UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TITULO DEL TRABAJO DE TITULACIÓN

DESARROLLO DE UNA GUÍA DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL DEPARTAMENTO DE SISTEMAS DEL GAD MUNICIPAL DE LA LIBERTAD

AUTOR

Yagual Sánchez Gustavo Andrés

PROYECTO DE UNIDAD DE INTEGRACIÓN CURRICULAR

Previo a la obtención del grado académico en
INGENIERO EN TECNOLOGÍAS DE LA INFORMACIÓN

TUTOR

Ing. Iván Coronel Suárez. Mgtr.

Santa Elena, Ecuador

Año 2024

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

Ing. José Sánchez Aquino. Mgt.
DIRECTOR DE LA CARRERA

Ing. Iván Coronel Suárez. Mgt.
TUTOR

Lsi. Daniel Quirumbay Yagual, MSIA.
DOCENTE ESPECIALISTA

Ing. Marjorie Coronel Suárez. Mgt.
DOCENTE GUÍA UIC

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN

Certifico que luego de haber dirigido científica y técnicamente el desarrollo y estructura final del trabajo, este cumple y se ajusta a los estándares académicos, razón por el cual apruebo en todas sus partes el presente trabajo de titulación que fue realizado en su totalidad por YAGUAL SÁNCHEZ GUSTAVO ANDRÉS, como requerimiento para la obtención del título de Ingeniero en Tecnologías de la Información.

La Libertad, a los 10 días del mes de Julio del año 2024

TUTOR

Firmado electrónicamente por:
IVAN ALBERTO
CORONEL SUAREZ

Ing. Iván Coronel Suárez. Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

Yo, **GUSTAVO ANDRÉS YAGUAL SÁNCHEZ**

DECLARO QUE:

El trabajo de Titulación, "Desarrollo de una guía de Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para el departamento de Sistemas del GAD Municipal de La Libertad" previo a la obtención del título en Ingeniero en Tecnologías de la Información, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

La Libertad, a los 10 días del mes de Julio del año 2024

EL AUTOR

Gustavo Andrés Yagual Sánchez

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CERTIFICACIÓN DE ANTIPLAGIO

Certifico que después de revisar el documento final del trabajo de titulación denominado "Desarrollo de una guía de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para el departamento de Sistemas del GAD Municipal de La Libertad", presentado por el estudiante, YAGUAL SÁNCHEZ GUSTAVO ANDRÉS fue enviado al sistema anti plagio, presentando un porcentaje de similitud correspondiente al 5%, por lo que se aprueba el trabajo para que continúe con el proceso de titulación.

CERTIFICADO DE ANÁLISIS
magister

Proyecto UIC (Yagual Gustavo) 2

5% Textos sospechosos

6% Similitudes
1% similitudes entre comillas (ignorado)
< 1% entre las fuentes mencionadas
0% Idiomas no reconocidos

Nombre del documento: Proyecto UIC (Yagual Gustavo) 2.docx
ID del documento: 4a7c7dd11b67eee8dc705f36eed3f23f825ed1c1
Tamaño del documento original: 1,46 MB

Depositante: IVAN ALBERTO CORONEL SUAREZ
Fecha de depósito: 18/6/2024
Tipo de carga: interface
fecha de fin de análisis: 18/6/2024

Número de palabras: 26.118
Número de caracteres: 177.261

TUTOR

Firmado electrónicamente por:
IVAN ALBERTO CORONEL SUAREZ

Ing. Iván Coronel Suárez. Mgtr.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

AUTORIZACIÓN

Yo, **YAGUAL SÁNCHEZ GUSTAVO ANDRÉS**

Autorizo a la Universidad Estatal Península de Santa Elena, para que haga de este trabajo de titulación o parte de él, un documento disponible para su lectura consulta y procesos de investigación, según las normas de la Institución.

Cedo los derechos en línea patrimoniales del trabajo de titulación profesional con fines de difusión pública, además apruebo la reproducción de este artículo académico dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica y se realice respetando mis derechos de autor.

La Libertad, a los 10 días del mes de Julio del año 2024

EL AUTOR

Gustavo Andrés Yagual Sánchez

AGRADECIMIENTO

Le agradezco a Dios por ser una fuente inagotable de perseverancia y guía, por darme fortaleza y el conocimiento necesario para llevar a cabo este proyecto de titulación.

A mi familia, quienes han sido mi apoyo incondicional constante, durante todo este proceso. Quienes estuvieron presente en mis momentos más difíciles, cuando quise abandonar y tirar la toalla, gracias por no permitir rendirme, por su amor incondicional y por ser la fuente de mi inspiración. Especialmente a mi madre, Vanessa Sánchez, y a mi padre, Gustavo Yagual, quienes, con su sacrificio y esfuerzo, me han ayudado a alcanzar este objetivo.

Agradezco también a la Universidad Estatal Península de Santa Elena y a mis docentes, cuyos conocimientos ayudaron a mi formación académica. De manera especial, expreso mi gratitud al Ing. Iván Coronel, mi docente tutor, por su apoyo y experiencia brindada.

Gustavo Andrés, Yagual Sánchez

DEDICATORIA

Le dedico este proyecto a Dios, quien me otorgó la sabiduría necesaria para concluir mi trabajo y brindarme fortaleza en tiempos difíciles. A mi madre, por todo el amor que me ha dado a lo largo de mi vida, como un hombre de bien y siempre estando a mi lado.

A mi padre, quien me proporciono ayuda económica y apoyo moral para mi culminar mi proceso académico, inculcándome valores y valentía para enfrentar los obstáculos.

Y en general a mis seres queridos y personas fundamentales que estuvieron apoyándome y dándome las fuerzas necesarias para no rendirme en este duro camino.

Gustavo Andrés, Yagual Sánchez

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Actualmente, la información es uno de los recursos más importantes y valiosos dentro de cualquier organización. Es fundamental analizar la seguridad de la información para la detección temprana de riesgos y garantizar que se mantenga la integridad, confidencialidad y disponibilidad de la información de forma óptima. El proyecto tiene como objetivo elaborar una guía para la implementación de un Sistema de Gestión de Seguridad de la Información y proteger los activos que maneja el departamento de Sistemas del GAD Municipal La Libertad, basados en la norma ISO 27001.

En primer lugar, se realizó el levantamiento de información para verificar el estado actual del Departamento Sistemas, se realizaron entrevistas y encuestas dirigidas al jefe y empleados del departamento. La metodología utilizada fue el ciclo Deming en sus 4 fases (Planear, Implementar, Verificar y Actuar), en cada punto se constituyen actividades que permiten definir el alcance, inventario y tasación de activos con el objetivo de determinar vulnerabilidades que influyen en la gestión de seguridad y elaborar un plan de seguridad de la información. Por último, se llevó a cabo la elaboración de políticas de seguridad sugeridas, en base a los controles establecidos y se entregó documentación que permita garantizar la integridad de la información, además los resultados se comunicaron al gerente del departamento para que puedan tomar acciones de la implementación del SGSI en un futuro.

Palabras claves: seguridad – sistema – gestión – normas

ABSTRACT

Currently, information is one of the most important and valuable resources within any organization. It is essential to analyze information security for the early detection of risks and to ensure that the integrity, confidentiality and availability of information is optimally maintained. The project aims to develop a guide for the implementation of an Information Security Management System and protect the assets managed by the Systems Department of the GAD Municipal La Libertad, based on the ISO 27001 standard.

First, information was gathered to verify the current status of the Systems Department, interviews and surveys were conducted with the head and employees of the department. The methodology used was the Deming cycle in its 4 phases (Plan, Implement, Verify and Act), in each point there are activities that allow defining the scope, inventory and valuation of assets in order to determine vulnerabilities that influence security management and develop an information security plan. Finally, the development of suggested security policies was carried out, based on the established controls and documentation was provided to ensure the integrity of the information, and the results were communicated to the manager of the department so that they can take actions for the implementation of the ISMS in the future.

Keywords: safety - system - management - standards

INTRODUCCIÓN

Es un hecho que la información es uno de los activos más importantes dentro de una organización o entidad. La protección de estos activos frente a amenazas que puedan comprometer su confidencialidad, integridad y disponibilidad se han convertido en una parte fundamental. A partir de ese contexto, la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se presenta como una solución indispensable para que las organizaciones puedan gestionar de manera efectiva los riesgos relacionados con la seguridad de la información.

El Gobierno Autónomo Descentralizado de La Libertad requiere cubrir esta necesidad. El departamento de Sistemas y Recursos Tecnológicos de la organización maneja una gran cantidad de información, que requiere una protección adecuada contra posibles amenazas, ya sean de tipo internas o externas. La ausencia de una estructura formal para la gestión de la seguridad de la información puede llevar a amenazas significativas, poniendo en riesgo tanto la información como la operación del GAD Municipal.

El objetivo de este trabajo de titulación es desarrollar una guía práctica para la implementación de un SGSI en el departamento de Sistemas del GAD Municipal de La Libertad teniendo su contexto organizacional. El desarrollo de la guía no solo contribuirá a salvaguardar la información confidencial del departamento de Sistemas, sino que también mejorará la confianza de los ciudadanos en la capacidad de la organización para gestionar sus datos de manera segura y responsable.

1 CAPÍTULO. FUNDAMENTACIÓN

1.1 Antecedentes

Actualmente el uso de las TIC's se ha convertido en una herramienta fundamental, en el fortalecimiento de las procesos técnicos y administrativos de las empresas. Además, con el constante crecimiento del internet, las amenazas y vulnerabilidades también tienen un impacto negativo en la seguridad informática y se ven mucho más afectadas. Es por ello que el correcto manejo de esas amenazas, basadas en un estándar de seguridad, como las normas ISO 27001 brindan un apoyo crucial que permite establecer, implantar y mejorar un Sistema de Gestión de la Seguridad de la Información de una empresa [1].

Dentro de la investigación preliminar realizada en los diferentes repositorios de las Universidades del mundo, se encontraron proyectos de titulación que sirven como antecedentes para el presente trabajo de investigación, entre los más relevantes se encuentra el trabajo 'Elaboración de una guía de implementación de un SGSI para la corporación ecuatoriana para el desarrollo de la investigación y la academia - CEDIA' realizado por la Srta. María Auxiliadora Orellana Toledo en el 2022, como resultado nos explica que la empresa CEDIA cuenta con activos muy importantes, que deben ser protegidos y garantizar la seguridad de la información, mismo objetivo que se logró implementando la metodología de análisis de riesgo ISO/IEC 27001, debido a que esta norma tiene controles que verifican y llevan seguimiento a los 3 pilares fundamentales de la seguridad de la información, confidencialidad, disponibilidad e integridad de los datos, los cuales son indispensables para alcanzar un nivel de seguridad adecuado [2].

A nivel mundial y latinoamericano se encontró el trabajo 'Auditoría Informática en los procesos administrativos del departamento de informática de Chocolatera Moctezuma, S.A. de C.V' elaborado por la Sra. Evelia Zamora Reyes en el 2004, en la Universidad Nacional Autónoma de México, dicho trabajo también hace énfasis en los procesos generales de la empresa, específicamente al departamento de TI, los controles que se realizan para verificar el correcto funcionamiento de los sistemas informáticos y que la empresa se encuentre actualizada respecto a sus políticas de seguridad y evitar riesgos legales y fiscales [3].

El trabajo encontrado de ‘Auditoría Informática aplicando la norma ISO 27001 para optimizar la seguridad de la información en el departamento de TIC’s del centro de investigación y desarrollo FAE’ se realizó a nivel local en Ecuador específicamente en la ciudad de Ambato, dicho trabajo tiene la finalidad de brindar seguridad a la información que el departamento maneja y minimizar los riesgos implementando las normas ISO 27001, además de garantizar la confidencialidad, integridad y disponibilidad de los activos de información [4].

1.2 Problema Científico

La problemática del proyecto, parte de la necesidad a nivel organizacional, de contar con información documentada y actualizada de políticas de seguridad, con la finalidad de prevenir y mitigar vulnerabilidades presentes en el entorno. Además del inexistente análisis de vulnerabilidades y valoración de activos informáticos en el período de tiempo que lleva la institución laborando. Esto puede traer repercusiones al tratar con la información que allí se maneja [5].

En base a los trabajos revisados, se obtiene la información correspondiente para realizar la guía de implementación del SGSI al departamento de Sistemas GAD municipal de La Libertad, mediante la observación y utilización de técnicas e instrumentos de recolección de datos, específicamente entrevistas y encuestas realizadas al personal que labora en el departamento, se desconoce la realización de una auditoría de carácter informática en los últimos años.

