo, 5 situaciones que se encuentran en nivel de riesgo moderado es decir se pueden tomar medidas en un tiempo razonable o por el contrario se puede aceptar el nivel de riesgo.

La identificación de los riesgos a los que se encuentra expuesta la institución constituye uno de los pasos más importantes para la implementación de la NTP-ISO/IEC 27001:2014 debido a que va permitir conocer a aquellos riesgos a los que se encuentran expuesta la institución y que generan un nivel de impacto extremo y alto; a fin de establecer medidas de control que permitan mitigar, evitar o transferir los riesgos; el mismo análisis que se apoya en lo indicado por los autores de la tesis “Diseño e Implementación de un Sistema de Gestión de Seguridad de Información para proteger los activos de información de la Clínica MEDCAM PERÚ SAC” (Cruz Dias & Fukusaki Infantas, 2017); en donde indica que los riesgos de la seguridad de información deben ser conocidos, asumidos, gestionados y minimizados; de esta manera se protege la información de un amplio rango de amenazas.

VI.1.3. Seleccionar los controles y objetivos de control de la seguridad de información ajustados a las vulnerabilidades detectadas

Para realizar la selección de controles se ha desarrollado la declaración de aplicabilidad de la NTP-ISO/IEC 27001:2014, en el que se ha desarrollado un análisis en el que se identificaron que existen 62 objetivos de control que se vienen desarrollando sin embargo estos no se encuentran sustentados en una política o documentación que ha sido dada de conocimiento a los colaboradores de la institución, así mismo, se han identificado 55 objetivos de control que serán excluidos debido a la falta de presupuesto, considerando también que en ciertos casos los objetivos de control evaluados se apoyan en otros que si han sido considerados de implementación o por el contrario la gerencia durante la evaluación determino que dicho objetivo de control puede ser excluido por no ser necesario, de igual forma entre los objetivos de control existentes y los que no se encuentran implementados se han identificado 59 objetivos de control que serán implementados como parte del desarrollo del Sistema de Gestión de Seguridad de Información; para ello se han identificado diversas actividades que de ser aprobado por la Gerencia General, deberán ser desarrolladas para llevar a cabo la implementación de dichos controles. Así mismo, se ha establecido que el costo total de implementación asciende a 2, 241,855.75 soles, sin embargo, se evidenció que en la actualidad existe un proyecto de Renovación del Centro de Datos que esta valorizado en 2, 221,936.94 soles los cuales se reducen del costo de la implementación del SGSI quedando a evaluación por parte de la Gerencia General el monto total de 19,918.81 soles, a fin de determinar la viabilidad económica de la misma.

Es preciso señalar, que la implementación de los objetivos de control provee a la Gerencia General dirección y apoyo para gestionar la seguridad de información de la institución, de igual forma, la implementación asegura la correcta y segura operación de la información de la institución, debido a que se van a gestionar los riesgos con la finalidad de mitigar, evitar o transferir los riesgos; generando la confidencialidad, disponibilidad e integridad de la información.

Este resultado es similar a lo obtenido en la tesis “Implementación de Controles y Cumplimiento de Requisitos de la ISO/IEC 27001:2013 para la seguridad de información de una PYME Consultora” (Crystobal & Mechan, 2018); en donde el autor concluye que al implementar los controles requeridos se ha reducido el nivel de exposición en el que se encontrarían los activos de información, así mismo, la implementación de los controles de seguridad cumplió con los requisitos mínimos aceptables, relacionados a la Norma 27001

De acuerdo a lo expuesto se puede definir que, para que la gestión de seguridad de la información pueda ser implementada y mantenida en el tiempo, es importante contar con

el factor económico pues permitirá realizar las capacitaciones constantes en temas de seguridad de la información a los miembros integrantes del comité de seguridad de información de la institución, teniendo así también el equipamiento de hardware y software actualizado, mantener y hacer de conocimiento a los colaboradores de la institución la documentación de procesos y procedimientos referentes a la seguridad de información además de segmentar las funciones del oficial de seguridad y responsable de la oficina de Tecnología de información de tal forma que se dé cumplimiento a la Resolución Gerencial N° 260-2018 y por consiguiente a lo establecido en la Resolución Ministerial N°004-2016-PCM, modificada por la Resolución Ministerial Nº 166-2017-PCM. Este resultado es similar al obtenido en la tesis “Relación de la NTP ISO/IEC 27001:2008 EDI y la seguridad de la Información en los Ministerios del Estado Peruano al 2015” (Flores Solis & Guerra Farfan, 2017), donde los autores concluyen que al realizar el análisis a los Ministerios del estado Peruano, se hace fundamental establecer estrategias respecto de la implementación del SGSI en la Administración Pública Peruana basadas en la NTP-ISO/IEC 27001, que se encuentren orientadas a brindar una estructura organizacional de gestión de la información que permita el alineamiento de las tecnologías de información con la estrategia de negocios, el logro de beneficios, la reducción de costos, el control de riesgos y en general mejora en las operaciones de TI de las organizaciones.

VI.2. Conclusiones

La investigación desarrollada logró diseñar un Sistema de Gestión de Seguridad de la Información para proteger los activos de información de las instalaciones de la institución, lo cual se evidencia en:

- Se identificó las brechas existentes de seguridad, mediante el análisis GAP en donde se determinó que el nivel de cumplimiento a los requisitos de la NTP-ISO/IEC 27001:2014 es del 25% es decir, no se cumplen los requisitos mínimos necesarios para llevar a cabo el desarrollo del Sistema de Gestión de Seguridad de Información. Así mismo, se determinó el nivel de cumplimiento de los dominios establecidos en el anexo A de la misma norma, obteniendo un nivel de cumplimiento del 30%, es decir en la institución existen controles que se están ejecutando sin embargo no están documentados o no se soportan en una política documentada, aprobada y de conocimiento a los colaboradores de la institución.

- Se evaluó el proceso de gestión de riesgos de la institución donde se identificaron los activos, vulnerabilidad y amenazas que ayudaron a determinar el nivel de riesgo a los que se encuentran expuestos demostrando que existe un 20% de nivel de riesgo extremo, 60% de nivel de riesgo alto y el 20% de nivel de riesgo moderado; riesgos de seguridad de información que afectan los activos de información de la institución.

- Se realizó la selección de objetivos y objetivos de control de la seguridad de información establecidos en el Anexo A de la NTP-ISO/IEC 27001:2014, mediante la declaración de aplicabilidad Tabla N° 25, como propuesta de implementación aplicados según la tabla N° 24 Plan de Tratamiento de Riesgos los cuales serán ejecutados mediante la aprobación de Gerencia General.

VI.3. Recomendaciones

- Se recomienda la implementación del Sistema de Gestión de Seguridad de la Información para proteger los activos de información de la institución, con la finalidad de mantener un adecuado control y planificación de los incidentes que amenazan la seguridad de información de esta forma se logrará mantener la confidencialidad, integridad y disponibilidad de la misma.
- Implementar el sistema de gestión de seguridad de información para reducir la brecha de cumplimiento existente y aumentar el porcentaje de cumplimiento de seguridad de información, con la finalidad de garantizar el cumplimiento de las mismas; ello debe garantiza que los objetivos del negocio serán alcanzados y que los incidentes que puedan ocurrir serán prevenidos, detectados o corregidos.
- Contar con el proceso de gestión de riesgos en la institución va determinar la decisión sobre los riesgos que serán tratados mediante la aplicación de controles con la finalidad de evitar y mitigar la ocurrencia de los mismos.
- Implementar los dominios y objetivos de control de la seguridad de información que han sido analizados mediante el plan de tratamiento de riesgos, va permitir reducir el nivel de impacto de ocurrencia de los riesgos existentes en la institución.
- Finalmente se recomienda la implementación del Sistema de Gestión de Seguridad de la Información para proteger los activos de información de la institución, sin embargo la adopción del mismo constituye una decisión estratégica mediante la cual se va a preservar la información generando confianza a las partes interesadas debido a que los riesgos son adecuadamente manejados; sin embargo queda a cargo de la gerencia de la institución la toma de decisiones en base a los resultados obtenidos

VII. Lista de Referencias

Andrés Fabián Díaz, G. I. (2012). Implementacion de un SGSI en la comunidad Nuestra Señora de Gracia, alienado tecnológicamente con la Norma ISO 27001. Bogota - Colombia: Universidad EAN.

Barrantes, C. y. (2012). Diseño e Implementación de un Sistema de Gestión de Seguridad de Información en Procesos Tecnológicos. Lima - Perú: Universidad San Martín de Porres.

Carralli, R. A. (2004). The Critical Success Factor Method: Establishing a Foundation for Enterprise Security Managament.

CiberSeguridad. (2014). Gestion de Riesgo. En G. d. España, Gestion de Riesgo. Instituto Nacional de CiberSeguridad.

COBIT, M. d. (2021). Modelo de Madurez COBIT. Obtenido de COBIT: https://rincontic.org/2020/04/30/modelo-de-madurez-cobit/

CODESI. (2005). Plan de desarrollo de la sociedad de la información en el Perú - La Agenda Digital Peruana. (C. M. INFORMACIÓN, Ed.) Perú: Cortesia de Editora Perú S.A.

Cruz Dias, M., & Fukusaki Infantas, S. (2017). Diseño e Implementación de un Sistema de Gestión de Seguridad de Información para proteger los activos de información de la Clínica MEDCAM PERÚ SAC. Lima.

Crystobal & Mechan, d. l. (2018). Implementación de Controles y Cumplimiento de Requisitos de la ISO/IEC 27001:2013 para la seguridad de información de una PYME Consultora. Lima.

E & Y, E. &. (Octubre de 2013). Estar bajo Ciberataque. Recuperado el 24 de Noviembre de 2014, de http://www.ey.com/Publication/vwLUAssets/EY-Encuesta-Global-Seguridad-Informacion-EY-2013/$FILE/EY-Encuesta-Global-Seguridad-Informacion-EY-2013.pdf: http://www.ey.com/Publication/vwLUAssets/EY-Encuesta-Global-Seguridad-Informacion-EY-2013/$FILE/EY-Encuesta-Global-Seguridad-Informacion-EY-2013.pdf

El Peruano. (11 de Febrero de 2019). Obtenido de El peruano: https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

ElPeruano. (24 de mayo de 2012). Aprueban el uso obligatorio de 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” en todas las entidades integrantes del Sistema Nacional. NORMAS LEGALES.

ElPeruano. (08 de Enero de 2016). 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 Siste. Diario El Peruano. Obtenido de 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 to: https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/

ElPeruano. (Junio de 2017). Modifican el artículo 5 de la R.M. N° 004-2016-PCM. Diario El Peruano.

Eugenio Rivas, P. E. (2011). Implantación de un Sistema de Gestión de Seguridad de Información aplicada al dominio de Gestión de Activos para la Empresa Plásticos Internacionales PLASINCA SA. Ecuador: Escuela Superior Politécnica del Litoral.

Firma-e. (Octubre de 2014). Pilares de la Seguridad de Información. (F.-e. C. TI, Editor) Recuperado el de de 2017, de Seguridad de Informacion: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/

Flores Solis, F., & Guerra Farfan, J. (2017). Relación de la NTP ISO/IEC 27001:2008 EDI y la seguridad de la Información en los Ministerios del Estado Peruano al 2015. Callao.

Fonseca Herrera, O. (2019). “Modelo de un Sistema de Gestión de Seguridad de la Información en la organización GEOCONSULT cs” . Bogota.

Garcia Guevara, C. (2012). Establecimiento del Sistema de Seguridad de Información en SFG bajo los Estándares de la Norma ISO 27001: 2005. Bogota - Colombia: Universidad EAN.

Guano Zapata, M. (2020). Diseño de un SGSI bajo norma ISO/IEC 27001:2013 aplicado a un caso de estudio. Quito.

Huanambal, F. B. (20 de Noviembre de 2014). Monografías. com. Recuperado el 15 de Febrero de 2016, de http://www.mongrafías.com/trabajos103/sistema-bancario-peruano-historia-indicadores-bancarios-y-crisis-bancaria/sistema-bancario-peruano-historia-indicadores-bancarios-y-crisis-bancaria2.shtml

IEC/ISO27000. (2017). ISO27000.es. Obtenido de ISO27000.es: http://www.iso27000.es/iso27000.html

Informáticos, A. (2013). Activos Informáticos. Recuperado el 25 de Noviembre de 2014, de http://es.slideshare.net/meztli9/16-activos-inf.

ISO/IEC17799, I. (2005). Código de Buenas Practicas de la gestión de la Seguridad de Información.

ISO/IEC27000. (2005). El Directorio de la norma ISO 27000. En iso27000.es. Recuperado el 02 de Enero de 2015, de http://www.27000.org/: http://www.27000.org/

ISO/IEC-27002. (2013). NTP ISO IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la Información. Lima.