Esto conlleva a que no se tengan planes estratégicos y operativos del departamento actualizados, no poseer una correcta revisión de las políticas de seguridad de la información, un control de las metodologías de gestión de riesgo, en caso de poseerlo, esquemas de clasificación de información, además de la necesidad que tiene el departamento de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI).

Esos puntos pueden presentar un problema a la seguridad de la información del departamento, ya que los datos de clientes y usuarios que allí existen son activos de información valiosos para la empresa, sin un respectivo control y políticas de seguridad actualizadas o implementadas, la información puede pasar a manos de

gente no deseada y ocasionar serios problemas legales a la entidad de forma general, enfrentando demandas de usuarios y teniendo grandes pérdidas económicas.

Si el departamento cuenta con los puntos mencionados, se verifica que la información esté actualizada y aprobada por la alta gerencia, y que éstas vayan alineadas con las políticas generales de la empresa. Estos incidentes suceden por las inexistentes medidas de protección, causando perdidas de credibilidad, productividad y prejuicios financieros que comprometen la continuidad de la organización.

1.3 Descripción del Proyecto

Es fundamental tener en consideración que el objetivo principal del Departamento de Sistemas y Recursos Tecnológicos es lograr implementar un SGSI basado en las normas ISO 27001, para posteriormente obtener una certificación que valide todo el proceso realizado, por ello el proyecto se basó en el desarrollo de una guía que permita implementar un SGSI, más no se verificó que se efectué el cumplimiento del mismo, el cual es necesario para la certificación ISO. Dentro de la guía realizada se tomaron en cuenta solo 4 fases que son fundamentales para el desarrollo del SGSI las cuales van a ser detalladas a continuación:

FASE 1: Análisis del Contexto de la Organización

Dentro de esta fase se inició el desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI), para ello se debe identificar el contexto interno y externo de la organización. Este paso es importante, ya que ayuda a comprender las diversas circunstancias que pueden afectar la capacidad de la empresa para alcanzar sus objetivos de seguridad.

Así mismo, se define el alcance del sistema de gestión de seguridad de la información (SGSI), para ayudar a la organización a cumplir con sus requisitos de seguridad y planificar la implementación del sistema. Un alcance bien delimitado permite establecer los recursos necesarios, evitando pérdidas de tiempo, costos y esfuerzos. Esto deriva en una gestión de recursos más eficiente y en una mayor probabilidad de éxito en la implementación del SGSI [6]. Al tener un alcance bien definido, la organización puede alinear mejor sus requisitos de seguridad con los

ejercicios de análisis y evaluación de riesgos, asegurando la implementación de todas las medidas de seguridad.

FASE 2: Elaboración de Política - Objetivos del SGSI

En este punto, es necesario definir la política del Sistema de Gestión de Seguridad de la Información (SGSI), la cual se debe alinear con los objetivos, características, ubicación, y activos del Departamento de Sistemas y Recursos Tecnológicos de la entidad. Esta política debe ser revisada y aprobada por el gerente del departamento, y se debe revisar periódicamente cada año. Los objetivos de control que se establecen posteriormente están basados en el marco de la política del SGSI.

La política de seguridad es un documento que establece las reglas y principios para lograr los objetivos de seguridad aplicados a los sistemas informáticos. Estas políticas deben especificar las condiciones, derechos y obligaciones de los miembros de la organización con respecto a la utilización de los sistemas informáticos, además de cumplir con los principales aspectos de confiabilidad, integridad y disponibilidad [7].

FASE 3: Planificación del SGSI

En esta etapa, se debe realizar el inventario de activos junto con sus amenazas y vulnerabilidades, posteriormente elaborar una valoración de riesgos en base a la confidencialidad, disponibilidad e integridad de la información. El nivel de detalle alcanzado en la elaboración del inventario tendrá un efecto positivo en los resultados obtenidos, ya que aquí se registran todos los activos utilizados en los procedimientos del departamento. Además, se definió una metodología para la gestión de riesgos, lo que implica seleccionar procedimientos para el tratamiento efectivo de los riesgos [8].

Por último, se realizó una evaluación de los riesgos de seguridad de los activos, la cual se elaboró después de analizar su impacto en el desarrollo del procedimiento. Para concluir esta etapa, se deben identificar los controles aplicables de la norma ISO 27001, para lo cual se elaboró una declaración de aplicabilidad que incluye los objetivos de control y si son aplicables o no al contexto de la organización.

FASE 4: Documentación del SGSI

Finalmente, en la última fase es necesario documentar los procesos por dos razones principales. Primero, garantizar que el proceso pueda repetirse de forma constante con el pasar del tiempo. Sin una documentación adecuada, es difícil replicar de forma uniforme los procedimientos requeridos, lo que ocasiona inconsistencias y errores.

En segundo lugar, la documentación establece una base para la mejora continua. Tener un control del proceso proporciona información valiosa para determinar la eficacia del sistema de gestión de seguridad y posteriormente llegar a la implementación del SGSI en sus siguientes fases, esto permite tomar decisiones adecuadas, para modificar y mejorar aspectos del SGSI. De esta forma, la documentación será una herramienta clave para la mejora continua, uno de los principales objetivos de cualquier sistema de gestión, esto asegura que los procesos se optimicen constantemente, adaptándose a futuras necesidades [9].

1.4 Objetivos del Proyecto

1.4.1 Objetivo General

- Elaborar una guía de implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en las buenas prácticas y normas ISO 27001, para el departamento de Sistemas del GAD-LIBERTAD.

1.4.2 Objetivos Específicos

- Identificar activos y riesgos informáticos presentes en el departamento de Sistemas y recursos tecnológicos de la municipalidad de La Libertad.
- Determinar los controles de la norma ISO 27001, mediante la declaración de aplicabilidad, para el desarrollo de la guía del SGSI.
- Determinar una metodología de gestión de riesgos, para reducir incidentes de la seguridad de la información.
- Establecer recomendaciones y buenas prácticas en base a las normas ISO 27001, para la creación adecuada de políticas de seguridad.

1.5 Justificación del Proyecto

Actualmente, la mayoría de las organizaciones usan las tecnologías informáticas para almacenar, procesar y resguardar información. Cumplen un papel fundamental dentro del funcionamiento interno de sus procesos, a su vez, dicha información que allí se maneja está sometida a una gran cantidad de riesgos y amenazas informáticas.

El SGSI tiene como objetivo, establecer mecanismos de gestión para la confidencialidad, integridad y disponibilidad de la información dentro del estándar ISO 27001. Busca la identificación de activos y personal que basan el desarrollo de los sistemas informáticos en procesos de gestión de riesgos, relacionados a los servicios que presta la organización, también se enfoca en verificar la existencia de controles de seguridad que permitan una correcta integración a políticas de seguridad apoyadas en dicha norma [10].

El desarrollo de la guía de implementación del SGSI basada en normas ISO 27001, tendrá como principales beneficiaros al gerente del departamento de Sistemas y Recursos Tecnológicos, a su vez, los empleados encargados del desarrollo de software, manejo de bases de datos, redes y cableados, entre otros. Los beneficiarios directos son los usuarios que maneja la entidad, ya que guardan sus datos en dichos sistemas y tienen la seguridad de que su información no se usará para fines negativos [11].

La auditoría informática es una herramienta que asiste a la organización, en la detección de posibles fallos en el sistema, de igual forma identifica oportunidades para mejorar los procesos internos. Esto, permite realizar acciones importantes, tales como la evaluación de la efectividad de los controles internos, verificación del cumplimiento de las normas, y el análisis de la aparición de nuevos riesgos, lo que facilita la implementación de procedimientos destinados a minimizar su impacto [4].

La elaboración de un Sistema de Gestión de Seguridad de la Información se alinea al Plan de creación de oportunidades, en el eje de seguridad integral, según el objetivo 9, el cual busca garantizar la seguridad ciudadana, orden público y la gestión de riesgos [12].

1.6 Alcance del Proyecto

El objetivo principal del proyecto, es desarrollar una guía de implementación de un Sistema de Gestión de Seguridad de la Información, basado en el estándar ISO 27001. El proyecto incluye revisión de políticas, procedimientos, controles técnicos y organizativos, para garantizar que el departamento maneje la información de forma correcta y así prevenir fallas en los procesos y procedimientos relacionados con la seguridad de la información.

Dentro de los controles establecidos, se llevó a cabo un análisis de vulnerabilidades en los servidores del departamento de Sistemas. Dicho análisis incluye la identificación de posibles brechas de seguridad, tales como puertos abiertos, servicios utilizados y vulnerabilidades encontradas, para finalmente presentar los resultados en una matriz donde determinaremos la vulnerabilidad y el tipo de riesgo que representa, sea este alto, medio o bajo. Del mismo modo, se realizó una tasación de activos informáticos, incluyendo hardware y datos relacionados con la tecnología de la información.

Adicionalmente se desarrollaron pautas y recomendaciones para establecer un marco de gestión de seguridad de la información en el departamento de Sistemas. Dichas recomendaciones sirven como base para futuras iniciativas de seguridad y proporcionen una dirección clara para la implementación de un SGSI, si así lo requiere el departamento. No se llegó al punto de implementación del SGSI, de acuerdo a los objetivos del proyecto, cantidad de información abordada y tiempo de ejecución.

Por último, se elaboró documentación que ayude al seguimiento y revisión de los controles que están establecidos dentro de la norma, sean éstos de control de acceso, procesos para realizar respaldos, mantenimiento de equipos informáticos, clasificación de información, entre otros. En resumen, el proyecto brinda una evaluación de la seguridad de la información, con el objetivo de identificar áreas de mejora y fortalecer controles de seguridad existentes.

1.7 Beneficiarios del Proyecto

Los principales beneficiarios del proyecto son los empleados del Departamento de TI del GAD-Libertad, ya que contarán con una guía detallada para la implementación de un sistema de Gestión de Seguridad de la Información que evitará riesgos informáticos, que pueden afectar los activos de información que maneja la organización. Además, como beneficiarios indirectos, están todos los departamentos del GAD que manejan procedimientos e información delicada de los usuarios en caso de llevar a cabo la implementación del SGSI a toda la entidad.

2 CAPÍTULO. PROPUESTA

2.1 Marco Contextual

Descripción de la Empresa

El municipio de La Libertad, como otros municipios en Ecuador, se gobierna de manera independiente del poder central, de acuerdo con la Constitución. Su administración está a cargo de un alcalde, quien ejerce el poder ejecutivo, y de un concejo cantonal, que representa el poder legislativo. Esta autonomía municipal se fundamenta en los artículos 253 y 264 de la Carta Magna, así como en los artículos 1 y 16 de la Ley de Régimen Municipal, que le confieren independencia en sus funciones, finanzas y gestión [13].

El GAD-LIBERTAD se encuentra ubicado en la provincia de Santa Elena en la AV. Eleodoro Solorzano y calle 11 frente al paseo Shopping, su horario laboral y atención al cliente es de 8:30 AM a 5:30 PM, está encargado de ofrecer 3 servicios principales a la ciudadanía los cuales son: acceso a la información pública, acreditación para permiso de funcionamiento para Centros de Desarrollo infantil, privados y públicos, por último brinda asesorías a ciudadanos que presenten problemas, acercándose directamente a las oficinas de la entidad exponiendo su caso o inconformidad frente a un servidor público.

Para acceder a la información, es importante realizar una solicitud y llenar un formulario el cual le permite verificar la información pública, que se genera o se encuentra en poder de la entidad, de conformidad con la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP (ARTS. 9 Y 19).

Objetivos Principales de la empresa

- **Sistema de Participación Ciudadana:** Instituir el poder ciudadano del Cantón La Libertad, como resultado de procesos de participación individual y colectiva de las ciudadanas y ciudadanos de la jurisdicción cantonal, sin discriminación de ninguna clase, quienes, de manera protagónica participan en la toma de decisiones, planificación y gestión de asuntos públicos; así como, en el control social de todos los niveles de gobierno, las funciones e instituciones del Estado, y de las personas naturales o jurídicas del sector privado que manejan fondos públicos, prestan servicios o desarrollan actividades de interés público en la jurisdicción del cantón.
- **Concejo Municipal:** Ejercer la facultad normativa y expedir los acuerdos y resoluciones en materia de competencia del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad, aprobar los actos que le competan para la ejecución de planes y programas a través de la Función Ejecutiva; fiscalizar y evaluar las actuaciones u omisiones del ejecutivo en el cumplimiento de sus funciones, observando el ordenamiento jurídico y competencias previstas en la ley, a fin de fortalecer el control interno y la correcta administración de la cosa pública para el desarrollo económico y social del cantón.
- **Alcaldía:** Liderar, coordinar, supervisar y disponer todas las acciones y procesos de trabajo del Gobierno Autónomo Descentralizado Municipal del Cantón La Libertad, asegurando el cumplimiento de los objetivos y estrategias institucionales; evaluar los procesos administrativos y agregadores de valor para asegurar la eficiencia, eficacia, calidad y calidez de la gestión municipal para beneficio de la ciudadanía del cantón.
- **Unidad de Gestión de Riesgos:** Prevenir y mitigar los impactos producidos por los fenómenos naturales, antrópicos y tecnológicos, con sustento en una adecuada planificación, generación de políticas regulatorias, capacitación y coordinación con los diferentes actores de la prevención y gestión de riesgos en el cantón, provincia y a nivel nacional; realizar estudios y establecer lugares seguros para albergues, organizar a la ciudadanía para enfrentar y

reducir riesgos, manejar emergencias y desastres con el apoyo técnico y logístico del GAD Municipal del Cantón La Libertad.

- **Unidad de Sistemas y Recursos y Tecnológicos:** Coordinar y administrar eficientemente los recursos tecnológicos informáticos, mediante la utilización de tecnologías de información y la automatización de procesos, a través de la web institucional, servicios informáticos, redes, equipos de computación para el procesamiento automático de datos, acceso a la información y seguridad de los sistemas informáticos, a fin de apoyar de manera eficaz el desarrollo tecnológico y gestión municipal y la toma de decisiones en beneficio de la colectividad del cantón.

2.1.1 Base Legal

LOTAIP: La Ley Orgánica de Transparencia y Acceso a la Información Pública, protege y regula el derecho primordial de las personas a obtener información. Por ello, se hace pública la gestión del CPCCS y se cumple parcialmente con el proceso de rendición de cuentas a la ciudadanía.

Art.7 Difusión de la información pública: Todas las instituciones públicas, según lo establecido en la Constitución y en la presente Ley, tienen la obligación de difundir información a través de sus portales web y otros medios accesibles al público. Esta información, que se considera de carácter obligatorio, incluye un conjunto mínimo de datos actualizados que permiten a la ciudadanía conocer la gestión administrativa de dichas entidades [14].

LOPDGDD: El objetivo de la Ley Orgánica de Protección de Datos Personales es garantizar el derecho de la ciudadanía a conocer el paradero de sus datos personales y cómo las organizaciones los utilizan. Todas las entidades, ya sean públicas o privadas, deberán cumplir con los lineamientos establecidos en esta ley. De acuerdo con la legislación vigente, este reglamento define los elementos necesarios para implementar y hacer efectivo el marco legal que protege, procesa y custodia la información constitucionalmente amparada [15].

Art. 10.-Principios. Sin perjuicio de otros principios establecidos en la Constitución de la República, los instrumentos internacionales ratificados por el Estado u otras normas jurídicas, la presente Ley se regirá por los principios de:

j) Los responsables y encargados deben tomar todas las medidas de seguridad necesarias para proteger los datos personales de cualquier riesgo o amenaza. Estas medidas deben ser acordes con el estado actual de la tecnología, ya sean de índole organizativa, técnica o de cualquier otra naturaleza. La implementación de estas medidas debe tener en cuenta la naturaleza de los datos personales, así como el contexto y ámbito en el que se manejan [16].

Organigrama Estructural

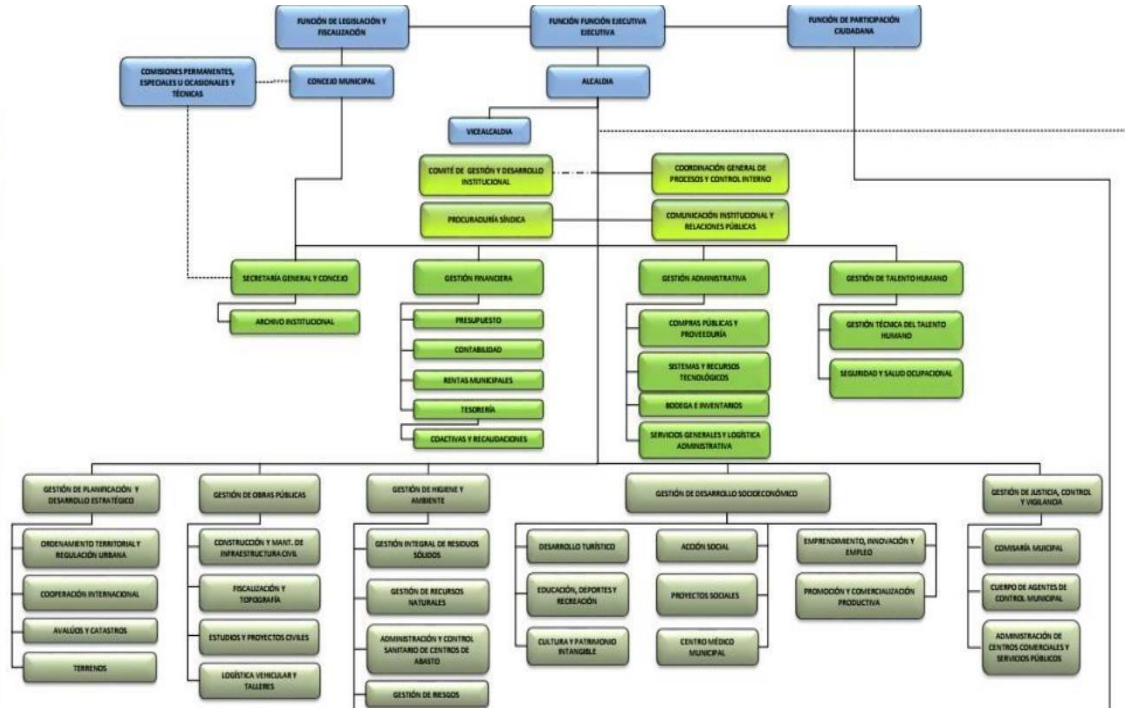

Figura 1. Organigrama Estructural del GAD Libertad

2.2 Marco Conceptual

Auditoría informática

La auditoría informática es una herramienta para la evaluación de infraestructuras, aplicaciones y procedimientos relacionados con la tecnología dentro de una organización. Permite evaluar la eficiencia y eficacia de los controles internos y seguridad de los sistemas de información, además de controlar el cumplimiento de

las normas y procedimientos vigentes, tener una gestión de riesgos optima y otros puntos relevantes dependiendo del tipo de auditoría que se desea realizar [4].

Entre los beneficios de una auditoría interna específicamente de la seguridad de la información es mejorar las gestiones y procesos de una empresa, ayuda a la concientización de los empleados respecto a la calidad de sus políticas y sus sistemas de gestión de seguridad de la información (SGSI), así como su participación en la mejora de del sistema de gestión [5].

Las tecnologías brindan muchas facilidades a la hora de llevar el manejo de una empresa, pero a su vez, se presentan muchos y riesgos y vulnerabilidades de la información que allí se maneja. Por lo que es indispensable establecer controles para mantener y garantizar que la información que allí se maneja, no será perpetuada por delincuentes o estar propensa a ataques informáticos. De allí nace la necesidad de contar con auditores especializados en el área informática, que prueben dichos controles y sean efectivos. Por lo que periódicamente se realizaran estas evaluaciones a los sistemas para diagnosticar el correcto manejo de las tecnologías de la información [11].

Seguridad de la Información

Según Oscar Muñoz en su trabajo ‘Sistema de Gestión de Seguridad de la Información basado en normas ISO/IEC 27001’ [17] se basa en 3 pilares fundamentales para la protección de la información:

- **Confidencialidad:** se refiere a la comunicación de un mensaje de datos y a la restricción del acceso, solamente con las personas o entidades autorizados.
- **Integridad:** característica que tiene el mensaje, comunicación o datos, la cual nos asegura que el mismo no haya sido modificado, desde su momento de envío, hasta llegar a su destino. Implica exactitud y totalidad de la información.
- **Disponibilidad:** capacidad de un servicio, aplicativo o sistema de datos de mantenerse en línea, siempre y en todo lugar donde el usuario lo requiera. Accesibilidad y uso oportuno de la información.

Gestión de Seguridad

Su objetivo principal es garantizar una correcta implementación de los controles de seguridad a través de evaluaciones políticas de una organización. Una de sus funciones es administrar la integridad y privacidad de la información que se procesa, en la infraestructura tecnológica. Tiene como enfoque la revisión de actividades de tipo administrativo, donde se evaluará el correcto funcionamiento del hardware, software, programas, aplicaciones, sitios web y todo lo relacionado a activos informáticos [4].

La gestión de la seguridad tiene el apoyo de todos los departamentos de una entidad u organización. Colabora con áreas de tecnología de la información, recursos humanos, gestión de riesgos y cumplimiento, para así cumplir con un enfoque equilibrado de la seguridad de la información. Con el avance de la tecnología surgen nuevas formas que afectan la seguridad de la información, por eso se deben analizar estas vulnerabilidades, para desarrollar un sistema de gestión de seguridad de la información, que pretende minimizar riesgos, que se puedan presentar en todo el proceso.

Evento de Seguridad de la Información

Es un evento detectado del estado de un sistema, servicio o red que sugiere un posible incumplimiento de las normas de seguridad de la información, falla en las políticas de protección, o una situación previamente desconocida que puede ser relevante para la seguridad [18].

Evaluación de Riesgo

Consiste en la comparación de las debilidades identificadas en cada riesgo y contrastarlas con el nivel de riesgo aceptable. Bajo este enfoque, se deben llevar a cabo dos tipos de evaluaciones: una previa a la implementación de controles y otra posterior, según los resultados obtenidos en la etapa anterior [19].

Sistema de Gestión de Seguridad de la Información

Un plan integral de seguridad informática se basa en las normas, procesos, recursos y acciones que una empresa gestiona para proteger su información. Este sistema

abarca políticas y procedimientos que la organización utiliza con el fin de salvaguardar sus datos y activos digitales [20].

La gestión de la seguridad de la información se realiza mediante un proceso documentado y conocido por toda la organización. Según Gómez Cristian en su trabajo 'Diseñar un sistema de Gestión de la Seguridad de la Información para la empresa QWERTY S.A a partir de la norma ISO 27001' el objetivo de un SGSI es garantizar que los riesgos de la seguridad de la información sean conocidos y gestionados de una forma documentada y que pueda adaptarse a los cambios que producen dichos riesgos, por la organización o entidad [21].

Activos de Información

Un activo de información es cualquier componente que aborda uno o más procesos de cualquier tipo de organización o entidad, ya sean de tipos humanos, tecnológicos, documental, estructura, hardware y software, entre otros. En consecuencia, dicho activo debe protegerse adecuadamente [22].

Norma

Conjunto de pautas necesarias para implementar políticas. Las normas detallan específicamente las tecnologías, metodologías, procedimientos de aplicación y otros elementos involucrados, además su cumplimiento es obligatorio [23].

2.3 Marco Teórico

Evolución de Normas ISO y aplicativa universal

La norma ISO (Organización Internacional de Estandarización) establece estándares y requisitos diseñados para satisfacer las expectativas del cliente, automatizar procesos y minimizar diferencias en la producción. Los primeros procesos estandarizados se remontan a los años 1930 con la producción en cadena de Henry Ford. Durante la Segunda Guerra Mundial, se establecieron normas estandarizadas de fabricación de armas. En 1971, el Instituto de Estandarización Británico (BS) diseñó normas estandarizadas para la industria electrónica y en 1979 se emitió la norma BS5750 para todo tipo de industrias [24].

En 1947 se creó la Organización Internacional de Normalización (ISO) con el objetivo de integrar las normas de diferentes países. En 1980, ISO designó sus Comités Técnicos y su familia de Normas se convirtió en el lenguaje universal de los Sistemas de Calidad. En 1994, se establecieron las normas ISO 9001, que certifican que el sistema de gestión de calidad utilizado en la producción es adecuado.

Seguridad de la Información en Latinoamérica

Un estudio realizado por la Asociación Colombiana de Ingenieros de Sistemas (ACIS) junto con universidades de México y el centro de atención de incidentes de Uruguay. Indica que, en Latinoamérica, los estándares y buenas prácticas más utilizados en las áreas de seguridad de la información y departamentos de TI son ISO 27000, ITIL, Cobit 4.1 y un gran numero señaló que no se consideran estándares. Estas metodologías proporcionan marcos de planificación y gestión en temas de tecnologías de información, con el objetivo de organizar y estructurar estas áreas en las organizaciones [25].