ISO/IEC27002:2013. (s.f.). ISO/IEC 27002:2013- El Anexo de ISO 27001. Recuperado el 10 de Enero de 2015, de ISO/IEC 27002:2013- 14 dominios, 35 objetivos de control y 114 controles: http://www.iso27002.es/

ISO31000. (2021). ISO31000. Obtenido de ISO31000: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es

ISO31010:2019. (s.f.). ISO 31010:2019 PARA LAS TÉCNICAS DE EVALUACIÓN DE RIESGOS. Obtenido de https://www.globalstd.com/blog/iso31010

ISOTools-ISO27001. (Febreró de 2019). ¿Qué es un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001? Obtenido de PLATAFORMA TECNOLÓGICA PARA LA GESTIÓN DE LA EXCELENCIA: https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

Mega, P. (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Montevideo Uruguay: Universidad de la Republica.

NIST800. (2014). SEGU.INFO- SEGURIDAD DE INFORMACION. Recuperado el 22 de Noviembre de 2014, de http://www.segu-info.com.ar/guias/nist.htm.

NTP-ISO/IEC17799:2007. (2007). NTP-ISO/IEC 17799:2007 Código de Buenas Prácticas para la Gestión de Seguridad de Informacion. Lima - Perú: ONGEI.

NTP-ISO/IEC27001:2014. (2014). Information technology - Security techniques - Information security management systems - Requirements. Lima.

NTP-ISO/IEC27001-2014. (2014). TECNOLOGIA DE INFORMACION. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Lima.

NTP-ISO/IEC27005:2009. (2011). NTP-ISO/IEC 27005: 2009 - Tecnología de la información - Técnicas de seguridad - Información de gestión de riesgos de seguridad. R.029-2009/INDECOPI-CNB. Recuperado el 24 de Noviembre de 2014, de http://translate.google.com.pe/translate?hl=es&sl=en&u=http://www.iso.org/iso/catalogue_detail%3Fcsnumber%3D42107&prev=search.

ONGEI. (2017). UN GOBIERNO ELECTRONICO. Obtenido de UN GOBIERNO ELECTRONICO: http://gobiernoelectronicope.blogspot.com/2013/07/que-es-el-ongei.html

Peruano, E. (2021). Plataforma del Estado Peruano. Obtenido de Plataforma del Estado Peruano: https://www.gob.pe/14086-sistema-de-gestion-de-seguridad-de-la-informacion

Rodriguez Correa, J. (2017). Diseño de un SGSI (Sistema de Gestión de Seguridad de Información) basado en la ISO27001 para laboratorios de servicios farmacéuticos de Calidad SFC LTDA. Bogota.

Salinas Rodríguez, M. S. (2017). Sistema de Gestión de Seguridad de la Información y Riesgos de Información en seis sedes de una entidad bancaria del Perú. Trujillo.

Sampieri, R. H. (1998). Metodologia de la Invesitgación - Cuarta Edición.

Seclen Arana, J. (2016). Factores que afectan la implementación del sistema de gestión de la seguridad de información en las entidades públicas peruanas de acuerdo a la NT-ISO/IEC 27001. Lima, Peru: UNIVERSIDAD NACIONAL MAYOR DE SAN MARCOS.

SGSI-ISO27000.ES. (s.f.). Sistema de Gestión de la Seguridad de la información. Obtenido de Sistema de Gestión de la Seguridad de la información: WWW.ISO27000.ES

Torres León, M. (2018). Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/ IEC 27001:2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones. Lima.

Valdunciel, L. M. (2007). Análisis de la Calidad de Servicio que prestan las Entidades Bancarias y su repercusión en la satisfacción del cliente y la lealtad hacia la Entidad. . Revista Asturiana de Economía, 85

Valencia, A. (2012). Una visión para hacer mas eficiente el desempeño del Sector Bancario en América Latina. IDC- Analyze The Future, 1.

VIII. ANEXOS

VIII.1. Anexo N° 01: Acta de Establecimiento de nivel de madurez mínimo aceptado acordado

Acta de Establecimiento de nivel de madurez mínimo aceptado acordado	
1. Información General	
Nombre de la Investigación:	Diseño de un Sistema de Gestión de Seguridad de Información para proteger los activos del Servicio de Administración Tributaria de la Zona Norte del Perú
Locación:	Servicio de Administración Tributaria de la Zona Norte del Perú
Preparado por:	Ing. Miryam Liliana Méndez Navarro
Hallazgos:	Se realizó el análisis con la finalidad de identificar la situación actual de la institución con respecto a la seguridad de la información, encontrándose que el nivel de cumplimiento de los requisitos de cumplimiento de la NTP-ISO/IEC 27001:2014 y controles referidos en el anexo A de la misma es del 25% (0.7) y 35% (1.04) respectivamente, es decir la institución se encuentra en un nivel de inexistente para los requisitos e inicial para la aplicación de controles de la norma referida.
Acuerdo:	Mediante la presente acta se acuerda que el Nivel “Mínimo aceptable”, sin necesidad que sea el óptimo deseado, al menos afirma cubrir los requerimientos clave de la administración; es 3 donde se tienen procesos que están definidos y documentados mediante políticas, procedimientos documentados, formalizados, aprobados y difundidos a todos los colaboradores de la institución.

VIII.2. Anexo N° 02: Guía de entrevista basado en los requisitos del SGSI

Guía de Evaluación de los Requisitos de la NTP-ISO/IEC 27001:2014			
Objetivo: Obtener la información necesaria sobre los requisitos indicados en la NTP-ISO/IEC 27001:2014 para la implementación del Sistema de Gestión de Seguridad de Información en el Servicio de Administración Tributaria de la Zona Norte del Perú; con la finalidad de determinar el nivel de cumplimiento de los mismos.			
Fecha:			
Nombre:	Cargo:		
Criterio NTP-ISO/IEC 27001:2014	**Pregunta**	**Si**	**No**
4. CONTEXTO DE LA ORGANIZACIÓN			
4.1. Comprender la Organización y su Contexto	¿Están identificados los objetivos del SGSI?		
	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?		
	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?		
4.2. Comprender las necesidades y expectativas de las partes interesadas	¿Se han identificado las partes interesadas?		
4.3. Determinar el alcance del Sistema de Gestión de Seguridad de Información	¿Se ha determinado el alcance del SGSI y se conserva información documentada?		
4.4. Sistema de Gestión de Seguridad de Información	¿El SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?		
5. LIDERAZGO			
5.1. Liderazgo y Compromiso	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?		
	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?		
	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?		
5.2. Política	¿Se ha definido una Política de la Seguridad de la Información?		
	¿Se ha comunicado la política de la Seguridad de la información a toda la administración?		
5.3. Roles, responsabilidades y autoridades organizacionales	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?		
6. PLANIFICACIÓN			
6.1. Acciones para tratar los riesgos y las oportunidades	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?		
	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?		
	¿Se ha definido un proceso de tratamiento de riesgos?		
6.2. Objetivos de seguridad de la información y planificación para conseguirlos	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?		
7. SOPORTE			
7.1. Recursos	¿Se identifican y asignan los recursos necesarios para el SGSI?		
7.2. Competencias	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?		

	¿Se mantiene información actualizada sobre la competencia del personal?		
7.3. Concientización	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?		
	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?		
7.4. Comunicación	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?		
	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?		
7.5. información Documentada	¿Se dispone de la documentación requerida por la norma más la requerida por la Norma ISO 27001 incluyendo registros?		
8. OPERACIÓN			
8.1. Planificación y Control operacional	¿Se han definido actividades basadas en un sistema de mejora continua que permita cumplir los objetivos, políticas y requisitos de la seguridad de la información?		
8.2. Evaluación de riesgos de seguridad de información	¿Realiza la administración la evaluación de riesgos de manera periódica?		
8.3. Tratamiento de riesgos de seguridad de información	¿La administración cuenta con un plan de tratamiento de riesgos de seguridad de información?		
9. EVALUACIÓN DEL DESEMPEÑO			
9.1. Monitoreo, medición, análisis y evaluación	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?		
9.2. Auditoría Interna	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?		
	¿Se ha definido el alcance y los requisitos para el informe de auditoría?		
9.3. Revisión por la Gerencia	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?		
10. MEJORA			
10.1. No conformidades y acción correctiva	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?		
10.2. Mejora Continua	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?		

VIII.3. Anexo N° 03: Guías de entrevista basado en el cumplimiento de controles del anexo A de la NTP-ISO/IEC 27001:2014

Guía de Evaluación de los controles del anexo A de la NTP-ISO/IEC 27001:2014			
Objetivo: Obtener la información necesaria sobre la aplicación de los controles referidos en el Anexo A de la NTP-ISO/IEC 27001:2014 para la implementación del Sistema de Gestión de Seguridad de Información en el Servicio de Administración Tributaria de la Zona Norte del Perú; con la finalidad de determinar el nivel de cumplimiento de los mismos.			
Fecha:			
Nombre:			
Anexo A NTP-ISO/IEC 27001:2014	**Descripción**	**Si**	**No**
A.5. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN			
A.5.1. Dirección de la Gerencia para la Seguridad de la Información			
A.5.1.1. Políticas para la seguridad de información	¿La administración ha publicado y aprobado las políticas sobre la Seguridad de la Información?		
A.5.1.2. Revisión de las políticas para la seguridad de la información	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?		
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN			
A.6.1. Organización Interna			
A.6.1.1. Roles y Responsabilidades para la seguridad de la información	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?		
A.6.1.2. Segregación de Funciones	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?		
A.6.1.3. Contacto con autoridades	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?		
A.6.1.4. Contacto con grupos especiales de interés	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?		
A.6.1.5. Seguridad de la información en la gestión de proyectos	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la administración?		
A.6.2. Dispositivos Móviles y teletrabajo			
A.6.2.1. Política de dispositivos móviles.	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?		
A.6.2.2. Teletrabajo	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?		
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS			
A.7.1. Antes del Empleo			
A.7.1.1. Selección	¿Se investigan los antecedentes de los candidatos?		
A.7.1.2. Términos y condiciones del empleo	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?		
A.7.2. Durante el Empleo			
A.7.2.1. Responsabilidades de la Gerencia	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?		
A.7.2.2. Conciencia, educación y capacitación sobre la seguridad de la información	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?		
A.7.2.3. Proceso disciplinario	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?		

A.7.3. Terminación y cambio de empleo			
A.7.3.1. Terminación o cambio de responsabilidades del empleo	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?		
A.8. GESTIÓN DE ACTIVOS			
A.8.1. Responsabilidad de los Activos			
A.8.1.1. Inventario de Activos	¿Se ha realizado un inventarios de activos que dan soporte al negocio y de Información?		
A.8.1.2. Propiedad de los Activos	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?		
A.8.1.3. Uso aceptable de los activos	¿Se han establecido normas para el uso de activos en relación a su seguridad?		
A.8.1.4. Retorno de Activos	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?		
A.8.2. Clasificación de la Información			
A.8.2.1. Clasificación de la Información	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?		
A.8.2.2. Etiquetado de la Información	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?		
A.8.2.3. Manejo de Activos	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?		
A.8.3. Manejo de los Medios			
A.8.3.1. Gestión de Medios Removibles	¿Existen controles establecidos para aplicar a soportes extraíbles?		
A.8.3.2. Disposición de Medios	¿Existen procedimientos establecidos para la eliminación de soportes?		
A.8.3.3. Transferencia de los medios	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad?		
A.9. CONTROL DE ACCESOS			
A.9.1. Requisitos de la Empresa para el Control de Accesos			
A.9.1.1. Política de Control de Accesos	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?		
A.9.1.2. Accesos a redes y Servicios de red	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?		
A.9.2. Gestión de Accesos de usuario			
A.9.2.1. Registro y baja de usuarios	¿Existen procesos formales de registros de usuarios?		
A.9.2.2. Aprovisionamiento de acceso de usuario	¿Existen procesos formales para asignación de perfiles de acceso?		
A.9.2.3. Gestión de derechos de acceso privilegiado	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?		
A.9.2.4. Gestión de información de autenticación secreta de usuario	¿Se ha establecido una política específica para el manejo de información clasificada como secreta?		
A.9.2.5. Revisión de derechos de acceso de usuario	¿Se establecen periodos concretos para renovación de permisos de acceso?		