ESTÁNDARES Y BUENAS PRACTICAS	PORCENTAJES
ISO 27001	45,8
No se consideran	37,7
ITIL	26,9
Cobit 4.1	23,4
Guías del NIST (National Institute of Standards and Technology) USA	12,3
OSSTM - Open Standard Security Testing Model	7,5

ESTÁNDARES Y BUENAS PRACTICAS	PORCENTAJES
Top 20 de fallas de seguridad del SANS	7,1
Common Criteria	5,2
Magerit	5,2
ISM3 - Information Security Management Maturity Model	3,9
Guías de la ENISA (European Network of Information Security Agency)	2,3
Octave	2,3

Tabla 1. Encuesta realizada a profesionales de tecnología de la Información [25]

La encuesta fue realizada tomando una muestra de 513 profesionales de la tecnología de la información y carreras relacionadas, este análisis nos dio a conocer que la mayor parte de empresas y organizaciones utilizan el estándar ISO 27001, otra cantidad bastante alta no tienen establecido un estándar claro en cuanto a la seguridad de la información, dejando una brecha que se puede materializar en amenazas para la institución, además dentro del mismo estudio muestran otros datos que resultan relevantes para la presente investigación.

Normas ISO/IEC 27000

El conjunto de normas ISO 27000 elaborado por la ISO/IEC, proporciona un marco de referencia para la gestión de la seguridad de la información, que puede ser adoptado por cualquier tipo de organización. Este marco establece un modelo a seguir para la elaboración de un Sistema de Gestión de Seguridad de la Información (SGSI), permitiendo a las empresas implementar un sistema para administrar la

seguridad de sus activos, ya sean datos intelectuales, financieros, de empleados o clientes [20]. Principalmente un SGSI requiere que cada organización lleve a cabo cuatro actividades: establecer, implementarlo, mantenerlo, y monitorear su desempeño.

Fundamentación basada en Norma ISO/IEC 27001

La norma ISO/IEC 27001 se desarrolló en 2005 como una evolución de la norma británica BS 7799. Esta norma internacional establece requisitos para que las organizaciones, implementen y mantengan un Sistema de Gestión de la Seguridad de la Información (SGSI). Los requisitos de la norma son genéricos y tienen como objetivo ser aplicables a todas las organizaciones. Cabe destacar que ISO/IEC 27001 es el único estándar de la familia ISO 27000 que se utiliza para certificar a las organizaciones, mientras que el resto de normas de esta familia brindan un apoyo sólido y profundo para que las empresas puedan construir e implementar su SGSI de forma adecuada y duradera [26].

Norma ISO/IEC 27002

Esta norma, formalmente conocida como Técnica de Seguridad o Código de Prácticas para Controles de Seguridad de la Información, fue diseñada de acuerdo a ISO para asistir a las organizaciones en las siguientes áreas, seleccionar controles dentro del proceso de implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001, implementar controles de seguridad de la información comúnmente aceptados y por último desarrollar sus propias guías de gestión de seguridad de la información. La estructura de los controles de seguridad de la información incluye 14 dominios, 35 objetivos de control y 114 controles, los cuales se encuentran divididos entre controles organizacionales, controles técnicos y controles normativos [19].

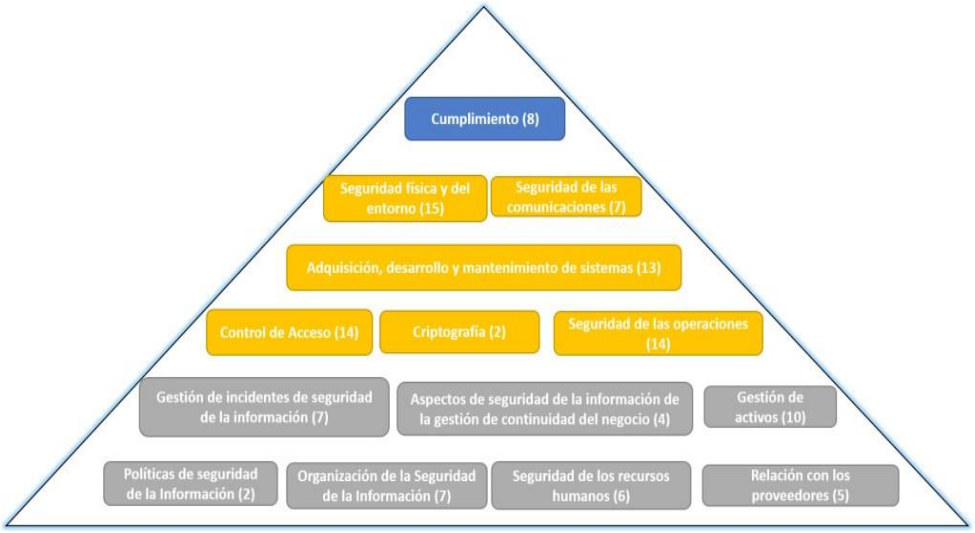

Figura 2. Estructura de los controles del anexo A 27002[19]

2.4 Requerimientos

En el contexto de una investigación, los requerimientos se refieren a las necesidades y funciones específicas que el proyecto debe cumplir para lograr sus objetivos. A continuación, se presenta una lista de los principales requerimientos que se necesita para la elaboración de la guía resultante del trabajo:

- Objetivos del Proyecto.
- Modalidad de Investigación.
- Metodología del Proyecto.
- Población y Muestra.
- Métodos para la Recolección de Datos.
- Análisis de Datos.
- Alcance del SGSI.
- Políticas de Seguridad de la Información.
- Metodología de Gestión de Riesgos.
- Resultados de evaluación de riesgos de seguridad de la información.
- Evidencia del monitoreo y análisis de vulnerabilidades.

En base al anexo A de la norma ISO 27002, donde se verifica los controles que son aplicables al contexto de la organización, existen otros requerimientos que se muestran, a continuación:

- Inventario de Activos.
- Política para el uso aceptable de activos.
- Política de control de acceso.
- Política para el control Criptográfico
- Registros de actividades del usuario.

2.5 Técnicas e instrumentos de recolección de información

Las técnicas cuantitativas y cualitativas son dos enfoques diferentes a la hora de levantar información. Las cuantitativas tiene como objetivo la medición y cuantificación de variables, también emplea métodos estadísticos para el análisis de datos. Mientras que las técnicas cualitativas se basan en datos no necesariamente numéricos, aquí se utilizan descripciones y observaciones, los métodos tradicionales son las entrevistas, observación participante y análisis de contenido [27].

Este proyecto utiliza una investigación mixta, ya que se usa la técnica cuantitativa y cualitativa, entrevistas para saber cómo funcionan ciertos procesos relacionados con la seguridad de la información y encuestas para evaluar que todas las respuestas estén acordes a los resultados esperados, aplicando la norma ISO 27001. (Véase el formulario de la entrevista y la encuesta en el anexo 2)

2.6 Modalidad de Investigación

Según el libro tecnológico RECIMUNDO en el artículo de 'Metodologías de la Investigación', nos dice que la investigación experimental implica exponer a un objeto o conjunto de individuos a ciertos estímulos, condiciones o tratamientos (variable independiente), para observar los efectos que se producen (variable dependiente). En el enfoque el investigador maneja una o más variables de estudio, para controlar el aumento o disminución de dichas variables y su efecto en los procedimientos observados [28].

El trabajo se desarrolló con la metodología experimental, debido a que aborda aspectos importantes para la elaboración de la guía del SGSI, tales como validación de controles de seguridad, políticas de acceso, controles de seguridad de la información, entre otros. Dichas políticas fueron validadas de forma experimental

para garantizar su eficacia en la protección de la información. También se hacen uso de instrumentos de recolección de información, para saber el contexto de la organización y el estado actual del departamento de Sistemas.

Según Esteban Nicomedes en su artículo 'Tipos de Investigación', la investigación explicativa es un enfoque de segundo nivel, cuyo objetivo principal es la verificación de hipótesis explicativas. Esta investigación comprueba sus hipótesis, a través de diseños no experimentales y experimentales. La formulación de hipótesis es fundamental, ya que orienta el camino a seguir dentro de la investigación [29].

Dentro del proyecto se utilizó un enfoque Explicativo, debido a que se identificó factores de riesgo, verificación de actualizaciones de software, falta de capacitación del personal, gestión de activos informáticos, control de procedimientos, análisis de incidentes de seguridad, entre otros. El enfoque explicativo busca comprender las causas de estos incidentes, por último, se realizó un análisis detallado para identificar fallos en los controles de seguridad y errores humanos que contribuyen al incidente.

2.7 Población y Muestra

La población que se considera dentro del proyecto es el siguiente:

Población	Número
Jefe del departamento de Sistemas	1
Programador de Sistemas	3
Bases de Datos	3
Soporte técnico	4
Total	**11**

Tabla 2. Población y Muestra

No se utilizó una muestra debido a que todas las herramientas y encuestas utilizadas para levantar información, se dirigió a quienes trabajan en el departamento de Sistemas de la organización, abarcando el 100% de la población.

2.8 Procesamiento de la evaluación: Validez y confiabilidad de los instrumentos aplicados para el levantamiento de información

Para la validación de los instrumentos de levantamiento y recolección de información, se utilizó el juicio de expertos. Se solicitó la ayuda de una docente de la Universidad UPSE, experta en el tema de Gestión de Tecnologías de la Información, la Ingeniera Marjorie Coronel. Ella colaboró con las debidas correcciones a las entrevistas y encuestas para tener una mayor confiabilidad de los instrumentos utilizados. Además, se solicitaron sus consejos en caso de que faltaran preguntas que puedan contribuir al desarrollo de la investigación.

2.9 Análisis de Datos

La información obtenida se interpretó, para presentar los resultados en gráfico y porcentajes, los cuales fueron de ayuda para resolver la problemática del proyecto. Se realizaron los siguientes procedimientos:

- Elaboración de instrumentos de recolección de información validados por el juicio de expertos en el tema propuesto.
- Tabulación de la información obtenida, para la presentación de los resultados de forma estadística.
- Análisis e interpretación de resultados.

2.10 Desarrollo de la Propuesta

Para el desarrollo de la metodología de gestión de seguridad de la información del SGSI, se utilizó la metodología del ciclo de Deming, también conocida como ciclo continuo (PDCA), sirve para la gestión de la calidad y mejora continua de procesos, sistemas y productos. Fue desarrollado por el estadístico W. Edwards Deming, esta metodología cuenta con 4 fases que serán detalladas a continuación [17]:

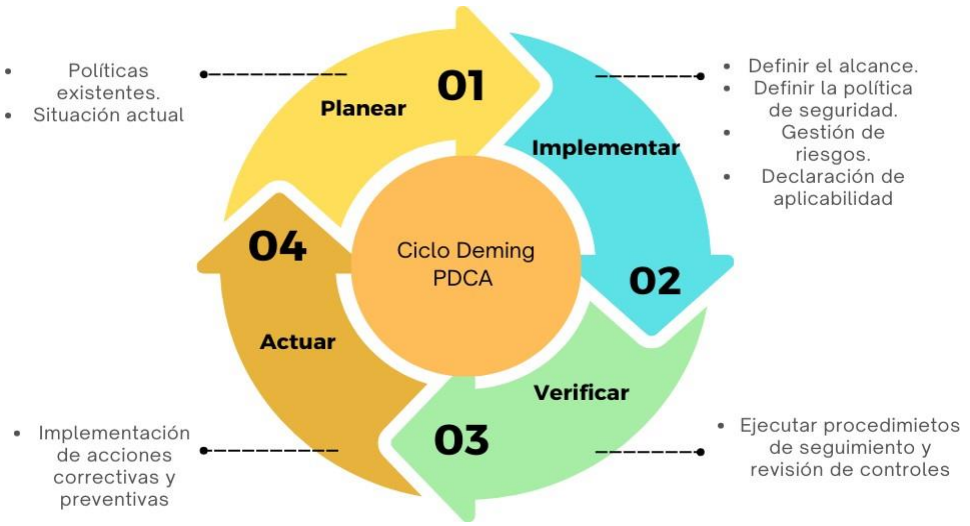

Figura 3. Ciclo PDCA para implementación de SGSI [30]

FASE 1: PLANIFICAR

Esta etapa implica verificar el contexto de la organización y sus respectivas políticas, objetivos y procesos relacionados con la gestión de riesgos y la mejora de la seguridad de la información, con el fin de proporcionar los resultados esperados alineados con los objetivos de la organización, uso de herramientas de software libre para realizar el análisis de vulnerabilidades a los sistemas o estructuras tecnológicas e identificar los posibles riesgos y amenazas. Esta fase se puede encontrar en las cláusulas 4, 5 y 6 de la norma ISO 27001, que se refieren al contexto de la organización, liderazgo y la planificación [2].