A.9.2.6. Remoción o ajustes de derechos de acceso	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?		
A.9.3. Responsabilidad de los Usuarios			
A.9.3.1. Uso de Información de autenticación secreta	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?		
A.9.4. Control de Acceso a Sistema y aplicación			
A.9.4.1. Restricción de acceso a la información	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?		
A.9.4.2. Procedimientos de acceso seguro	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?		
A.9.4.3. Sistema de Gestión de contraseñas	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?		
A.9.4.4. Uso de programas utilitarios privilegiados	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?		
A.9.4.5. Control de acceso al código fuente de los programas	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?		
A.10. CRIPTOGRAFÍA			
A.10. Controles Criptográficos			
A.10.1.1. Política sobre el uso de controles criptográficos	¿Existe una política para el establecimiento de controles criptográficos?		
A.10.1.2. Gestión de claves	¿Existe un control del ciclo de vida de las claves criptográficas?		
A.11. SEGURIDAD FÍSICA Y DEL AMBIENTE			
A.11.1. Áreas Seguras			
A.11.1.1. Perímetro de Seguridad física	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?		
A.11.1.2. Controles de acceso físico	¿Existen controles de acceso a personas autorizadas en áreas restringidas?		
A.11.1.3. Asegurar oficinas, áreas e instalaciones	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?		
A.11.1.4. Protección contra amenazas externas y ambientales	¿Se establecen medidas de protección contra amenazas externas y ambientales?		
A.11.1.5. Trabajo en áreas seguras	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?		
A.11.2. Equipos			
A.11.2.1. Emplazamiento y protección de equipos	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?		
A.11.2.2. Servicio de suministro	¿Se protegen los equipos contra fallos de suministro de energía?		
A.11.2.3. Seguridad en el cableado	¿Existen protecciones para los cableados de energía y de datos?		
A.11.2.4. Mantenimiento de equipos	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?		

A.11.2.5. Remoción de activos	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. que puedan contener información?		
A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?		
A.11.2.7. Disposición o reutilización segura de equipos	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?		
A.11.2.8. Equipos de usuarios desatendidos	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?		
A.11.2.9. Política de escritorio limpio y pantalla limpia	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?		
A.12. SEGURIDAD DE LAS OPERACIONES			
A.12.1. Procedimientos y responsabilidades operativas			
A.12.1.1. Procedimientos operativos documentados	¿Se documentan los procedimientos y se establecen responsabilidades?		
A.12.1.2. Gestión de cambio	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?		
A.12.1.3. Gestión de la capacidad	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?		
A.12.1.4. Separación de los entornos de desarrollo, pruebas y operaciones	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?		
A.12.2. Controles contra código malicioso			
A.12.2.1. Controles contra código malicioso	¿Existen sistemas de detección para Software malicioso o malware?		
A.12.3. Respaldo			
A.12.3.1. Respaldo de la información	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?		
A.12.4. Registro y monitoreo			
A.12.4.1. Registro de eventos	¿Se realiza un registro de eventos?		
A.12.4.2. Protección de información de registro	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?		
A.12.4.3 Registro del administrador y del operador	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?		
A.12.4.4. Sincronización de reloj	¿Existe un control de sincronización de los distintos sistemas?		
A.12.5. Control de Software en la Producción			
A.12.5.1. Instalaciones de Software en sistemas operacionales	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?		
A.12.6. Gestión de vulnerabilidad técnica			
A.12.6.1. Gestión de Vulnerabilidades técnicas	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?		
A.12.6.2. Restricciones de instalación de software	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?		
A.12.7. Consideraciones para la auditoria de los sistemas de información			
A.12.7.1. Controles de auditoría de información	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?		

A.13. SEGURIDAD DE LAS COMUNICACIONES			
A.13.1. Gestión de la Seguridad de la Red			
A.13.1.1. Controles de la red	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?		
A.13.1.2. Seguridad de los servicios de red	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?		
A.13.1.3. Segregación en redes	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?		
A.13.2. Transferencia de información			
A.13.2.1. Políticas o procedimientos para la transferencia de información	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?		
A.13.2.2. Acuerdos de transferencia de información	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?		
A.13.2.3. Mensajes Electrónicos	¿Se establecen normas o criterios de seguridad en mensajería electrónica?		
A.13.2.4. Acuerdos de confidencialidad o no divulgación	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades?		
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS			
A.14.1. Requisitos de Seguridad en los Sistemas de Información			
A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?		
A.14.1.2. Aseguramiento de servicios de aplicaciones sobre redes públicas	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?		
A.14.2. Seguridad en los procesos de desarrollo y soporte			
A.14.2.1. Política de desarrollo seguro	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?		
A.14.2.2. Procedimientos de control de cambios del sistema	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?		
A.14.2.3. Revisión Técnica de aplicaciones después de cambios a la plataforma operativa	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?		
A.14.2.4. Restricciones sobre cambios a los paquetes de software	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?		
A.14.2.5. Principios de ingeniería de sistemas seguros	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?		
A.14.2.6. Ambiente de desarrollo seguro	¿Se cuenta con un entorno de desarrollo aislado de los analistas?		
A.14.2.7. Desarrollo de contratado externamente	¿Se realizan desarrollo de software por parte de terceros?		
A.14.2.8. Pruebas de Seguridad del sistema	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?		
A.14.2.9. Pruebas de aceptación del sistema	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?		
A.14.3. Datos de Prueba			

A.14.3.1. Protección de datos de prueba	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?		
A.15. RELACIONES CON LOS PROVEEDORES			
A.15.1. Seguridad de la Información en las relaciones con los proveedores			
A.15.1.1. Política de seguridad de la información para las relaciones con los proveedores	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?		
A.15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?		
A.16. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN			
A.16.1. Gestión de incidentes de la Seguridad de la Información y mejoras			
A.16.1.1. Responsabilidades y procedimientos	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?		
A.16.1.2. Reporte de eventos de seguridad de la información	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?		
A.16.1.3. Reporte de debilidades de seguridad de la información	¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?		
A.16.1.4. Evaluación y decisión sobre eventos de seguridad de la información	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?		
A.16.1.5. Respuesta de incidentes de seguridad de la información	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?		
A.16.1.6. Aprendizaje de los incidentes de la seguridad de información	¿La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?		
A.16.1.7. Recolección de evidencias	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?		
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
A.1.7.1. Continuidad de Seguridad de la información			
A.17.1.1. Planificación de continuidad de seguridad de la información	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?		
A.17.1.2. Implementación de continuidad de seguridad de la información	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?		
A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?		
A.17.2. Redundancias			
A.17.2.1. Instalaciones de procesamiento de la información	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?		
A.18. CUMPLIMIENTO			
A.18.1. Cumplimiento con los Requisitos Legales y Contractuales			

A.18.1.1. Identificación de los requisitos contractuales y legislación aplicables	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento?		
A.18.1.2. Derechos de propiedad intelectual	¿Existen procedimientos implementados sobre la propiedad intelectual?		
A.18.1.3. Protección de Registros	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?		
A.18.1.4. Privacidad y protección de datos personales	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?		
A.18.1.5. Regulación de controles criptográficos	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?		
A.18.2.1. Revisión independiente de la Seguridad de la Información	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?		
A.18.2. Revisiones de seguridad de la información			
A.18.2.2. Cumplimiento de políticas y normas de seguridad	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?		
A.18.2.3. Revisión de Cumplimiento Técnico.	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?		

VIII.4. Anexo N° 04: Guía para la Revisión Documentaria

Guía para la Revisión Documentaria del Servicio de Administración Tributaria de la Zona Norte del Perú				
Objetivo: Verificar que la documentación requerida para la implementación del SGSI se encuentra documentada y actualizada.				
Fecha:				
Documento	**Se encuentra**		**Estado**	**Observación**
	Si	**No**		
Políticas y Objetivos de seguridad de Información				
Alcance del SGSI				
Documento de Evaluación de Riesgos				
Declaración de Aplicabilidad				
Plan de Tratamiento de Riesgos				
Informe sobre evaluación y tratamiento de riesgos				
Definición de funciones y responsabilidades de seguridad				
Inventario de Activos				
Política de control de Acceso				
Procedimientos operativos para la gestión de TI				
Procedimiento para la gestión de incidentes				
Procedimientos para la continuidad de negocios				
Plan de Continuidad de negocio				
Registro de capacitaciones de seguridad de información				
Resultado de la supervisión y medición del SGSI				
Plan de auditoria interna				
Resultado de acciones correctivas				
Registro sobre actividades de los usuarios, excepciones y registro de eventos				
Plan de Mantenimiento de equipos				

VIII.5. Anexo N° 05: Medición Nivel de Madurez de los requisitos de cumplimiento de la norma técnica peruana NTP-ISO/IEC 27001:2014

Criterio NTP-ISO/IEC 27001:2014	Descripción	Hallazgos	Evidencia	Nivel de Madurez
4. CONTEXTO DE LA ORGANIZACIÓN				
4.1. Comprender la Organización y su Contexto	¿Están identificados los objetivos del SGSI?	No existe	No se cuenta con el SGSI por lo tanto no se han identificados cuales son los objetivos.	0
	¿Se han identificado las cuestiones internas y externas relacionadas con la Seguridad de la Información?	Requisito Cumplido	Se han identificados cuales son las situaciones internas y externas que afectan el cumplimiento de la seguridad de la información.	1
	¿Se han identificado como las partes internas y externas pueden suponer amenazas o riesgos para la seguridad de la Información?	No existe	A pesar de haber identificado las situaciones internas y externas, no se ha realizado el análisis de riesgos a los que se encuentra expuesta la administración	0
4.2. Comprender las necesidades y expectativas de las partes interesadas	¿Se han identificado las partes interesadas?	Requisito Cumplido	Mediante Resolución Gerencial N° 260-2018 se determinó la conformación del comité de Seguridad de la Información en la administración.	2
4.3. Determinar el alcance del Sistema de Gestión de Seguridad de Información	¿Se ha determinado el alcance del SGSI y se conserva información documentada?	No existe	No se ha determinado el alcance del SGSI.	0
4.4. Sistema de Gestión de Seguridad de Información	¿El SGSI está establecido, implementado y se revisa de forma planificada considerando oportunidades de mejora?	No existe	La administración no cuenta con un SGSI documentado y aprobado.	0
5. LIDERAZGO				
5.1. Liderazgo y Compromiso	¿Se han establecido objetivos de la Seguridad de la Información acordes con los objetivos del negocio?	No existe	No se ha establecido los objetivos de la seguridad de la información acorde a los objetivos estratégicos de la administración.	0
	¿La dirección provee de los recursos materiales y humanos necesarios para el cumplimiento de los objetivos del SGSI?	Requisito Cumplido	Mediante Resolución Gerencial se determinó la conformación del comité de Seguridad de la Información en la administración.	1
	¿La dirección revisa directamente la eficacia del SGSI para garantizar que se cumplen los objetivos del SGSI?	No existe	La administración no cuenta con un SGSI documentado y aprobado.	0
5.2. Política	¿Se ha definido una Política de la Seguridad de la Información?	Requisito Cumplido	La administración cuenta con políticas documentadas, sin embargo estas se encuentran desfasadas.	1

	¿Se ha comunicado la política de la Seguridad de la información a toda la administración?	Requisito Cumplido	Las políticas con las que cuenta la administración se encuentran a disposición de los colaboradores.	2
5.3. Roles, responsabilidades y autoridades organizacionales	¿Se han asignado las responsabilidades y autoridades sobre la Seguridad de la Información?	Requisito Cumplido	Mediante Resolución Gerencial se determinó la conformación del comité de Seguridad de Información en la administración	2
6. PLANIFICACIÓN				
6.1. Acciones para tratar los riesgos y las oportunidades	¿El plan para abordar riesgos y oportunidades considera las expectativas de las partes interesadas en relación a la Seguridad de la Información?	No existe	La administración no cuenta con un plan para gestionar los riesgos a los que se encuentra expuestos la administración.	0
	¿Se identifican y analizan los riesgos mediante un método de evaluación y aceptación de riesgos?	No existe	No se han identificado cuales son los riesgos a los que se encuentran expuestos la administración.	0
	¿Se ha definido un proceso de tratamiento de riesgos?	No existe	No se ha definido un proceso para el tratamiento de los riesgos.	0
6.2. Objetivos de seguridad de la información y planificación para conseguirlos	¿Se han integrado los objetivos de la Seguridad de la Información en los procesos de la organización teniendo en cuenta las funciones principales dentro de la Organización?	No existe	No se han identificado cuales son los objetivos de seguridad de la información dentro de la administración.	0
7. SOPORTE				
7.1. Recursos	¿Se identifican y asignan los recursos necesarios para el SGSI?	Requisito Cumplido	El comité de Seguridad de Información en la administración se encuentra conformado.	3
7.2. Competencias	¿Se evalúa la competencia en materias de Seguridad de la Información para personas que efectúan tareas que puedan afectar a la seguridad?	Requisito Cumplido	La administración cuenta con personal de OTIC, cuyos conocimientos lograrían llevar a cabo el cumplimiento del SGSI.	3
	¿Se mantiene información actualizada sobre la competencia del personal?	Requisito Cumplido	Constantemente se mantiene actualizado el legajo del personal dentro de la administración.	3
7.3. Concientización	¿El personal está involucrado y es consciente de su papel en la Seguridad de la Información?	Requisito Cumplido	El comité de seguridad de la información se encuentra involucrado en temas relacionados con seguridad de la información.	1
	¿Existe conciencia de los daños que se pueden producir de no seguir las pautas de la Seguridad de la Información?	No existe	Los colaboradores no conocen sobre las cláusulas que indican el manejo de información confidencial	0
7.4. Comunicación	¿Se comunica la política de la Seguridad de la Información con las responsabilidades de cada uno?	Requisito Cumplido	Las políticas con las que cuenta la administración se encuentran a disposición de los colaboradores.	2

	¿Existe un proceso para comunicar las deficiencias o malas prácticas en la seguridad de la Información?	No existe	No se ha definido un proceso para comunicar las deficiencias con respecto a la seguridad de la información.	0
7.5. información Documentada	¿Se dispone de la documentación requerida por la norma más la requerida por la Norma ISO 27001 incluyendo registros?	No existe	La administración no cuenta con la documentación requerida para el desarrollo del SGSI.	0
8. OPERACIÓN				
8.1. Planificación y Control operacional	¿Se han definido actividades basadas en un sistema de mejora continua que permita cumplir los objetivos, políticas y requisitos de la seguridad de la información?	No existe	No se han definido un sistema de mejora continua para el cumplimiento de los requisitos de la seguridad de la información.	0
8.2. Evaluación de riesgos de seguridad de información	¿Realiza la administración la evaluación de riesgos de manera periódica?	No existe	La administración no realiza la evaluación de los riesgos a los cuales se encuentra expuesto.	0
8.3. Tratamiento de riesgos de seguridad de información	¿La administración cuenta con un plan de tratamiento de riesgos de seguridad de información?	No existe	La administración no cuenta con un plan de tratamientos de los riesgos de seguridad de la información.	0
9. EVALUACIÓN DEL DESEMPEÑO				
9.1. Monitoreo, medición, análisis y evaluación	¿Se ha establecido un proceso continuo de monitoreo de los aspectos clave de la seguridad de la información teniendo en cuenta los controles para la seguridad de la información?	No existe	No se ha establecido un proceso de medición para el SGSI.	0
9.2. Auditoría Interna	¿Se ha establecido una programación de Auditorías Internas y asignado responsables?	No existe	No se ha establecido un programa de auditorías internas.	0
	¿Se ha definido el alcance y los requisitos para el informe de auditoría?	No existe	No se ha determinado el alcance y requisitos para los informes de auditoría.	0
9.3. Revisión por la Gerencia	¿Existe una programación para los informes de la dirección y existe constancia de su realización periódica?	No existe	No se ha determinado la programación para llevar a cabo la medición del desempeño del SGSI.	0
10. MEJORA				
10.1. No conformidades y acción correctiva	¿Existe un procedimiento documentado para identificar y registrar las no conformidades y su tratamiento?	Requisito Cumplido	Se ha determinado el procedimiento para identificar y registrar el incumplimiento a los requisitos de la norma; sin embargo no se encuentran actualizados.	3
10.2. Mejora Continua	¿Existe un proceso para garantizar la mejora continua del SGSI identificando las oportunidades de mejora?	No Existe	No se ha determinado un proceso para garantizar la mejora continua del SGSI	0

VIII.6. Anexo N° 06: Medición Nivel de Madurez Anexo A de la norma técnica peruana NTP-ISO/IEC 27001:2014

Anexo A NTP-ISO/IEC 27001:2014	Descripción	Hallazgos	Comentarios	Nivel de Madurez
A.5. POLÍTICAS DE SEGURIDAD DE INFORMACIÓN				
A.5.1. Dirección de la Gerencia para la Seguridad de la Información				
A.5.1.1. Políticas para la seguridad de información	¿La administración ha publicado y aprobado las políticas sobre la Seguridad de la Información?	Control Implementado	La administración cuenta con políticas documentadas, sin embargo estas se encuentran desfasadas.	2
A.5.1.2. Revisión de las políticas para la seguridad de la información	¿Existe un proceso planificado y verificable de revisión de las políticas de Seguridad de la información?	Control Implementado	La oficina de Planificación es la encargada de la revisión y publicación de las políticas de la institución	2
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE INFORMACIÓN				
A.6.1. Organización Interna				
A.6.1.1. Roles y Responsabilidades para la seguridad de la información	¿Se han asignado y definido las responsabilidades sobre la seguridad de la Información en las distintas tareas o actividades de la organización?	Control Implementado	Mediante Resolución Gerencial se determinó la conformación del comité de Seguridad de la Información en la administración.	2
A.6.1.2. Segregación de Funciones	¿Se han segregado las diversas áreas de responsabilidad sobre la Seguridad de la Información para evitar usos o accesos indebidos?	No existe	No se evidencia la segregación de funciones para el comité de Seguridad de la información	0
A.6.1.3. Contacto con autoridades	¿Existe un proceso definido para contactar con las autoridades competentes ante incidentes relacionados con la Seguridad de la Información?	No existe	No se evidencia la existencia de un proceso definido.	0
A.6.1.4. Contacto con grupos especiales de interés	¿Existen medios y se han establecido contactos con grupos de interés y asociaciones relacionadas con la seguridad de la información para mantenerse actualizado en noticias e información sobre Seguridad?	No existe	No se evidencia la existencia de comunicaciones con grupos de interés con respecto a temas relacionados con seguridad de la información	0
A.6.1.5. Seguridad de la información en la gestión de proyectos	¿Existen requisitos para afrontar cuestiones sobre la seguridad de la información en la gestión de proyectos de la administración?	No existe	Se evidencia que no existen controles que incluyan temas de seguridad de la información en la gestión de proyectos.	0
A.6.2. Dispositivos Móviles y teletrabajo				
A.6.2.1. Política de dispositivos móviles.	¿Se consideran requisitos especiales para la Seguridad de la Información en la utilización de dispositivos móviles?	No existe	La institución no asigna dispositivos móviles para la ejecución de funciones	0
A.6.2.2. Teletrabajo	¿Se aplican los criterios de Seguridad para los accesos de teletrabajo?	Control Implementado	Se han identificado medidas que evitan accesos no autorizados mediante la conexión remota.	1
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS				

A.7.1. Antes del Empleo				
A.7.1.1. Selección	¿Se investigan los antecedentes de los candidatos?	Control Implementado	Se realiza la revisión de la documentación presentada por los colaboradores durante el proceso de selección.	3
A.7.1.2. Términos y condiciones del empleo	¿Se incluyen cláusulas relativas a la Seguridad de la Información en los contratos de trabajo?	Control Implementado	Existen clausulas sobre seguridad de la información en los contratos	3
A.7.2. Durante el Empleo				
A.7.2.1. Responsabilidades de la Gerencia	¿El cumplimiento de las responsabilidades sobre la Seguridad de la Información es exigida de forma activa a empleados y contratistas?	No existe	No existe un procedimiento de formación continua para mantener las habilidades en el desarrollo de las acciones antes y durante al acceso a los activos de información.	0
A.7.2.2. Conciencia, educación y capacitación sobre la seguridad de la información	¿Existen procesos de información, formación y sensibilización sobre las responsabilidades sobre la Seguridad de la Información?	Control Implementado	El reglamento interno de trabajo regula los temas relacionados a la confidencialidad de información por parte de los colaboradores.	2
A.7.2.3. Proceso disciplinario	¿Existe un plan disciplinario donde se comunica a los empleados y contratistas las consecuencias de los incumplimientos sobre las políticas de la Seguridad de la Información?	Control Implementado	El reglamento interno de trabajo indica las sanciones disciplinarias para los colaboradores que infrinjan la confidencialidad de la información.	2
A.7.3. Terminación y cambio de empleo				
A.7.3.1. Terminación o cambio de responsabilidades del empleo	¿Existe un procedimiento para garantizar la Seguridad de la Información en los cambios de empleo, puesto de trabajo o al finalizar un contrato?	No existe	No se han definido procedimientos que garanticen la seguridad de la información al término de vínculo laboral.	2
A.8. GESTIÓN DE ACTIVOS				
A.8.1. Responsabilidad de los Activos				
A.8.1.1. Inventario de Activos	¿Se ha realizado un inventarios de activos que dan soporte al negocio y de Información?	Control Implementado	La administración cuenta con inventario de activos, pero dicho inventario no está estandarizado además de no contar con las actualizaciones pertinentes.	1
A.8.1.2. Propiedad de los Activos	¿Se ha identificado al responsable de cada activo en cuanto a su seguridad?	Control Implementado	El responsable de cada oficina es el responsable del activo informático que se encuentra dentro de su ámbito laboral.	1
A.8.1.3. Uso aceptable de los activos	¿Se han establecido normas para el uso de activos en relación a su seguridad?	Control Implementado	La administración cuenta con la documentación necesaria para el uso aceptable de los activos.	1
A.8.1.4. Retorno de Activos	¿Existe un procedimiento para la devolución de activos cedidos a terceras partes o a la finalización de un puesto de trabajo o contrato?	Control Implementado	Se ha definido un procedimiento, sin embargo no se encuentra documentado.	1
A.8.2. Clasificación de la Información				

A.8.2.1. Clasificación de la Información	¿Se clasifica la información según su confidencialidad o su importancia en orden a establecer medidas de seguridad especificas?	No existe	La administración no cuenta con la clasificación de los activos, la documentos son almacenados sin contar con los rótulos respectivos	0
A.8.2.2. Etiquetado de la Información	¿Los activos de información son fácilmente identificables en cuanto a su grado de confidencialidad o su nivel de clasificación?	No existe	La administración no cuenta con un control de etiquetado de información.	0
A.8.2.3. Manejo de Activos	¿Existen procedimientos para el manipulado de la información de acuerdo a su clasificación?	No existe	La administración no cuenta con procedimientos de manipulación de la información	0
A.8.3. Manejo de los Medios				
A.8.3.1. Gestión de Medios Removibles	¿Existen controles establecidos para aplicar a soportes extraíbles?	Control Implementado	La administración cuenta con el control de medios removibles, sin embargo, no ha sido documentado.	1
A.8.3.2. Disposición de Medios	¿Existen procedimientos establecidos para la eliminación de soportes?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.8.3.3. Transferencia de los medios	¿Existen procedimientos para el traslado de soportes de información para proteger su seguridad?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.9. CONTROL DE ACCESOS				
A.9.1. Requisitos de la Empresa para el Control de Accesos				
A.9.1.1. Política de Control de Accesos	¿Existe una política para definir los controles de acceso a la información que tengan en cuenta el acceso selectivo a la información según las necesidades de cada actividad o puesto de trabajo?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.9.1.2. Accesos a redes y Servicios de red	¿Se establecen accesos limitados a los recursos y necesidades de red según perfiles determinados?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.9.2. Gestión de Accesos de usuario				
A.9.2.1. Registro y baja de usuarios	¿Existen procesos formales de registros de usuarios?	Control Implementado	La administración cuenta con el control de procesos formales para el registro y baja de usuarios.	2
A.9.2.2. Aprovisionamiento de acceso de usuario	¿Existen procesos formales para asignación de perfiles de acceso?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.9.2.3. Gestión de derechos de acceso privilegiado	¿Se define un proceso específico para la asignación y autorización de permisos especiales de administración de accesos?	Control Implementado	El control de accesos es definido por el perfil del puesto del colaborador	1
A.9.2.4. Gestión de información de autenticación secreta de usuario	¿Se ha establecido una política específica para el manejo de información clasificada como secreta?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1