FASE 2: IMPLEMENTAR

Aquí se utilizó la información recopilada en la primera fase, se tomaron acciones para aplicar las políticas y objetivos de seguridad de la información, diseñar y definir el alcance del Sistema de Gestión de Seguridad de la Información, por último, se estableció una metodología para la gestión de riesgos y control de incidentes de seguridad y de esta forma controlar los activos de información y recursos informáticos [31].

FASE 3 VERIFICAR

Dentro de esta fase se analizaron los resultados y se definieron donde son aplicables los procesos relacionados con la Política del Sistema de Gestión de Seguridad de la Información, desarrollo de documentación para los controles ISO e informar los resultados a la administración para su revisión. Además de ejecutar procedimientos de seguimiento y revisión de controles [30].

FASE 4 ACTUAR

Establecer mejoras continuas en el SGSI a través de medidas correctivas y preventivas, derivadas de los hallazgos de la auditoría interna y la revisión de la gerencia, u otra información pertinente [18]. Finalmente, se elaboraron políticas enbase a la información recolectada e implementación de nuevas mejoras basadas en las buenas prácticas de la norma ISO 27001. Realizar los informes correspondientes del proceso completo y comunicarlos a la gerencia del departamento.

Herramientas utilizadas dentro del proyecto:

- **NMAP:** Software de código abierto, utilizado para el escaneo de redes y puertos con el objetivo de obtener información sobre la red y controlar la seguridad [32].
- **NEXPOSE:** Herramienta para evaluar vulnerabilidades de seguridad, validación de hallazgos y la planificación de acciones correctivas. Incorpora estándares clave de gestión de riesgos y configuración, como PCI DSS, NERC CIP y FISMA, entre otros [33].
- **KALI LINUX:** Distribución de Linux basada en Debian, preparada para realizar ataques de seguridad, realizar análisis de red, recopilación de información, entre otras funciones [34].
- **VIRTUAL BOX:** Emulador de sistemas operativos. Se caracteriza por utilizar los recursos del mismo computador o Hardware. Sirve para trabajar desde el mismo sistema operativo y probar en un equipo virtual otro sistema operativo [35].

2.10.1 Desarrollo de Planificación

Para la fase de planificación es importante analizar el contexto de la organización y verificar que existan políticas relacionadas con la seguridad de la información del departamento, para ello se procedió a realizar el levantamiento de información respectivo con las técnicas o instrumentos de recolección de información seleccionados, como las encuestas y entrevista al personal, además se determinaron los riesgos existentes informáticos existentes del Departamento de sistemas mediante un análisis de vulnerabilidades. Información relevante de la empresa, estructura organizacional, objetivos departamentales y el contexto de la organización, se encuentra establecido en el marco contextual del trabajo.

2.10.1.1 Determinación de riesgos informáticos en el departamento de Sistemas del GAD-LIBERTAD

Resultados de la Entrevista

El objetivo de la entrevista radica en verificar el grado de conocimiento y cumplimiento de las políticas de seguridad de la información por parte del personal del departamento de Sistemas. Una vez realizada la entrevista a la jefa del departamento se obtuvieron los siguientes resultados:

Preguntas para el encuestado	Respuestas
1. ¿Existen políticas que gestionen la seguridad de la información actualmente?	Existen políticas, pero solo son verbales. Restricción de AnyDesk, restricción de ancho de banda, restricción de redes inalámbricas, restricción de páginas, restricción al servicio de internet.
2. ¿Se presentan riesgos informáticos en la empresa y cuál es el más constante?	Pérdida de información, ya que actualmente recién se están implementando servidores nuevos y

	están en proceso de migración, y el otro riesgo es que tenemos un UPS de 10 KVA y con los apagones se pueden quemar.
3. ¿Los usuarios se encuentran capacitados para el uso de los recursos tecnológicos?	Sí.
4. ¿Los sistemas informáticos han sido víctimas de robo de información?	No.
5. ¿Existen controles sobre el acceso al personal interno y externo al equipamiento y sistemas que maneja dentro de la institución?	Sí.
6. ¿Cuál es el proceso que se lleva a cabo para la gestión y administración de los activos informáticos de la empresa?	A través de los inventarios se hace seguimiento a los activos del GAD Municipal.
7. ¿Se realizan tareas de monitoreo a los sistemas de información con los empleados del departamento?	Sí.
8. ¿Usted conoce acerca de algún Sistema de Gestión de Seguridad de la Información (SGSI)?	Solo se escucha de una ordenanza que quieren aprobar. Ordenanza que regula la protección de datos de los GAD, pero debe ser específico porque hay muchas opciones para seguridad de la información.
9. ¿Cree usted que se debería realizar una Auditoría Informática dentro del departamento de TI?	Sí.

Tabla 3. Formulario Entrevista

Conclusiones de la entrevista

Pregunta 1: Se pudo determinar que existen políticas de seguridad de información que ellos manejan, sin embargo, dichas políticas se transmiten verbalmente, no existe una documentación específica que determine reglas o procedimientos que debe tomar el personal del departamento en caso de un problema. Adicionalmente no todo el personal, está enterado de que existen dichas políticas debido a la falta de comunicación y conocimiento.

Pregunta 2: La pérdida de información es uno de los riesgos informáticos más comunes que se dan con regularidad en el departamento de Sistemas, esto puede llevar a que se realicen ataques informáticos y llegue a sufrir graves consecuencias. Otro riesgo mencionado es el UPS de 10 KVA, por motivo de los apagones a nivel nacional, puede quemarse y tener pérdidas económicas y de información.

Pregunta 3: Los empleados que trabajan en departamento de Sistemas se encuentran capacitados y con el conocimiento necesario para trabajar con los recursos tecnológicos y resolver problemas de tipo de informático.

Pregunta 4: Los sistemas informáticos no han sufrido robo de información, dando a entender que los procesos realizados para la seguridad de la información están teniendo un impacto positivo al departamento de Sistemas.

Pregunta 5: El departamento cuenta con un control de acceso a personas que manejan los servidores dentro de la institución.

Pregunta 6: Se evidencia que también se realizan inventarios para el control de activos informáticos. Sin embargo, no se establece una metodología para la gestión de riesgos relacionados con los activos.

Pregunta 7: Cada cierto tiempo se realizan tareas de monitoreo a los sistemas que maneja el departamento. Previniendo así filtraciones o pérdida de información.

Pregunta 8: Se tiene conocimiento que la alta gerencia está en proceso de implementar un SGSI, mas no está establecido por completo, ya que existen diferentes alternativas que se están analizando.

Pregunta 9: Existe una postura positiva por la alta gerencia del departamento de sistemas, de solicitar o requerir la implementación de un SGSI.

Resultados de la Encuesta

Aplicada la encuesta a los 11 empleados del departamento de Sistemas, se obtuvieron los siguientes resultados y respuestas:

Pregunta 1: ¿Con que políticas de seguridad para la gestión de la información cuenta actualmente el departamento de Sistemas?

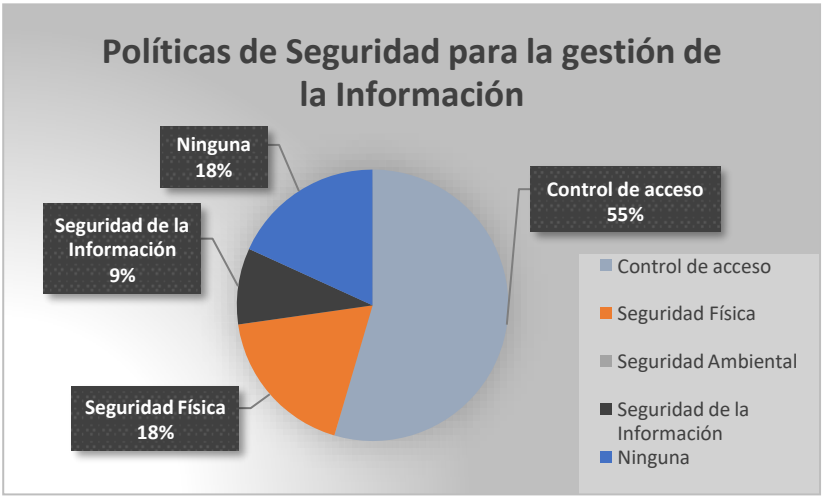

Figura 4. Políticas de Seguridad

Análisis e interpretación de resultados:

Según los resultados presentado en la Figura 2, se determina que el 55% de los encuestados señalan que existen políticas de control de acceso, el 18% afirma que existen de Seguridad Física, otro 18% señala que no existe ninguna política establecida y el 9% un porcentaje mínimo que existe una política de seguridad de la información.

Pregunta 2: ¿Se aplica algún proceso o técnica de seguridad para el cuidado y uso de la información?

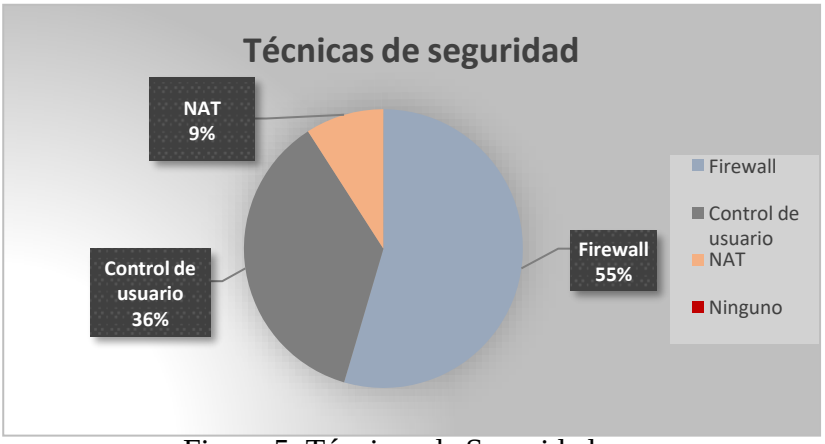

Figura 5. Técnicas de Seguridad

Análisis e Interpretación de resultados:

En la pregunta relacionada a las técnicas de seguridad, el 55% de los encuestados señalan que existen técnicas de seguridad como Firewall, el 36% afirma que presentan el control de usuario, y un 9% señala que una técnica utilizada es el NAT. Lo que demuestra que existe cierto control para el manejo de la información.

Pregunta 3: ¿Se presentan problemas en los equipos de cómputo de la entidad, que conlleven a la pérdida de la información?

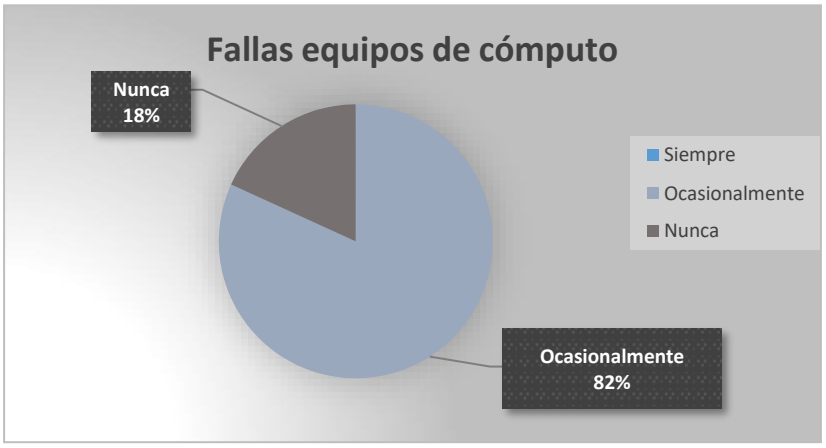

Figura 6. Fallas equipos de cómputo

Análisis e Interpretación de resultados:

Según los resultados de la pregunta 3, un 82% de los encuestados indican que Ocasionalmente se dan fallos en los equipos de cómputo, de la misma forma un 18% señala que no existen fallas nunca y no han presentado problemas como

pérdida de información, demostrando que los equipos regularmente tienen problemas y fallas.

Pregunta 4: ¿Cada que tiempo se realizan mantenimientos de tipo preventivo y correctivo de los equipos informáticos de la empresa?