A.9.2.5. Revisión de derechos de acceso de usuario	¿Se establecen periodos concretos para renovación de permisos de acceso?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.9.2.6. Remoción o ajustes de derechos de acceso	¿Existen un proceso definido para la revocación de permisos cuando se finalice una actividad, puesto de trabajo o cese de contratos?	Control Implementado	La administración cuenta con el control, sin embargo, no ha sido documentado.	1
A.9.3. Responsabilidad de los Usuarios				
A.9.3.1. Uso de Información de autenticación secreta	¿Se establecen normas para la creación y salvaguarda de contraseñas de acceso?	Control Implementado	Existe el control pero no se encuentra documentado, sin embargo, se detectó que las contraseñas son compartidas por los colaboradores.	1
A.9.4. Control de Acceso a Sistema y aplicación				
A.9.4.1. Restricción de acceso a la información	¿Se establecen niveles y perfiles específicos de acceso para los sistemas de Información de forma que se restringa la información a la actividad específica a desarrollar?	Control Implementado	El control se encuentra implementado, sin embargo, no se ha documentado.	1
A.9.4.2. Procedimientos de acceso seguro	¿Se han implementado procesos de acceso seguro para el inicio de sesión considerando limitaciones de intentos de acceso, controlando la información en pantalla etc.?	Control Implementado	El control se encuentra implementado mediante los roles de acceso a los sistemas de información.	1
A.9.4.3. Sistema de Gestión de contraseñas	¿Se establecen medidas para controlar el establecimiento de contraseñas seguras?	Control Implementado	El control se encuentra implementado mediante el procedimiento de cambio de contraseñas.	1
A.9.4.4. Uso de programas utilitarios privilegiados	¿Se controla la capacitación y perfil de las personas que tienen permisos de administración con perfiles bajos de Seguridad?	Control Implementado	El control se encuentra implementado mediante los roles de acceso a los sistemas de información.	1
A.9.4.5. Control de acceso al código fuente de los programas	¿Se restringe el acceso a códigos fuente de programas y se controla cualquier tipo de cambio a realizar?	Control Implementado	El control se encuentra implementado mediante la gestión de cambios de los sistemas de información.	1
A.10. CRIPTOGRAFÍA				
A.10. Controles Criptográficos				
A.10.1.1. Política sobre el uso de controles criptográficos	¿Existe una política para el establecimiento de controles criptográficos?	Control Implementado	La administración cuenta con la política sobre el uso de controles criptográficos.	2
A.10.1.2. Gestión de claves	¿Existe un control del ciclo de vida de las claves criptográficas?	Control Implementado	La administración cuenta con el procedimiento para la gestión de claves criptográficas	2
A.11. SEGURIDAD FÍSICA Y DEL AMBIENTE				
A.11.1. Áreas Seguras				
A.11.1.1. Perímetro de Seguridad física	¿Se establecen perímetros de seguridad física donde sea necesario con barreras de acceso?	Control Implementado	El área e tratamiento de información cuenta con las medidas de control establecidas, puertas con entrada por	2

			recepción.	
A.11.1.2. Controles de acceso físico	¿Existen controles de acceso a personas autorizadas en áreas restringidas?	Control Implementado	La administración cuenta con el control de acceso a áreas restringidas, sin embargo, se pudo evidenciar que los colaboradores ingresan constantemente al área de tratamiento de información	2
A.11.1.3. Asegurar oficinas, áreas e instalaciones	¿Se establecen medidas de seguridad para zonas de oficinas para proteger la información de pantallas etc. en áreas de accesibles a personal externo?	No existe	La administración cuenta con el control de aseguramiento de oficinas	0
A.11.1.4. Protección contra amenazas externas y ambientales	¿Se establecen medidas de protección contra amenazas externas y ambientales?	No existe	La administración no cuenta con un Plan de Recuperación ante desastres.	0
A.11.1.5. Trabajo en áreas seguras	¿Se controla o supervisa la actividad de personal que accede a áreas seguras?	No existe	La administración no cuenta con un control de supervisión a los colaboradores o visitantes.	0
A.11.2. Equipos				
A.11.2.1. Emplazamiento y protección de equipos	¿Se protegen los equipos tanto del medioambiente como de accesos no autorizados?	Control Implementado	La administración cuenta con el control de protección de equipos.	1
A.11.2.2. Servicio de suministro	¿Se protegen los equipos contra fallos de suministro de energía?	Control Implementado	Los ups tienen un nivel de cobertura de 15 minutos, posterior a ello entra en funcionamiento el Grupo Electrógeno	3
A.11.2.3. Seguridad en el cableado	¿Existen protecciones para los cableados de energía y de datos?	Control Implementado	Se evidenció que los cables de red y energía cuentan con la protección adecuada, sin embargo existen oficinas en las que se encuentran expuestos.	1
A.11.2.4. Mantenimiento de equipos	¿Se planifican y realizan tareas de mantenimiento sobre los equipos?	Control Implementado	Se evidenció que se realiza mantenimiento preventivo durante el año, sin embargo la falta del plan de mantenimiento correctivo de equipos informáticos, ha ocasionado fallas en las unidades de almacenamiento de los servidores del centro de datos, ocasionando pérdidas económicas.	2
A.11.2.5. Remoción de activos	¿Se controlan y autorizan la salida de equipos, aplicaciones etc. que puedan contener información?	Control Implementado	La administración cuenta con el control de salida de equipos.	2
A.11.2.6. Seguridad de equipos y activos fuera de las instalaciones	¿Se consideran medidas de protección específicas para equipos que se utilicen fuera de las instalaciones de la propia empresa?	Control Implementado	La administración mantiene el registro de custodia de los equipos que se encuentran fuera de las instalaciones.	2

A.11.2.7. Disposición o reutilización segura de equipos	¿Se establecen protocolos para proteger o eliminar información de equipos que causan baja o van a ser reutilizados?	Control Implementado	Los equipos son formateados en las unidades de almacenamiento, toda vez que sea coordinado con cada responsable de oficina.	2
A.11.2.8. Equipos de usuarios desatendidos	¿Se establecen normas para proteger la información de equipos cuando los usuarios abandonan el puesto de trabajo?	Control Implementado	Los equipos se encuentran dentro del directorio activo y se cuentan con políticas de escritorio limpio.	2
A.11.2.9. Política de escritorio limpio y pantalla limpia	¿Se establecen reglas de comportamiento para abandonos momentáneos o temporales del puesto de trabajo?	Control Implementado	Los equipos se encuentran dentro del directorio activo y se cuentan con políticas de escritorio limpio.	2
A.12. SEGURIDAD DE LAS OPERACIONES				
A.12.1. Procedimientos y responsabilidades operativas				
A.12.1.1. Procedimientos operativos documentados	¿Se documentan los procedimientos y se establecen responsabilidades?	Control Implementado	Los procedimientos en los que están involucrados actividades de procesamiento de información se encuentran definidos y documentados, sin embargo estos no se encuentran actualizados.	1
A.12.1.2. Gestión de cambio	¿Se dispone de un procedimiento para evaluar el impacto en la seguridad de la información ante cambios en los procedimientos?	No existe	La administración no cuenta controles para la gestión de cambios.	0
A.12.1.3. Gestión de la capacidad	¿Se controla el uso de los recursos en cuanto al rendimiento y capacidad de los sistemas?	Control Implementado	Se realizan pruebas sobre rendimientos de sistemas, optimización de procedimientos a fin de evitar cuellos de botellas; sin embargo no se encuentran documentados.	1
A.12.1.4. Separación de los entornos de desarrollo, pruebas y operaciones	¿Los entornos de desarrollo y pruebas están convenientemente separados de los entornos de producción?	Control Implementado	La administración cuenta con entornos de desarrollo y pruebas por separados.	3
A.12.2. Controles contra código malicioso				
A.12.2.1. Controles contra código malicioso	¿Existen sistemas de detección para Software malicioso o malware?	Control Implementado	La administración cuenta con antivirus con licencias vencidas, motivo por el cual sufrieron un ataque por Ransomware.	1
A.12.3. Respaldo				
A.12.3.1. Respaldo de la información	¿Se ha establecido un sistema de copias de seguridad acordes con las necesidades de la información y de los sistemas?	Control Implementado	La administración cuenta con la actividad de realizar copias de seguridad de base de datos, sin embargo no se realizan la verificación de validez.	1
A.12.4. Registro y monitoreo				
A.12.4.1. Registro de eventos	¿Se realiza un registro de eventos?	No existe	La administración no cuenta con un registro de eventos para los cambios que se hagan manualmente a la base de datos.	0

A.12.4.2. Protección de información de registro	¿Se ha establecido un sistema de protección para los registros mediante segregación de tareas o copias de seguridad?	Control Implementado	Se ha establecido un sistema de protección para los registros.	3
A.12.4.3 Registro del administrador y del operador	¿Se protege convenientemente y de forma específica los accesos o los de los administradores?	No existe	La administración no cuenta con un registro de eventos para los cambios que se hagan manualmente a la base de datos.	0
A.12.4.4. Sincronización de reloj	¿Existe un control de sincronización de los distintos sistemas?	No existe	La administración no cuenta con un procedimiento para el registro de eventos.	0
A.12.5. Control de Software en la Producción				
A.12.5.1. Instalaciones de Software en sistemas operacionales	¿Las instalaciones de nuevas aplicaciones SW o modificaciones son verificadas en entornos de prueba y existen protocolos de seguridad para su instalación?	Control Implementado	La administración en la etapa de desarrollo de sistemas cuenta con un entorno de pruebas antes del pase a producción.	1
A.12.6. Gestión de vulnerabilidad técnica				
A.12.6.1. Gestión de Vulnerabilidades técnicas	¿Se establecen métodos de control para vulnerabilidades técnicas "hacking ético" etc.?	Control Implementado	No se han establecido métodos para identificar las posibles vulnerabilidades técnicas a las que podrían estar expuestas los activos de información.	1
A.12.6.2. Restricciones de instalación de software	¿Se establecen medidas restrictivas para la instalación de Software en cuanto a personal autorizado evitando las instalaciones por parte de usuarios finales?	No existe	No se han establecido medidas restrictivas para la instalación de software, un usuario con perfil de administrador en el AD puede realizar descarga e instalaciones de aplicativos.	0
A.12.7. Consideraciones para la auditoria de los sistemas de información				
A.12.7.1. Controles de auditoría de información	¿Existen mecanismos de auditorías de medidas de seguridad de los sistemas?	Control Implementado	Se realizan auditorías a nivel institucional, sin embargo no se ha tenido hasta el momento una auditoria a los sistemas de información	1
A.13. SEGURIDAD DE LAS COMUNICACIONES				
A.13.1. Gestión de la Seguridad de la Red				
A.13.1.1. Controles de la red	¿En el entorno de red se gestiona la protección de los sistemas mediante controles de red y de elementos conectados?	Control Implementado	Se han gestionado los elementos físicos que dan soporte a la red.	1
A.13.1.2. Seguridad de los servicios de red	¿Se establecen condiciones de seguridad en los servicios de red tanto propios como subcontratados?	No existe	No se han establecido los requisitos de disponibilidad de la red, así mismo no se ha realizado la evaluación de riesgos a los que se encuentra expuesta la red.	0
A.13.1.3. Segregación en redes	¿Existe separación o segregación de redes tomando en cuenta condiciones de seguridad y clasificación de activos?	Control Implementado	La administración implantó hace un mes la segregación de la red, como medida de prevención ante el ataque de Ransomware que se presentó.	1
A.13.2. Transferencia de información				

A.13.2.1. Políticas o procedimientos para la transferencia de información	¿Se establecen políticas y procedimientos para proteger la información en los intercambios?	Control Implementado	No se han establecido políticas y procedimientos que regulen la transferencia de información, sin embargo a nivel gerencial se tienen las pautas para realizar el envío de la misma	1
A.13.2.2. Acuerdos de transferencia de información	¿Se delimitan y establecen acuerdos de responsabilidad en intercambios de información con otras entidades?	Control Implementado	No se han establecido acuerdos para el intercambio de información, sin embargo a nivel gerencial se tienen las pautas para realizar el envío de la misma	1
A.13.2.3. Mensajes Electrónicos	¿Se establecen normas o criterios de seguridad en mensajería electrónica?	Control Implementado	No se han establecido criterios del envió de mensajería electrónica, sin embargo a nivel gerencial se tienen las pautas para realizar el envío de la misma	1
A.13.2.4. Acuerdos de confidencialidad o no divulgación	¿Se establecen acuerdos de confidencialidad antes de realizar intercambios de información con otras entidades?	Control Implementado	Se han establecido acuerdos de confidencialidad para el intercambio de información.	3
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS				
A.14.1. Requisitos de Seguridad en los Sistemas de Información				
A.14.1.1. Análisis y especificación de requisitos de seguridad de la información	¿Se definen y documentan los requisitos de Seguridad de la Información para los nuevos sistemas de Información?	Control Implementado	Los requisitos de sistemas no son documentados.	2
A.14.1.2. Aseguramiento de servicios de aplicaciones sobre redes públicas	¿Se consideran requisitos de seguridad específicos para accesos externos o de redes públicas a los sistemas de información?	Control Implementado	Se cuenta con la seguridad a nivel WAF (Firewall de aplicaciones web)	2
A.14.2. Seguridad en los procesos de desarrollo y soporte				
A.14.2.1. Política de desarrollo seguro	¿Se establecen procedimientos que garanticen el desarrollo seguro del Software?	Control Implementado	No existe una política documentada	2
A.14.2.2. Procedimientos de control de cambios del sistema	¿Se gestiona el control de cambios en relación al impacto que puedan tener en los sistemas?	Control Implementado	Se Mantiene un control de cambios de sistemas, mediante un repositorio.	2
A.14.2.3. Revisión Técnica de aplicaciones después de cambios a la plataforma operativa	¿Se establecen procedimientos de revisión después de efectuar cambios o actualizaciones?	Control Implementado	Se mantiene un procedimiento establecido para realizar pruebas del sistema antes del pase a producción	2

A.14.2.4. Restricciones sobre cambios a los paquetes de software	¿Se establecen procesos formales para cambios en versiones o nuevas funcionalidades para Software de terceros?	Control Implementado	se mantiene un control para las versiones generadas en los sistemas	2
A.14.2.5. Principios de ingeniería de sistemas seguros	¿Se definen políticas de Seguridad de la Información en procesos de ingeniería de Sistemas?	No existe	No existe documentación de procedimientos sobre la implementación de seguridad de la información en el proceso de desarrollo.	1
A.14.2.6. Ambiente de desarrollo seguro	¿Se cuenta con un entorno de desarrollo aislado de los analistas?	Control Implementado	La administración cuenta con un entorno de desarrollo de acceso restringido.	3
A.14.2.7. Desarrollo de contratado externamente	¿Se realizan desarrollo de software por parte de terceros?	No existe	No se realizan desarrollos de software por parte de terceros.	0
A.14.2.8. Pruebas de Seguridad del sistema	¿Se realizan pruebas funcionales de seguridad de los sistemas antes de su fase de producción?	Control Implementado	Se mantiene un procedimiento establecido para realizar pruebas funcionales en cuanto a seguridad de información antes del pase a producción.	2
A.14.2.9. Pruebas de aceptación del sistema	¿Se establecen protocolos y pruebas de aceptación de sistemas para nuevos sistemas y actualizaciones?	Control Implementado	Se mantiene un procedimiento establecido para realizar pruebas del sistema antes del pase a producción	2
A.14.3. Datos de Prueba				
A.14.3.1. Protección de datos de prueba	¿Se utilizan datos de prueba en los ensayos o pruebas de los sistemas?	Control Implementado	Se mantiene un entorno de pruebas con una base de datos copia del original cuyos datos pueden ser usados para las pruebas funcionales del sistema.	2
A.15. RELACIONES CON LOS PROVEEDORES				
A.15.1. Seguridad de la Información en las relaciones con los proveedores				
A.15.1.1. Política de seguridad de la información para las relaciones con los proveedores	¿Existe una política de Seguridad de la información para proveedores que acceden a activos de la información de la empresa?	Control Implementado	Existe un política de confidencialidad de información con el proveedor de servicios en la nube	2
A.15.1.2. Abordar la seguridad dentro de los acuerdos con proveedores	¿Se han establecido requisitos de seguridad de la información en contratos con terceros?	Control Implementado	Se han establecido los requisitos de seguridad de la información con el proveedor de servicios en la nube.	2
A.16. GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE INFORMACIÓN				
A.16.1. Gestión de incidentes de la Seguridad de la Información y mejoras				
A.16.1.1. Responsabilidades y procedimientos	¿Se definen responsabilidades y procedimientos para responder a los incidentes de la Seguridad de la Información?	No existe	No existen procedimientos que dirijan el proceso de gestión de incidentes de la seguridad de información.	0

A.16.1.2. Reporte de eventos de seguridad de la información	¿Se han implementado canales adecuados para la comunicación de incidentes en la seguridad de la Información?	Control Implementado	Se han establecido canales de comunicación para informar sobre algún incidente de seguridad de la información, comunicación de usuarios a OTIC y a su vez a gerencia.	1
A.16.1.3. Reporte de debilidades de seguridad de la información	¿Se promueve y se hayan establecidos canales para comunicar o identificar puntos débiles en la Seguridad de la Información?	No existe	No se ha definido un formato de reporte de debilidades de los sistemas en cuanto a seguridad de la información.	0
A.16.1.4. Evaluación y decisión sobre eventos de seguridad de la información	¿Se ha establecido un proceso para gestionar los incidentes en la Seguridad de la Información?	No existe	No se ha realizado la evaluación de riesgos en seguridad de la información dentro de la administración.	0
A.16.1.5. Respuesta de incidentes de seguridad de la información	¿Existen mecanismos para dar respuesta a los eventos de la Seguridad de la Información?	No existe	No se ha determinado un proceso para la resolución de incidentes de seguridad de la información.	0
A.16.1.6. Aprendizaje de los incidentes de la seguridad de información	¿La información que proporcionada por los eventos en la Seguridad de la información son tratados para tomar medidas preventivas?	No existe	No se ha establecido una base de conocimiento sobre los incidentes de seguridad de la información	0
A.16.1.7. Recolección de evidencias	¿Existe un proceso para recopilar evidencias sobre los incidentes en la seguridad de la Información?	Control Implementado	La evidencia ante un incidente de seguridad de la información queda al resguardo de OTIC.	1
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO				
A.1.7.1. Continuidad de Seguridad de la información				
A.17.1.1. Planificación de continuidad de seguridad de la información	¿Se ha elaborado un plan de continuidad del negocio ante incidentes de Seguridad de la Información?	No existe	La administración no cuenta con un Plan de Continuidad de negocio o Plan de contingencia frente a incidentes de seguridad de la información.	0
A.17.1.2. Implementación de continuidad de seguridad de la información	¿Se ha implementado las medidas de recuperación previstas en el plan de Continuidad del Negocio?	No existe	La administración no cuenta con un Plan de Continuidad de negocio o Plan de contingencia frente a incidentes de seguridad de la información.	0
A.17.1.3. Verificación, revisión y evaluación de continuidad de seguridad de la información	¿Se han verificado o probado las acciones previstas en el plan de Continuidad del Negocio?	No existe	La administración no cuenta con un Plan de Continuidad de negocio o Plan de contingencia frente a incidentes de seguridad de la información.	0
A.17.2. Redundancias				
A.17.2.1. Instalaciones de procesamiento de la información	¿Se ha evaluado la necesidad de redundar los activos críticos de la Información?	No existe	No se ha determinado que activos de información requieren ser redundados.	0

A.18. CUMPLIMIENTO				
A.18.1. Cumplimiento con los Requisitos Legales y Contractuales				
A.18.1.1. Identificación de los requisitos contractuales y legislación aplicables	¿Se han identificado las legislaciones aplicables sobre protección de datos personales y su cumplimiento?	Control Implementado	Si, el estado Peruano mediante Resolución Ministerial N°004-2016-PCM, modificada por la Resolución Ministerial Nº 166-2017-PCM, el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014.	3
A.18.1.2. Derechos de propiedad intelectual	¿Existen procedimientos implementados sobre la propiedad intelectual?	No existe	No se ha definido un procedimiento sobre la propiedad intelectual de los productos de software.	0
A.18.1.3. Protección de Registros	¿Se establecen criterios para clasificación de registros y medidas de protección según niveles?	No existe	No se han definido las políticas para la protección de información.	0
A.18.1.4. Privacidad y protección de datos personales	¿Se establecen medidas para la protección de datos personales de acuerdo con la legislación vigente?	Control Implementado	Si, el estado Peruano cuenta con una ley de protección de datos personales Ley N° 29733, la cual se rige la administración debido a tratamiento de información confidencial de contribuyentes.	3
A.18.1.5. Regulación de controles criptográficos	¿Si se utiliza el cifrado, se establecen controles criptográficos de acuerdo a la legislación?	Control Implementado	La administración cuenta con el procedimiento para la gestión de claves criptográficas	3
A.18.2.1. Revisión independiente de la Seguridad de la Información	¿Se revisan los controles de la Seguridad de la Información por personal independiente a los responsables de implementar los controles?	No existe	La administración no cuenta con un SGSI documentado e implementado	0
A.18.2. Revisiones de seguridad de la información				
A.18.2.2. Cumplimiento de políticas y normas de seguridad	¿Se revisa periódicamente el cumplimiento de las políticas y controles de la Seguridad de la información?	No existe	No se realiza el cumplimiento de las políticas y controles de seguridad de la información con las que cuenta la administración.	0
A.18.2.3. Revisión de Cumplimiento Técnico.	¿Se realizan evaluaciones sobre el correcto funcionamiento de las medidas técnicas de protección para la seguridad de la información?	No existe	No se realiza la evaluación si los sistemas de información se encuentran configurados de acuerdo a las políticas existentes en la administración.	0

VIII.7. Anexo N° 07: Política General del Sistema de Gestión de Seguridad de Información

Política General del Sistema de Gestión de Seguridad de Información

1. **Resumen:**

   En la presente política se describe de forma general los lineamientos de seguridad mediante los cuales se deben manejar en la institución, tratamiento de los activos de información, roles y responsabilidades de la seguridad de información y las posibles sanciones a las que están expuestos por incumplimiento de las políticas de seguridad.

2. **Objetivo:**

   Establecer los lineamientos para la gestión de la seguridad de información que permita proteger los activos de información de la institución y la tecnología utilizada para el procesamiento de la misma, frente a amenazas internas o externas, con el fin de asegurar la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

3. **Alcance**

   La siguiente política de seguridad de la información es aplicable a todos los colaboradores de la institución, este documento debe ser revisado y actualizado de manera periódica según se manifiesten cambios de infraestructura, nuevas tecnologías, nuevos servicios, entre otros.

   Compromiso Institucional:

   Es compromiso de las Gerencias y Jefaturas establecer de manera clara el apoyo de la dirección, funcionamiento y cumplimiento de las Políticas de Seguridad de Información.

   Límites:

   Las Políticas de Seguridad de Información, involucra a todos los sistemas y personas que tratan información de la institución. En general, se suele traducir en la implementación de políticas en la Oficina de Tecnología de Información, por ser uno de los principales responsables del tratamiento y conservación de la información.

4. **Generalidades**

   - La Institución, reconoce que la seguridad de la información es un compromiso esencial en todos los procesos y colaboradores; por ello es necesario implementar mecanismos que permitan proteger los activos de información con la finalidad de gestionar eficientemente la información asegurando la confidencialidad, disponibilidad e integridad.

- Los accesos y uso de información estarán alineadas a las normativas internas de la institución.
- Las políticas deben ser difundidas a todos los colaboradores de la institución.
- Se promoverá la cultura de seguridad de la información en todos los colaboradores de la institución.
- Los perfiles y roles de usuario deben ser autorizados.
- La información será clasificada según los siguientes niveles:

Tipo	Glosa	Descripción
C	Confidencial	Información de gran relevancia para la administración, se restringe el acceso a la misma.
R	Restringido	Accesible para determinados colaboradores según el desempeño de las funciones.
UI	Uso Interno	Accesible para todo los colaboradores de la administración.
P	Público	Información de dominio público como la publicada en la página web.

- Los puertos para medios de almacenamiento removibles serán desactivados en todos los equipos de cómputo de la institución.
- El inventario de activos debe tener un proceso periódico de actualización, según sea conveniente.
- La presente políticas y políticas específicas deben ser revisadas y actualizadas de manera periódica.

5. Responsabilidades

Las Políticas de Seguridad de Información son de aplicación para todo el personal de la institución.

6. Sanciones

La violación de un control o política de seguridad de información justifica la aplicación de las sanciones comprendidas en el reglamento interno de trabajo, las cuales serán aplicadas teniendo en consideración lo siguiente: gravedad de la falta, antecedentes del colaborador, reincidencia y circunstancias en las que se cometió la falta u omisión de las políticas.

7. Políticas Especificas

Las políticas específicas de seguridad de la información deben estar alineadas y soportadas bajo la política general del Sistema de Gestión de seguridad de Información, las cuales son las siguientes:

- Política para la asignación y baja de usuarios
- Política para el control de accesos
- Política para la seguridad entre comunicaciones.
- Política para la seguridad de información involucrando al colaborador

- Política para las seguridad física y ambiental
- Política para el desarrollo y mantenimiento de sistemas
- Política para la Administración de la continuidad de las actividades de la institución

VIII.8. Anexo N° 08: Roles y Responsabilidades para la Seguridad de la Información

Responsable de la Of de Tecnología de Información	
Responsabilidad: Velar por el correcto uso y administración de los recursos informáticos de la institución.	
Responsabilidades Generales	Responsabilidades con el SGSI
Coordinar y apoyar en las labores de auditoría y consultoría, administración de la información, diseño y desarrollo de software y mantenimiento e implementación de infraestructura tecnológica.	Generar el cronograma de mantenimiento de equipos informáticos.
	Realizar el inventario de activos informáticos.
	Participar en la elaboración de las capacitaciones del SGSI y velar por el cumplimiento.
Gestionar el diseño e implementación de proyectos correspondientes a la oficina de Tecnología de información.	Reportar e identificar las condiciones inseguras durante el desarrollo de las actividades.
Responsable por la disponibilidad, desempeño, crecimiento y operación del hardware, software, acceso a recursos tecnológicos.	Respetar y cumplir con los objetivos de la seguridad de información
	Implementar las mejoras del SGSI
	Cumplir con las medidas de seguridad de la información que se definan en los procedimientos.

Soporte	
Responsabilidad: Implementar procedimientos para mejorar la eficiencia de los servicios de red y el correcto funcionamiento de los equipos.	
Responsabilidades Generales	Responsabilidades con el SGSI
Realizar el mantenimiento preventivo de los equipos informáticos de la institución	Actualizar el inventario de los activos.
Solucionar los inconvenientes con el hardware.	Cumplir con el cronograma de mantenimiento de los equipos informáticos.
Instalar el software requerido.	Implementar acciones preventivas y correctivas.
Gestionar los accesos a la red y administrar las restricciones en base a la seguridad de información.	Respetar y cumplir con los objetivos de la seguridad de información
Instalar y mantener el antivirus en los equipos informáticos.	Cumplir con las medidas de seguridad de la información que se definan en los procedimientos.