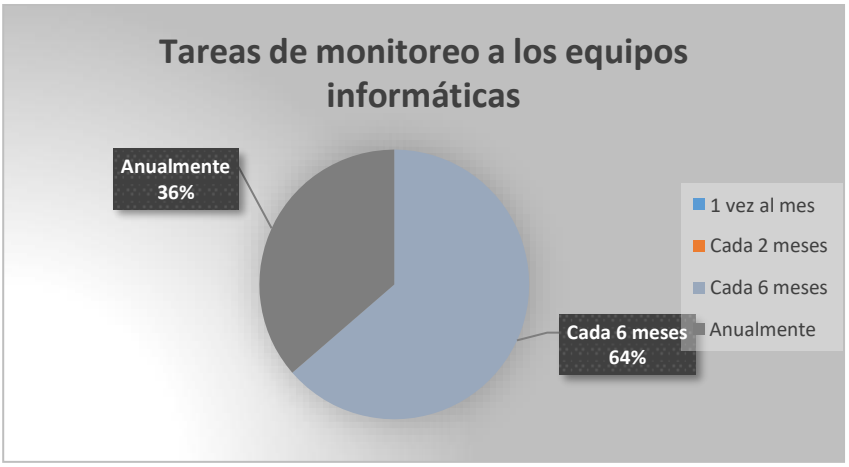

Figura 7. Tareas de monitoreo a equipos informáticos

Análisis e Interpretación de resultados:

De acuerdo a los resultados de la pregunta 4, el 64% de los encuestados afirman que se realizan tareas de monitoreo cada 6 meses, mientras que el 36% afirma que dichas tareas se realizan cada año. Demostrando que existen problemas regularmente con los equipos, debido a que no se les da el mantenimiento adecuado.

Pregunta 5: ¿Se lleva un control adecuado para el inventario de activos informáticos del departamento?

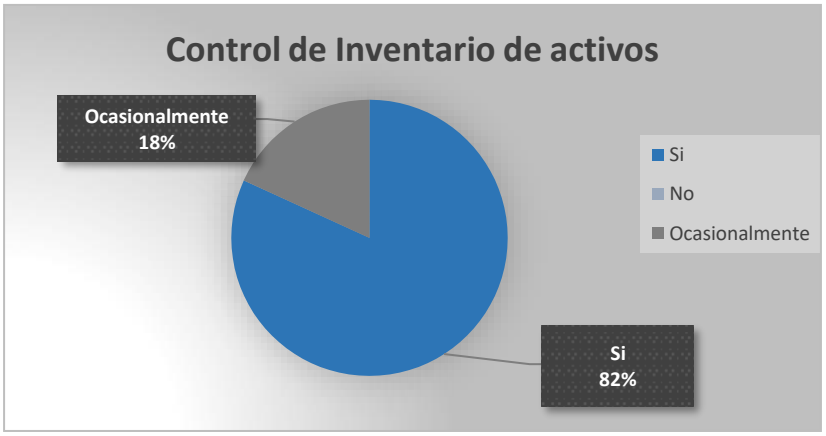

Figura 8. Control de Inventario

Análisis e Interpretación de resultados:

Los resultados obtenidos de la pregunta 5, el 82% de los encuestados mencionan que existe un control para el inventario de activos informáticos, y un 18% señala que Ocasionalmente se hace control de inventarios. Dando a conocer que tienen existen ciertos procedimientos para el uso de los activos informáticos.

Pregunta 6: ¿Se realizan tareas de monitoreo a los sistemas de información en conjunto con los empleados?

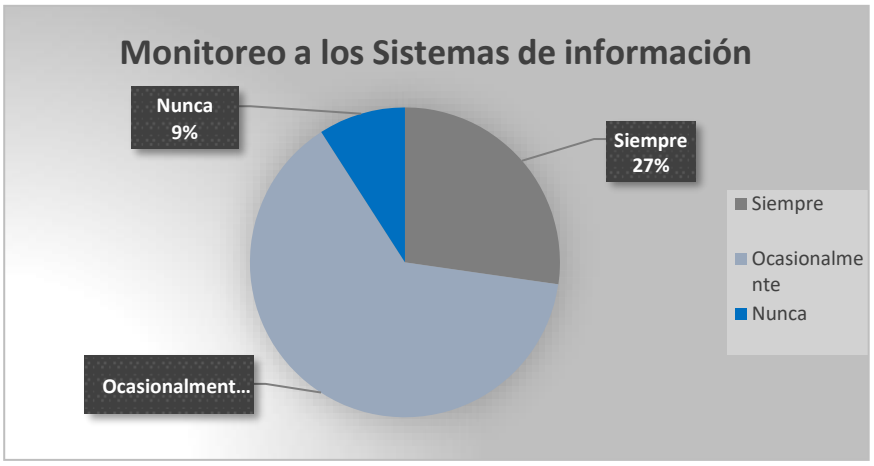

Figura 9. Monitoreo de Sistemas de Información

Análisis e Interpretación de resultados:

En los resultados de la pregunta 6, el 64% de los encuestados afirman que Ocasionalmente se realizan tareas de monitoreo a los sistemas de información, el 27% que siempre se realizan monitoreos en conjunto con los empleados, y un 9% que nunca se revisan los sistemas de información. Dando a conocer que no existe un proceso claro para los empleados, de revisar y monitorear los sistemas que maneja el departamento de Sistemas.

Pregunta 7: ¿Los sistemas informáticos que maneja la entidad presentan fallos o irregularidades?

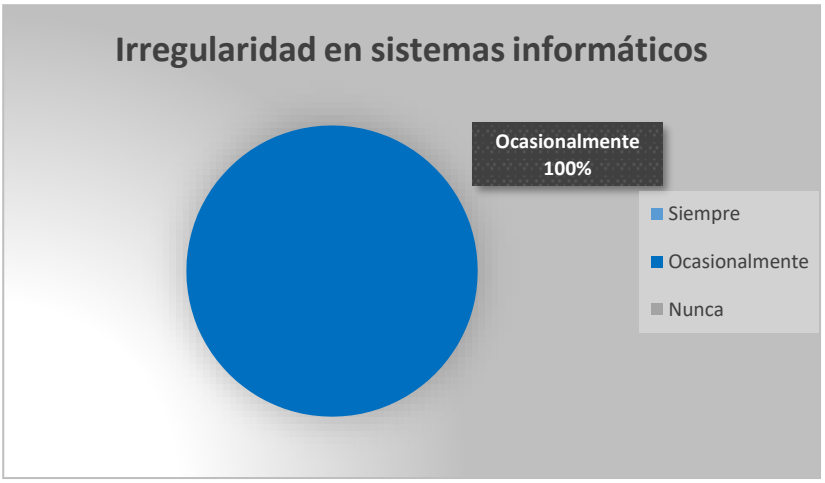

Figura 10. Fallos en los Sistemas Informáticos

Análisis e Interpretación de resultados:

Según los resultados de la pregunta 7, el 100% de los encuestados presentan regularmente problemas o fallos en los sistemas informáticos que maneja el departamento de Sistemas. Esto puede llevar a tener consecuencias con la información procesada.

Pregunta 8: ¿Cuál es el nivel de conocimiento en seguridad de la información del personal en el departamento de Sistemas?

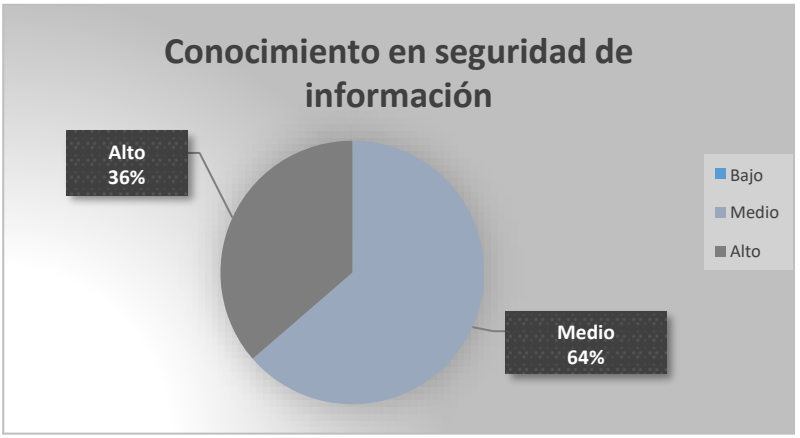

Figura 11. Conocimiento en Seguridad de la Información

Análisis e Interpretación de resultados:

En la pregunta 8, el 64% de los encuestados señalan que el nivel de conocimiento de los empleados en seguridad de la información es medio, y el 36% afirma que el conocimiento es alto, dando a entender que el personal está capacitado para trabajar y dar solución a problemas presentados en el área informática.

Pregunta 9: ¿Cada que tiempo se realizan backups o copias de seguridad de la información?

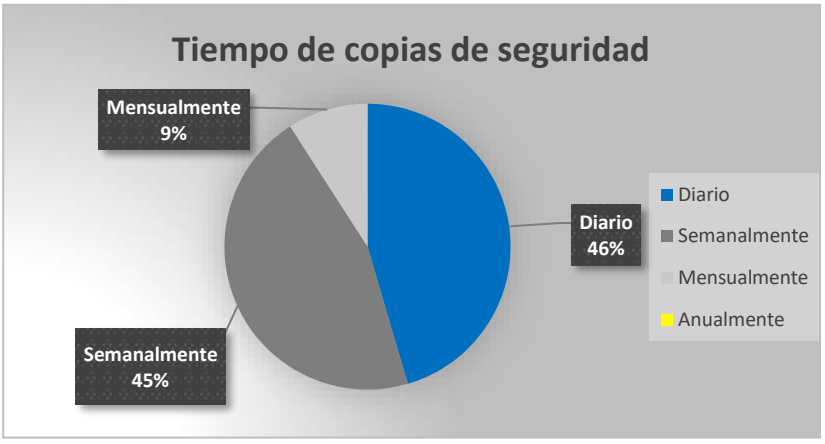

Figura 12. Tiempo de Copias de Seguridad

Análisis e Interpretación de resultados:

Según los resultados de la pregunta 9, el 46% de los encuestados afirma que se realizan copias de seguridad diario, así mismo, un 45% señala se realizan backups Semanalmente, y por último un 9% indica que se realizan copias o respaldos cada mes. Evidenciando que hay porcentajes divididos y no se sabe con certeza el tiempo establecido para las copias de seguridad, o si se realizan cuando se las requieran.

Pregunta 10: ¿Existen fallos en las redes de internet durante la transmisión de datos?

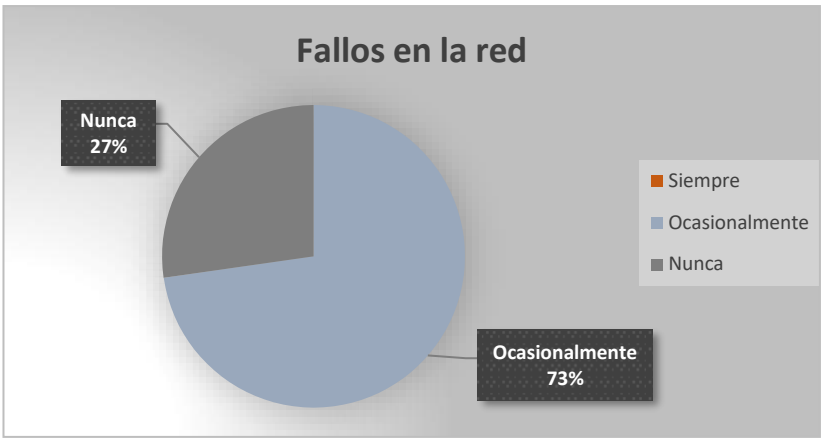

Figura 13. Fallos en la red

Análisis e Interpretación de resultados:

Dentro de la pregunta 10, el 73% de los encuestados afirman que se dan problemas en la red con regularidad, y el 27% que nunca han tenido problemas de red o para la transmisión de datos, evidenciando que existen problemas con el internet dentro del departamento ya que regularmente hay fallos y del mismo modo pueden existir problemas con el servidor.

Pregunta 11: ¿Con que frecuencia se actualizan los Sistemas Operativos y las aplicaciones?