Oficial de Seguridad de Información	
Responsabilidad: Verificar y coordinar el cumplimiento del SGSI.	
Responsabilidades Generales	Responsabilidades con el SGSI
Establecer los lineamientos referentes a la implementación del SGSI	Encaminar a la institución al cumplimiento de los requisitos de seguridad de información.
Reportar e identificar los riesgos e incidentes que se generen en las actividades desarrolladas en la institución.	Realizar el seguimiento y control del SGS, aplicando las acciones necesarias para el cumplimiento de los objetivos.
Elaborar informes mensuales sobre el cumplimiento de las acciones realizadas en ejercicios de sus funciones.	Emplear los procedimientos para el desarrollo de las actividades del SGSI adecuadamente.
Velar por el cumplimiento de los requisitos legales con respecto a la seguridad de información.	Cumplir con el plan de capacitación sobre temas relacionadas a seguridad de información.
	Cumplir con las medidas de seguridad de la información que se definan en los procedimientos.
Implementar las mejoras del SGSI	Respetar y cumplir con los objetivos de la seguridad de información

VIII.9. Anexo N° 09: Matriz de Riesgos o Matriz de probabilidad e impacto

Evaluación de Riesgos																																										
Identificación del riesgo				Análisis y valorización del riesgo																																						
				Impacto																																						
				Procesos de Negocio			Información							Hardware					Software									Red					Personal									Valorización de riesgo	Nivel de Riesgo
				A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29	A30	A31	A32	A33		
Riesgos	Amenaza	Tipo de Riesgo	Probabilidad de	5	5	5	5	5	4	3	5	4	3	5	3	2	2	3	3	3	3	3	2	2	2	2	3	3	2	2	2	2	1	1	1	1		
Pérdida de la información de la entidad	AM1	Seguridad de Información	4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM2		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM3		2	10	10	10	10	10	8	6	10	8	6	10	6	4	4	6	6	6	6	6	4	4	4	4	6	6	4	4	4	4	2	2	2	2	6	Moderado
	AM4		5	25	25	25	25	25	20	15	25	20	15	25	15	10	10	15	15	15	15	15	10	10	10	10	15	15	10	10	10	10	5	5	5	5	15	Extremo
	AM5		5	25	25	25	25	25	20	15	25	20	15	25	15	10	10	15	15	15	15	15	10	10	10	10	15	15	10	10	10	10	5	5	5	5	15	Extremo
	AM6		5	25	25	25	25	25	20	15	25	20	15	25	15	10	10	15	15	15	15	15	10	10	10	10	15	15	10	10	10	10	5	5	5	5	15	Extremo
	AM7		2	10	10	10	10	10	8	6	10	8	6	10	6	4	4	6	6	6	6	6	4	4	4	4	6	6	4	4	4	4	2	2	2	2	6	Moderado
	AM8		2	10	10	10	10	10	8	6	10	8	6	10	6	4	4	6	6	6	6	6	4	4	4	4	6	6	4	4	4	4	2	2	2	2	6	Moderado
Indisponibilidad de la información	AM9		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM10		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM11		5	25	25	25	25	25	20	15	25	20	15	25	15	10	10	15	15	15	15	15	10	10	10	10	15	15	10	10	10	10	5	5	5	5	15	Extremo
	AM12		5	25	25	25	25	25	20	15	25	20	15	25	15	10	10	15	15	15	15	15	10	10	10	10	15	15	10	10	10	10	5	5	5	5	15	Extremo
	AM13		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM14		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM15		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM16		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM17		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM18		2	10	10	10	10	10	8	6	10	8	6	10	6	4	4	6	6	6	6	6	4	4	4	4	6	6	4	4	4	4	2	2	2	2	6	Moderado
Fallas de seguridad por recurso humano	AM19		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM20		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM21		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto
	AM22		2	10	10	10	10	10	8	6	10	8	6	10	6	4	4	6	6	6	6	6	4	4	4	4	6	6	4	4	4	4	2	2	2	2	6	Moderado
	AM23		3	15	15	15	15	15	12	9	15	12	9	15	9	6	6	9	9	9	9	9	6	6	6	6	9	9	6	6	6	6	3	3	3	3	9	Alto
	AM24		3	15	15	15	15	15	12	9	15	12	9	15	9	6	6	9	9	9	9	9	6	6	6	6	9	9	6	6	6	6	3	3	3	3	9	Alto
	AM25		4	20	20	20	20	20	16	12	20	16	12	20	12	8	8	12	12	12	12	12	8	8	8	8	12	12	8	8	8	8	4	4	4	4	12	Alto

VIII.10. Anexo N° 10: Políticas específicas del SGSI

	POLÍTICA PARA LA ASIGNACIÓN Y BAJA DE USUARIOS		Nro. 01
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

- Estandarizar la asignación y baja de cuentas de usuario, mediante procedimientos de autorización y ejecución de las actividades.

ALCANCE

- Esta política abarca a todos los Sistemas informáticos que requieran la creación de cuentas de usuario.

POLÍTICA

1. **Asignación de Usuario**
   - El área usuaria juntamente con la Oficina de Talento Humano, deberán informar a la Oficina de Tecnología de Información los nuevos ingresos y los cargos que desempeñara cada uno, a fin de asignarles las respectivas cuentas de usuario según el perfil correspondiente.
   - El área usuaria juntamente con la Oficina de Talento Humano, deberán informar a la Oficina de Tecnología de Información las rotaciones de colaboradores dentro de la institución, a fin de realizar la modificación de perfil en las cuentas.
   - La Oficina de Tecnología de Información, tiene la responsabilidad de las creaciones de cuentas de usuarios.
   - Cada usuario es responsable de la administración de la cuenta asignada ya sea en el cambio de las contraseñas y la divulgación de la misma.

2. **Baja de Usuario**
   - La Oficina de Talento Humano, tendrá la responsabilidad de informar a la Oficina de Tecnología de Información cese o suspensión temporal de los colaboradores, con la finalidad de dar paso al procedimiento de baja o suspensión temporal de usuarios.
   - El área usuaria deberá verificar que el usuario cesado o suspendido no tenga carga de trabajo pendiente, en caso cuente con carga de trabajo se deberá realizar el balanceo de carga al usuario de reemplazo.
   - El área usuaria deberá validar el cese o suspensión temporal de las cuentas de los usuarios.

PROCEDIMIENTOS

- La v realizará la creación o baja de las cuentas de usuario indicadas por el área usuaria.
- Se validará la asignación de privilegios de las cuentas de usuario.
- El área usuaria deberá verificar las funciones a cargo del colaborador, contrastando con los permisos asignados al usuario del sistema. Para el caso de la baja de usuarios, el Responsable de la oficina usuaria deberá verificar la desactivación temporal o definitiva de la cuenta de usuario.
- El Responsable de la oficina usuaria solicitará la creación o baja de usuarios que tiene bajo su responsabilidad, así como también los cambios justificados a los privilegios a las cuentas de usuario y la eliminación de los accesos otorgados cuando el usuario deje de pertenecer a su oficina.

	POLÍTICA PARA EL CONTROL DE ACCESOS		Nro 02
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

- Impedir el acceso no autorizado a los sistemas de información y bases de datos.
- Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización de perfiles.
- Controlar la seguridad en la conexión entre la red de la institución y otras redes públicas o privadas.
- Registrar los eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.
- Concientizar a los usuarios respecto de su responsabilidad frente al uso de los equipos.

ALCANCE

- Esta política aplica a todas las formas de acceso a los usuarios que cuenten con permisos a los sistemas de información y bases de datos.
- Aplica al personal técnico que administra los permisos de acceso y las conexiones de red.

POLÍTICA

- El acceso a los sistemas de información debe estar controlado por la asignación de accesos según el perfil del colaborador.
- Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuario, desde la asignación de las cuentas hasta el bloqueo de las cuentas por motivos de cese o suspensión de labores.
- Es necesario concientizar a los colaboradores acerca de las responsabilidades por el mantenimiento de las cuentas de usuarios.

1. REQUERIMIENTOS PARA EL CONTROL DE ACCESO.

1.1. POLÍTICA DE CONTROL DE ACCESOS

En la aplicación de controles de acceso, se contemplarán los siguientes aspectos:

a. Identificar los requerimientos de seguridad de cada una de las aplicaciones.
b. Definir los perfiles de acceso de usuarios, según la naturaleza de sus funciones.
c. Verificar que el nivel de acceso otorgado es adecuado.
d. Entregar al responsable de cada oficina el detalle de accesos y permisos que tienen cada colaborador asignado a su oficina.
e. Los accesos de usuario no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

1.2. ADMINISTRACIÓN DE CONTRASEÑAS DE USUARIO

La asignación de contraseñas se controlará a través del siguiente proceso:

a. Garantizar que los usuarios cambien las contraseñas que les han sido asignadas la primera vez que ingresan al sistema.
b. Las contraseñas temporales que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez identificado el usuario.
c. Almacenar las contraseñas de manera encriptada.
d. Configurar los sistemas de tal manera que:
   - Las contraseñas tengan una cantidad no menor a 8 caracteres.
   - Suspensión o bloqueo permanente al usuario luego de 3 intentos de entrar con una contraseña incorrecta.
   - Solicitar el cambio de la contraseña cada 30 días

2. RESPONSABILIDADES DEL USUARIO

2.1. USO DE CONTRASEÑAS

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas garantizan la validación y autenticación de la identidad de un usuario.

Los usuarios deben cumplir las siguientes directivas:

a. Mantener las contraseñas en secreto.
b. Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.
c. Cambiar las contraseñas temporales en el primer inicio de sesión.

2.2. EQUIPOS DESATENDIDOS EN ÁREAS DE USUARIOS

Los usuarios deberán garantizar que los equipos desatendidos sean protegidos adecuadamente.

La Oficina de Tecnología de Información debe coordinar con la Oficina de Talento Humano las tareas de concientización a los colaboradores, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos

Los usuarios deben concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado.

3. CONTROL DE ACCESO A LA RED

El acceso a Internet será utilizado para los fines requeridos por la oficina usuaria.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a internet, con la finalidad de realizar revisiones de los accesos efectuados o analizar casos particulares.

4. CONTROL DE ACCESO AL SISTEMA OPERATIVO

4.1. IDENTIFICACIÓN Y AUTENTICACIÓN DE LOS USUARIOS

Todos los usuarios tendrán una cuenta de inicio de sesión único, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable.

4.2. SISTEMA DE ADMINISTRACIÓN DE CONTRASEÑAS

a. Permitir que los usuarios seleccionen y cambien sus propias contraseñas.
b. Incluir procedimientos de confirmación al cambio de contraseñas para evitar errores al ingreso.
c. Obligar a los usuarios a cambiar las contraseñas temporales en el primer ingreso a los sistemas de información.
d. Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.
e. Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
f. Modificar todas las contraseñas predeterminadas.

4.3. DESCONEXIÓN DE TERMINALES POR TIEMPO MUERTO

Esta herramienta de desconexión por tiempo muerto deberá cerrar la sesión iniciada. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para los equipos informáticos se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un colaborador debe abandonar su puesto de trabajo momentáneamente, bloqueara el equipo a fin de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

5. TRABAJO REMOTO

El trabajo remoto sólo será autorizado por la Oficina de Tecnología de Información, cuando se verifique que son adoptadas todas las medidas que correspondan a la seguridad de la información.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a. Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas de la institución.
b. La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.
c. Se debe definir el horario de trabajo remoto.

	POLÍTICA PARA LA SEGURIDAD ENTRE COMUNICACIONES		Nro 03
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

ALCANCE

- Todas las instalaciones de procesamiento y transmisión de información de la institución.

POLÍTICA

- La proliferación de software malicioso, hace necesario que se adopten medidas de prevención, a efectos de evitar la ocurrencia de tales amenazas.
- Es conveniente separar los ambientes de desarrollo, prueba y operaciones de los sistemas de la institución, estableciendo procedimientos que aseguren la calidad de los procesos que se implementen, con la finalidad de minimizar los riesgos producidos por la manipulación de información operativa.
- Los sistemas de información están comunicados entre sí; por lo tanto es necesario establecer criterios de seguridad en las comunicaciones que se establezcan.

1. PROCEDIMIENTOS DE MANEJO DE INCIDENTES

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida y eficaz frente a incidentes de seguridad de información.