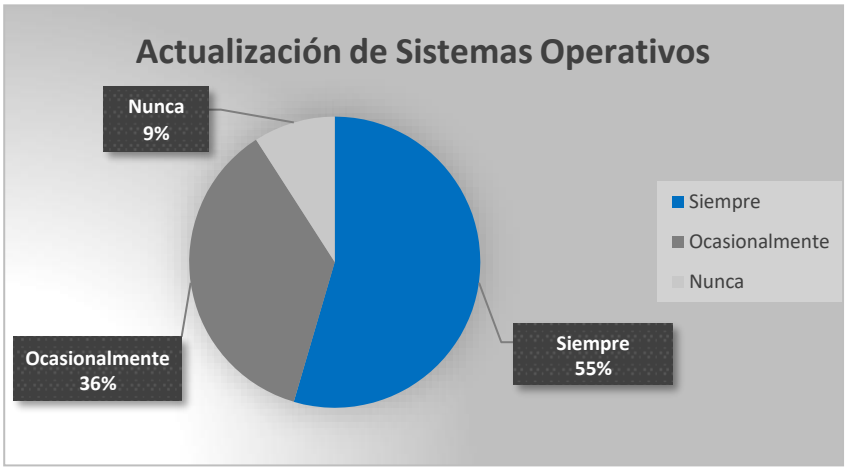

Figura 14. Actualización de Sistemas Operativos

Análisis e Interpretación de resultados:

De acuerdo a los resultados de la pregunta 11, un 55% de los encuestados indica que se actualizan los Sistemas Operativos siempre, un 36% señala que ocasionalmente se actualizan los sistemas operativos, y un 9% que nunca se actualizan los sistemas utilizados. Lo que manifiesta que equipos pueden presentar fallas o estar expuestos a vulnerabilidades.

2.10.1.2 Áreas o Controles establecidos por el Anexo A Norma ISO 27002

La norma ISO/IEC 27002 establece un conjunto de buenas prácticas que son aplicables a empresas o entidades que requieren garantizar la protección de los activos informáticos o establecer políticas de seguridad de la información. Los controles establecidos en el anexo A son los siguientes:

- A.5 Política de seguridad de la información.
- A.6 Organización de la seguridad de la información.
- A.7 Seguridad relativa a recursos humanos.
- A.8 Gestión de activos.
- A.9 Control de acceso.
- A.10 Criptografía.
- A.11 Seguridad Física y del entorno.
- A.12 Seguridad de las operaciones.
- A.13 Seguridad en las comunicaciones.
- A.14 Adquisición, desarrollo y Mantenimiento de los sistemas de información.
- A.15 Relaciones con proveedores.
- A.16 Gestión de Incidentes de seguridad de la información.
- A.17 Aspectos de Seguridad de la información para la Gestión de la continuidad del negocio.
- A.18 Cumplimiento.

A.5 Política de Seguridad de la Información

Estas normas se han creado como recursos formales con el objetivo de sensibilizar a cada uno de los miembros de una empresa sobre la relevancia de la información presente en los servicios esenciales, de modo que adquieran conocimientos sobre cómo desempeñar sus tareas de acuerdo con las pautas establecidas en dichas normas [36].

A.6 Organización de la Seguridad de la Información

En este apartado se gestiona la protección de la información dentro de la organización. En caso de ser necesario, buscar apoyo de expertos consultores en seguridad de la información. Además, determinar y asignar responsabilidades dentro de la organización y mantener comunicación con terceros, grupos externos y partes interesadas [37].

A.7 Seguridad Relativa a Recursos Humanos

Este control sirve para implementar acciones preventivas y evitar riesgos asociados con el uso inadecuado de los recursos informáticos. Las responsabilidades en materia de seguridad de la información deben quedar claramente establecidas en los términos y condiciones del contrato, y deben ser aceptadas por el candidato. Se toma como referencia la norma ISO/IEC 27001, que permite a las organizaciones incluir criterios de seguridad de la información en la gestión de Recursos Humanos, se identifican tres momentos clave durante la permanencia de los trabajadores en una organización: antes, durante y después de finalizar el empleo o cambiar de puesto de trabajo [38].

A.8 Gestión de Activos

Este control se refiere a la identificación de activos de información de la organización y la aplicación de controles para protegerlos adecuadamente. Esto incluye la clasificación de los activos de información según nivel de riesgo, alto, medio o bajo, la asignación de responsabilidades para su manejo y protección, y el mantenimiento de un inventario actualizado de activos de información.

A.9 Control de Acceso

El objetivo principal es garantizar que el acceso a los activos de información esté controlado y gestionado de manera adecuada. Incluye la implementación de controles de acceso físico, la asignación de derechos de acceso según la necesidad de cada usuario, la autenticación segura de usuarios y la gestión de privilegios.

A.10 Criptografía

Este control protege la información confidencial mediante la encriptación, asegurando que solo las personas autorizadas puedan acceder a ella y que los datos no sufran alteraciones. Ayuda a las organizaciones a cumplir con requisitos legales y regulatorios, y reduce los riesgos de seguridad asociados con la pérdida, robo o acceso no autorizado a la información sensible. Los dispositivos tecnológicos deben contar con una unidad central de datos protegida mediante codificación. Es fundamental establecer una normativa sobre la utilización de firmas digitales [39].

A.11 Seguridad Física y del Entorno

Se refiere a la protección de los activos de información física y la creación de un entorno seguro para su procesamiento. Para evitar el acceso no autorizado, el daño y la interferencia en las instalaciones y la información de la empresa, se implementan medidas de seguridad [40]. Estas medidas buscan proteger los activos y garantizar la integridad de los datos, previniendo actos maliciosos que puedan afectar el funcionamiento normal del negocio. Esto implica la implementación de controles físicos, como sistemas de acceso, cerraduras, sistemas de detección de intrusos, y la protección contra amenazas ambientales como incendios, inundaciones, etc.

A.12 Seguridad de las Operaciones

Establecer medidas y procedimientos para gestionar las actividades diarias dentro de una organización. Su propósito es garantizar que las operaciones administrativas y operacionales se lleven a cabo de manera segura, minimizando los riesgos de seguridad de la información. Incluye aspectos como la gestión de cambios, la gestión de la capacidad, la protección contra malware, la realización de copias de seguridad, la gestión de vulnerabilidades técnicas y la supervisión de los sistemas.

Al implementar estos controles, las organizaciones pueden actuar rápidamente a incidentes de seguridad, mantener la integridad y disponibilidad de los sistemas, y asegurar que las operaciones se realicen de acuerdo con las políticas de seguridad establecidas.

A.13 Seguridad de las Comunicaciones

El enfoque es proteger la información que se comparte dentro y fuera de la organización para mantener su confidencialidad, integridad y disponibilidad. El objetivo es garantizar que las comunicaciones sean seguras, tanto internas como externas, y que la información no sea accesible a terceras personas, durante su transmisión.

A.14 Adquisición, desarrollo y Mantenimiento de los Sistemas de Información

Este control prioriza asegurar la seguridad de los sistemas de información desde su creación hasta su mantenimiento. Su objetivo es integrar la seguridad en cada etapa del ciclo de vida de los sistemas, reduciendo los riesgos y protegiendo los datos. Aquí se presentan medidas y procedimientos para adquirir software y hardware de manera segura, crear aplicaciones seguras y mantener los sistemas de información de forma constante.

A.15 Relaciones con proveedores

El objetivo es proteger los recursos y la información de la organización al interactuar con proveedores y terceros. Es importante que los proveedores cumplan con los requisitos de seguridad establecidos por la organización, minimizando los riesgos asociados con la externalización de servicios y la colaboración con terceros. Cuando se establecen acuerdos con proveedores, contratistas o subcontratistas, se consideran controles clave para garantizar la seguridad y el acceso a los terminales y activos críticos de la organización. Además, se aplican los controles del Anexo A de la norma ISO/IEC 27001 para asegurar que tanto el proveedor como la organización utilicen los mismos protocolos de seguridad [41].

A.16 Gestión de Incidentes de Seguridad de la Información

Se refiere a la preparación y respuesta a incidentes de seguridad de la información. Esto incluye la creación de un plan de gestión de incidentes, la designación de un equipo de respuesta a incidentes, la definición de procedimientos para la notificación y manejo de incidentes. En caso de situaciones que demanden una respuesta rápida y efectiva, como la adecuada gestión de la continuidad empresarial, los incidentes de seguridad, el cumplimiento normativo y la externalización de la cadena de suministro, la comunicación apropiada con los medios internos y externos se vuelve fundamental. Esto permite evitar o, al menos, minimizar el impacto en la imagen de la empresa ante posibles situaciones de crisis [42].

A.17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio

Establecer un sistema de gestión dentro de la empresa que asegure la continuidad de las operaciones y atienda los requisitos de seguridad de la información requeridos para mantener la actividad comercial de la organización [43].

A.18 Cumplimiento

Esta sección ayuda a que la organización cumpla con todas las leyes, reglamentos y obligaciones relacionadas con la seguridad de la información. Su objetivo es asegurar que la organización no solo siga los requisitos legales, sino que también cumpla con sus propias políticas y estándares internos de seguridad.

También abarca la protección de los datos personales, además incluye la realización de auditorías internas, revisión constante de los controles y procedimientos de seguridad de la información. Al implementar estos controles, las organizaciones pueden evitar sanciones legales, proteger su reputación, y asegurarse de que sus prácticas de seguridad de la información sean sólidas y apropiadas.

2.10.1.3 Herramientas para la ejecución del análisis de vulnerabilidades

Para el escaneo de puertos, reconocimiento de información y análisis de vulnerabilidades se investigaron varias herramientas que podrían ser de utilidad para el proyecto. Se elaboró un cuadro comparativo mostrando características y especificaciones de cada una de ellas y así seleccionar la opción más óptima, de esta manera obtener resultados específicos en cada ámbito, entre las herramientas analizadas tenemos las siguientes:

Matriz de análisis de herramientas para la detección de vulnerabilidades

Herramientas	Open vas	Nexpose	Nessus
Costo	Libre	Libre y de paga	Paga
Plataforma	Windows/Linux	Windows/Linux	Windows/MAC/Linux
Funciones	• Escaneo concurrente de múltiples nodos. • Escaneo automático. temporizado • Servidor web integrado.	• Análisis en tiempo real de los hosts. • Controles, configuración y permisos de acceso • Escaneo de redes • Rastreo de sitios web	• Resultado de análisis en tiempo real. • Generación de archivos .nessus usados para productos de tenable como estándar para directivas de análisis de datos[44].

Tabla 4. Cuadro comparativo de herramientas de detección de vulnerabilidades

De acuerdo a las opciones analizadas, se concluyó que la herramienta Nexpose es la mejor opción para realizar el análisis de vulnerabilidades, ya que es una herramienta que permite trabajar con su versión libre y es de fácil instalación dentro del sistema Windows. No se utilizó la herramienta OpenVAS debido a incompatibilidad de sistemas operativos y problemas con su instalación. Por ello la mejor opción fue trabajar con Nexpose, ya que es de fácil acceso e instalación en el sistema operativo de Windows.

Matriz de herramientas utilizadas para el monitoreo de puertos

Herramientas	**SuperScan4**	**Nmap**	**NetScan6**
Costo	Libre	Libre y de paga	Libre
Plataforma	Windows/Linux	Windows/MAC/Linux	Windows
Funciones	• Escaneo de puertos TCP, pruebas de ping, servicios específicos y puertos.	• Escaneo de servidores, puertos abiertos, servicios o aplicaciones en curso, IP o MAC	• Escaneo de puertos NetBIOS, direcciones IP y MAC, sistemas operativos, acceso a carpetas compartidas.

Usos	• Monitoreo de host y dominios, evaluación de seguridad de la red.	• Auditorías Informáticas de Red, pruebas y recolección de información para futuros ataques informáticos.	• Administración de red y recopilación de información.

Tabla 5. Cuadro comparativo de herramientas para monitoreo de puertos

Una vez analizadas las herramientas para el monitoreo de puertos, se utilizó la herramienta de Nmap específicamente su interfaz gráfica de Zenmap, esta es una herramienta mayormente utilizada para la realización de auditorías informáticas, dando como resultado la identificación de puertos abiertos y los servicios que están corriendo dentro de los mismos.

2.10.1.4 Ejecución de análisis de vulnerabilidades de los servidores

Para realizar el análisis de vulnerabilidades se solicitaron todos los servidores que forman parte del Data Center Municipal del GAD-LIBERTAD, se presenta una matriz detallada donde se describen las características y el sistema operativo que maneja cada servidor. Sin embargo, por motivos de confidencialidad y seguridad, no se dio acceso a la IP de todos los servidores, únicamente se escribió el nombre del servicio manejado, sistema operativo y su descripción.