Contemplar y definir todos los tipos probables de incidentes relativos a seguridad, incluyendo:

1. Fallas operativas
2. Código malicioso
3. Intrusiones
4. Error humano
5. Catástrofes naturales

a. Comunicar los incidentes a través de canales gerenciales apropiados tan pronto como sea posible.

b. Contemplar los siguientes puntos en los procedimientos para los planes de contingencia:
   1. Definición de las primeras medidas a implementar
   2. Análisis e identificación de la causa del incidente.
   3. Planificación e implementación de soluciones para evitar la reincidencia del mismo.
   4. Comunicar a las personas involucradas en la recuperación del incidente.

c. Implementar controles detallados y formalizados de las acciones de recuperación respecto de las violaciones de la seguridad y de corrección de fallas del sistema, garantizando:
   1. Acceso a los sistemas y datos existentes sólo al personal claramente identificado y autorizado.
   2. Documentación de todas las acciones de emergencia emprendidas en forma detallada.
   3. Constatación de la integridad de los controles y sistemas en un plazo mínimo.
   4. En los casos en los que se considere necesario, se solicitará la participación del Responsable de la Oficina de Asuntos Legales en el tratamiento de incidentes de seguridad ocurridos.

2. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

a. Se Prohíbe el uso de software no autorizado por la Oficina de Tecnología de Información.
b. Se debe actualizar periódicamente software de detección y reparación de virus, examinado los equipos informáticos.
c. Mantener los sistemas al día con las últimas actualizaciones de seguridad disponibles
d. Verificar antes de su uso, la presencia de virus en archivos de medios electrónicos.

3. RESGUARDO DE LA INFORMACIÓN

El responsable de la Oficina de Tecnología de Información dispondrá y controlará la realización las copias de seguridad del software y bases de datos, así como la prueba periódica de su restauración. Para esto se deberá contar con instalaciones de resguardo que garanticen la disponibilidad de toda la información y del software.

Se definirán procedimientos para el resguardo de la información, que deberán considerar los siguientes puntos:

a. Definir un esquema de rótulo de las copias de resguardo, que permita contar con toda la información necesaria para identificar cada una de ellas.
b. Almacenar en una ubicación remota copias recientes de información de resguardo.
c. Verificar y probar periódicamente la restauración de las copias de seguridad garantizando su eficacia y cumplimiento dentro del tiempo asignado a la recuperación en los procedimientos operativos.

4. ADMINISTRACIÓN DE LA RED

El Responsable de la Oficina de Tecnología de Información definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes de la institución, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a. Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos y para proteger los sistemas conectados.
b. Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.

5. ADMINISTRACIÓN Y SEGURIDAD DE LOS MEDIOS DE ALMACENAMIENTO

El Responsable de la Oficina de Tecnología de Información, con la asistencia del oficial de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles.

Se deberán considerar las siguientes acciones para la implementación de los procedimientos:

a. Eliminar de forma segura los contenidos de cualquier medio reutilizable que ha de ser retirado o reutilizado por la institución.
b. Almacenar todos los medios en un ambiente seguro y protegido.

5. INTERCAMBIOS DE INFORMACIÓN Y SOFTWARE

Cuando se realicen acuerdos para el intercambio de información, se especificarán el grado de sensibilidad de la información y las consideraciones de seguridad sobre la misma. Se tendrán en cuenta los siguientes aspectos:

a. Responsabilidades gerenciales por el control y la notificación de transmisiones, envíos y recepciones.
b. Responsabilidades y obligaciones en caso de pérdida de datos.
c. Uso de procedimientos para la información clasificada, garantizando que la información sea adecuadamente protegida.

6. SEGURIDAD DEL CORREO ELECTRÓNICO

El Responsable de la Oficina de Tecnología de Información definirá y documentará los procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a. Protección contra ataques al correo electrónico.
b. Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
c. Se identificaran el tamaño máximo de información transmitida y recibida.

	POLÍTICA PARA LA SEGURIDAD DE INFORMACIÓN INVOLUCRANDO AL PERSONAL		Nro. 04
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

- Reducir los riesgos de error humano, comisión de faltas que atenten contra la seguridad de información, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.
- Garantizar que los usuarios se encuentren capacitados para respaldar la Política de Seguridad de la institución en el transcurso de sus tareas normales.
- Establecer Compromisos de Confidencialidad con los colaboradores de las instalaciones de procesamiento de información.

ALCANCE

- Aplica a todos los colaboradores.

POLÍTICA

Se deben de reducir los riesgos ocasionados por error humano, la comisión de faltas graves que atenten contra la seguridad de información; es decir se deben implementar procedimientos que garanticen que los temas de seguridad de información sean de conocimiento por los colaboradores desde la etapa de selección de personal e incluirlas en los acuerdos que de firmen; además de verificar el cumplimiento de las mismas durante el desempeño diario.

1. **SEGURIDAD EN LA DEFINICIÓN DE PUESTOS DE TRABAJO Y LA ASIGNACIÓN DE RECURSOS.**
   - **1.1. Incorporación de la Seguridad en los Puestos de Trabajo.**
     - Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo. Éstas incluirán las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.
   - **1.2. Compromiso de Confidencialidad**
     - Como parte de sus términos y condiciones iniciales de empleo, los colaboradores, cualquiera sea su la modalidad de contrato, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información. La copia firmada del Compromiso deberá ser incluida en el legajo del colaborador.

2. **CAPACITACIÓN DEL USUARIO**
   - **2.1. Formación y Capacitación en Materia de Seguridad de la Información**
     - Todos los colaboradores recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la institución.

3. **RESPUESTA A INCIDENTES Y ANOMALÍAS EN MATERIA DE SEGURIDAD**
   - **3.1. Comunicación de Incidentes Relativos a la Seguridad**
     - Los incidentes o violación de la seguridad que involucre recursos informáticos relativos a la seguridad serán comunicados a través del responsable de la oficina tan pronto como ocurra.
     - Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el oficial de Seguridad Informática debe ser informado a la brevedad. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo.

	POLÍTICA PARA SEGURIDAD FÍSICA Y AMBIENTAL		Nro 06
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

- Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la institución.
- Proteger el equipamiento de procesamiento de información crítica de la institución ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados.
- Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información de la institución.

ALCANCE

- Aplica a todo el personal de la institución.

POLÍTICA

La seguridad física y ambiental pretende evitar el riesgo de accesos físicos no autorizados, mediante el establecimiento de perímetros de seguridad.
Para ello se establece la política para:

1. PERÍMETRO DE SEGURIDAD FÍSICA

- La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes de la institución y de las instalaciones de procesamiento de información.
- Se utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado.
  Se considerarán e implementarán los siguientes lineamientos y controles, según corresponda:
  a. Definir y documentar claramente el perímetro de seguridad.
  b. Ubicar las instalaciones de procesamiento de información dentro del perímetro donde no pueda producirse fácilmente un acceso no autorizado.
  c. El control de acceso físico al área estará restringido exclusivamente al personal autorizado. Los métodos implementados registrarán cada ingreso y egreso en forma precisa.

2. CONTROL DE ACCESO FÍSICO

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, a fin de permitir el acceso sólo al personal autorizado. Estos controles de acceso físico tendrán, por lo menos, las siguientes características:

a. Supervisar o inspeccionar a los visitantes a áreas protegidas y registrar la fecha y horario de su ingreso y egreso.
b. Controlar y limitar el acceso a la información clasificada y a las instalaciones de procesamiento de información, exclusivamente a las personas autorizadas.
c. Revisar los registros de acceso a las áreas protegidas.

3. SUMINISTRO DE ENERGIA

El equipamiento de suministro de energía debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras fallas eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, se contemplarán las siguientes medidas de control:

a. Disponer de múltiples enchufes o líneas de suministro para evitar un único punto de falla en el suministro de energía.

b. Contar con un suministro de energía interrumpible (UPS) para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas de la institución
c. Los equipos de UPS serán inspeccionados y probados periódicamente para asegurar que funcionan correctamente y que tienen la autonomía requerida.
d. Se dispondrá de un adecuado suministro de combustible para garantizar que el grupo electrógeno pueda funcionar por un período prolongado. Cuando el encendido del grupo electrógeno no sea automático, se asegurará que el tiempo de funcionamiento de la UPS permita el encendido manual de los mismos.

4. SEGURIDAD EN EL CABLEADO

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño, mediante las siguientes acciones:

a. Utilizar canaletas siempre que sea posible.
b. Proteger el cableado de red contra daño.
c. Separar los cables de energía de los cables de comunicaciones para evitar interferencias.

5. MANTENIMIENTO DE EQUIPOS

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes. Para ello se debe considerar:

a. La Oficina de Tecnología de Información realizará el plan de manteniendo preventivo y correctivo de los equipos informáticos.
b. Establecer que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.

	POLÍTICA PARA EL DESARROLLO Y MANTENIMIENTO DE SISTEMAS		Nro 07
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

- Asegurar la inclusión de controles de seguridad y validación de datos en el desarrollo de los sistemas.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

ALCANCE

- Esta Política se aplica a todos los sistemas informáticos.

POLÍTICA

El desarrollo y mantenimiento de las aplicaciones es un punto crítico de la seguridad.
Durante el análisis y diseño de los procesos que soportan estas aplicaciones se deben identificar, documentar y aprobar los requerimientos de seguridad a incorporar durante las etapas de desarrollo e implementación.

1. REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS

1.1. ANÁLISIS Y ESPECIFICACIONES DE LOS REQUERIMIENTOS DE SEGURIDAD

Esta Política se implementa para incorporar seguridad a los sistemas de información y a las mejoras o actualizaciones que se les incorporen.
Se deben tener en cuenta las siguientes consideraciones:

a. Definir un procedimiento para que durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad.
   - Procedimientos que establezcan la revisión periódica de los registros de auditoría de forma de detectar cualquier anomalía en la ejecución de las transacciones.
   - Procedimientos que realicen la validación de los datos generados por el sistema.

2. PROTECCIÓN DE LOS DATOS DE PRUEBA DEL SISTEMA

Las pruebas de los sistemas se efectuarán sobre datos extraídos del ambiente operativo. Para proteger los datos de prueba se establecerán normas y procedimientos que contemplen lo siguiente:

a. Prohibir el uso de bases de datos operativas.
b. Solicitar autorización formal para realizar una copia de la base operativa como base de prueba, llevando registro de tal autorización.

3. PROCEDIMIENTO DE CONTROL DE CAMBIOS

A fin de minimizar los riesgos de alteración de los sistemas, se implementarán controles durante la implementación de cambios; para ello se establecerá un procedimiento que incluya las siguientes consideraciones:

a. Verificar que los cambios sean propuestos por usuarios autorizados.
b. Efectuar las actividades relativas al cambio en el ambiente de desarrollo.
c. Obtener la aprobación por parte del usuario autorizado.
d. Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.
e. Mantener un control de versiones para todas las actualizaciones de software.
f. Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar su operatoria.

	POLÍTICA PARA EL ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DE LA INSTITUCIÓN		Nro 08
	Aprobado por:	Fecha de entrada en vigencia:	Versión: 1.0

OBJETIVO

Minimizar los efectos de las posibles interrupciones de las actividades normales de la institución y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.

ALCANCE

- Esta Política se aplica a todos los procesos de la institución.

POLÍTICA

1. **PROCESO DE LA ADMINISTRACIÓN DE LA CONTINUIDAD DE LA INSTITUCIÓN**

   El Comité de Gobierno Digital, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la institución.

   Este Comité tendrá a cargo la coordinación del proceso de administración de la continuidad de las operaciones de los sistemas informáticos frente a interrupciones imprevistas, lo cual incluye las siguientes funciones:

   a. Elaborar y documentar una estrategia de continuidad de las actividades de la institución consecuente con los objetivos y prioridades acordados.
   b. Proponer planes de continuidad de las actividades de la institución de conformidad con la estrategia de continuidad acordada.
   c. Establecer un cronograma de pruebas periódicas de cada uno de los planes de contingencia, proponiendo una asignación de funciones para su cumplimiento.
   d. Coordinar actualizaciones periódicas de los planes y procesos implementados.
   e. Proponer las modificaciones a los planes de contingencia.

2. **CONTINUIDAD DE LAS ACTIVIDADES Y ANÁLISIS DE LOS IMPACTOS**

   Con el fin de establecer un Plan de Continuidad de las Actividades de la institución se deben contemplar los siguientes puntos:

   a. Identificar las amenazas que puedan ocasionar interrupciones en los procesos diarios.
   b. Evaluar los riesgos para determinar el impacto de riesgo, tanto en términos de magnitud de daño como del período de recuperación.
   c. Identificar los controles preventivos para mitigar el impacto de riesgo.

3. **ELABORACIÓN E IMPLEMENTACIÓN DE LOS PLANES DE CONTINUIDAD DE LAS ACTIVIDADES DE LA INSTITUCIÓN**

   El proceso de planificación de la continuidad de las actividades considerará los siguientes puntos:

   a. Identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
   b. Analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.
   c. Documentar los procedimientos y procesos acordados.
   d. Instruir adecuadamente al personal, en materia de procedimientos y procesos de emergencia acordados.
   e. Probar y actualizar los planes.