Finalmente, se obtuvo acceso y permiso de la gerencia, para un servidor que estaba en circulación recientemente y realizar las pruebas respectivas, dejando en claro que este procedimiento debe realizarse para los demás servidores de la entidad y así obtener la certificación ISO 27001. La lista de servidores se detalla a continuación:

N°	Dirección IP	Nombre	Sistema Operativo	Descripción
1	192.168.-----	HP Proliant DL560 Gen10	Proxmox 3.3-1	- Página web - DNS CNT - Firewall – Squid CNT
2	192.168.------	IBM System x3200 M2	Centos 5	- Oracle Application Server
3	120.40.69.244	Servidor Secundario	Ubuntu Linux	-Procesos nuevos, servicio de DNS name
4	192.168.------	IBM System x3650	Windows 2003 Server	- Sitac Electrónico - Cartografía AutoCad - Sistema de Contabilidad Oracle Forms
5	192.168.------	Iomega 450 R	Centos 6.5	- Base de Datos - Sitac Electrónico - Carpeta Inspectores
6	192.168.------	Clon	Proxmox 7.1-7	- DNS- Telconet - Firewall Squid Telconet

N°	Dirección IP	Nombre	Sistema Operativo	Descripción
7	192.168.------	Clon	Proxmox 7.1-7	- ERP-GUI-Todotek - Pagina web (Desarrollo y Pruebas)
8	192.168.------	Clon	Proxmox 3.3-1	- Oracle Aplicación Desarrollo - Oracle Data Base Desarrollo
9	192.168.------	Clon	Centos 7	- Carpetas compartidas

Tabla 6. Matriz de listado de Servidores de la entidad

2.10.1.5 Escaneo de Puertos y Servicios

Se realizó una exploración para reconocer los puertos abiertos y el servicio que corren dentro de los mismos, mediante la herramienta de Zenmap el cual es la interfaz gráfica de Nmap, a continuación, se muestran los resultados:

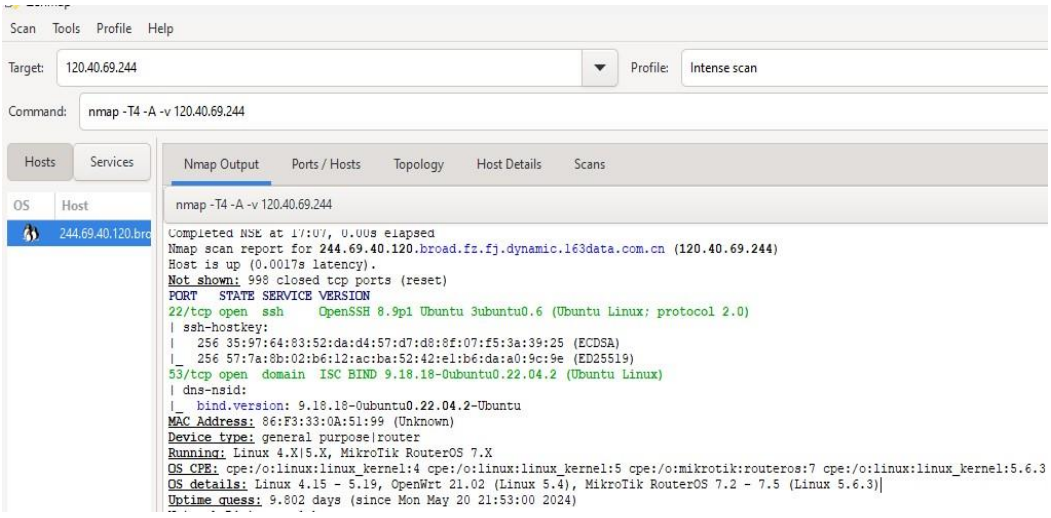

Figura 15. Nmap a 120.40.69.244

Puerto	Protocolo	Estado	Servicio	Detalle
22	tcp	Abierto	ssh	OpenSSH 8.9p1 Ubuntu 3ubuntu0.6 (Ubuntu Linux)
53	tcp	Abierto	Domain (DNS)	ISC BIND 9.18.18-0Ubuntu0.22 (Ubuntu Linux)

Tabla 7. Matriz de resultados de escaneo Nmap

Dentro de este reconocimiento, se pudo observar que se encuentran 2 puertos abiertos, el puerto 22 y 53, además se verificó que se encuentra activo el servicio (ssh) el cual es un mecanismo para autenticar a un usuario remoto, transferir entradas del cliente al host y viceversa. También observamos el servicio (DNS) Sistema de nombres de dominio y por último se obtuvo la versión, el cual es un Open SSH Ubuntu en el puerto 22 y ISC BIND (Ubuntu Linux). Como datos adicionales nos muestra el tipo de dispositivo y la distancia de la red.

2.10.1.6 Análisis de vulnerabilidades con Nexpose

A continuación, se utilizó la herramienta Nexpose el cual es un programa informático que ayuda a detectar, analizar y controlar los puntos débiles en una red, ofreciendo una visión general del estado de seguridad de una organización. Realizar la exploración de vulnerabilidades con Nexpose es fundamental para encontrar posibles fallas en el entorno tecnológico que podrían ser aprovechadas por intrusos.

Este análisis de vulnerabilidades debe ser realizado a todos los servidores que posee la entidad para la debida toma de decisiones entorno a los riesgos encontrados, sin embargo, por motivos de confidencialidad y privacidad el departamento solo se tuvo acceso a un servidor nuevo que estaba recientemente en circulación, de igual forma sirvió como punto de partida para realizar el respectivo análisis:

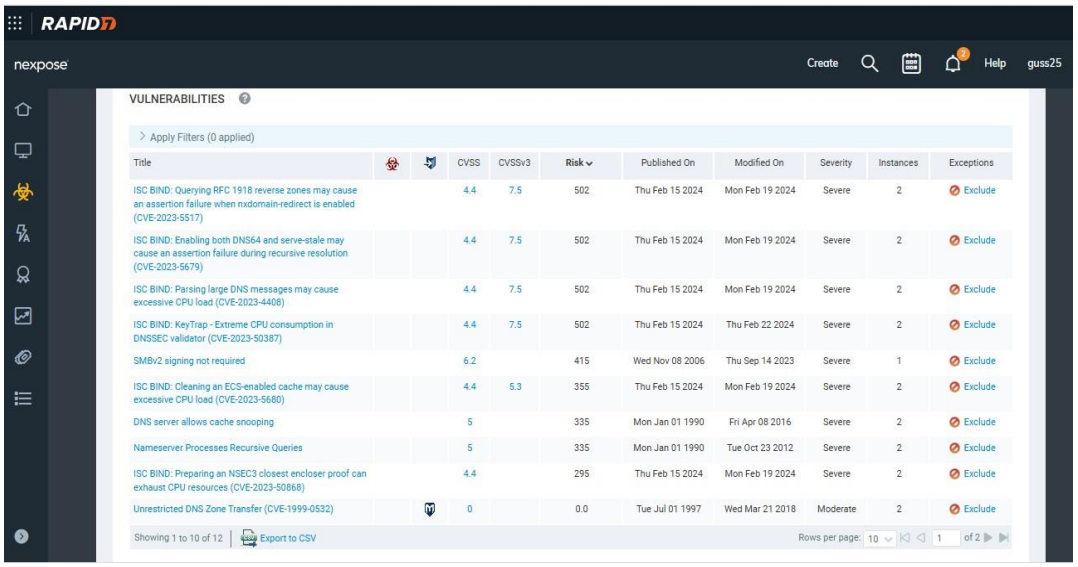

Figura 16. Vulnerabilidades encontradas con Nexpose en el servidor

Para la observación más detallada del análisis de vulnerabilidades, se elaboró una matriz donde se encuentra información resumida de los resultados obtenidos, la matriz se presenta a continuación:

Servidor Secundario

Servicio	Vulnerabilidad	Riesgo	Observación
53/tcp	ISC BIND: La consulta de zonas inversas RFC 1918 puede provocar un error de aserción cuando nxdomain-redirect está habilitado (CVE-2023-5517).	**Medio**	Un error en el código de control de consultas puede hacer que 'named' se cierre prematuramente con un error de aserción cuando: - 'nxdomain-redirect <domain>;' está configurado, y- el solucionador recibe una consulta PTR para una dirección RFC 1918 que normalmente daría como resultado una respuesta NXDOMAIN autoritativa. Este problema afecta a las versiones 9.12.0 a 9.16.45, 9.18.0 a 9.18.21

Servicio	Vulnerabilidad	Riesgo	Observación
53/tcp – 53/udp	ISC BIND: La habilitación de DNS64 y la obsolescencia de servicio puede provocar un error de aserción durante la resolución recursiva (CVE-2023-5679).	**Alto**	Una mala interacción entre DNS64 y serve-stale puede hacer que 'named' se bloquee con un error de aserción durante la resolución recursiva, cuando ambas características están habilitadas. Este problema afecta a las versiones 9.16.12 a 9.16.45, 9.18.0 a 9.18.21,
53/tcp – 53/udp	ISC BIND: El análisis de mensajes DNS de gran tamaño puede provocar una carga excesiva de CPU (CVE-2023-4408).	**Alto**	El código de análisis de mensajes DNS en 'named' incluye una sección cuya complejidad computacional es demasiado alta. No causa problemas para el tráfico DNS típico, pero las consultas y respuestas elaboradas pueden causar una carga excesiva de CPU en la instancia "nombrada" afectada al explotar esta falla. Este problema afecta tanto a los servidores autoritativos como a los solucionadores recursivos. Este problema afecta a las versiones 9.0.0 a 9.16.45

Servicio	Vulnerabilidad	Riesgo	Observación
53/tcp – 53/udp	ISC BIND: KeyTrap - Consumo extremo de CPU en el validador DNSSEC (CVE-2023-50387).	**Medio**	Ciertos aspectos de DNSSEC del protocolo DNS (en RFC 4033, 4034, 4035, 6840 y RFC relacionadas) permiten a los atacantes remotos causar una denegación de servicio (consumo de CPU) a través de una o más respuestas de DNSSEC, también conocido como el problema de 'KeyTrap'. Una de las preocupaciones es que, cuando hay una zona con muchos registros DNSKEY y RRSIG, la especificación del protocolo implica que un algoritmo debe evaluar todas las combinaciones de registros DNSKEY y RRSIG.
445/tcp	No se requiere la firma SMBv2.	**Medio**	Este sistema habilitó, pero no requiere la firma SMB. Firma SMB permite al destinatario de los paquetes SMB confirmar su autenticidad y ayuda a prevenir los ataques de intermediario contra las pymes. Firma SMB 2.x se puede configurar de dos maneras: no es necesario y requerido.

Servicio	Vulnerabilidad	Riesgo	Observación
53/tcp – 53/udp	ISC BIND: La limpieza de una caché habilitada para ECS puede provocar una carga excesiva de la CPU (CVE-2023-5680).	**Alto**	Si una caché de resolución tiene un gran número de registros ECS almacenados para el mismo nombre, el proceso de limpieza del nodo de la base de datos de caché para este nombre puede perjudicar significativamente el rendimiento de las consultas. Este problema afecta a las versiones 9.11.3-S1 a 9.11.37-S1, 9.16.8-S1
53/tcp – 53/udp	El servidor DNS permite la indagación de caché.	**Alto**	Este servidor DNS es susceptible a la indagación de la caché DNS, por lo que un atacante puede realizar consultas no recursivas a un servidor DNS, en busca de registros potencialmente ya resuelto por este servidor DNS para otros clientes. Dependiendo de la respuesta, un atacante puede usar esta información para potencialmente lanzar otros ataques.
53/tcp – 53/udp	El servidor de nombres procesa consultas recursivas.	**Alto**	Permitir que los servidores de nombres procesen consultas recursivas provenientes de cualquier sistema puede, en ciertas situaciones, ayudar a los atacantes a llevar a cabo la denegación de

Servicio	Vulnerabilidad	Riesgo	Observación
			servicio o Ataques de envenenamiento de caché.
53/tcp – 53/udp	ISC BIND: La preparación de una prueba de envolvente más cercano NSEC3 puede agotar los recursos de la CPU (CVE-2023-50868).	**Medio**	El aspecto de prueba de envolvente más cercano del protocolo DNS (en RFC 5155 cuando se omite la guía RFC 9276) permite a los atacantes remotos causar una denegación de servicio (consumo de CPU para cálculos SHA-1) a través de respuestas DNSSEC en un ataque de subdominio aleatorio, también conocido como el problema "NSEC3". La especificación RFC 5155 implica que un algoritmo debe realizar miles de iteraciones de una función hash en determinadas situaciones.
53/tcp – 53/udp	Transferencia de zona DNS sin restricciones (CVE-1999-0532).	**Alto**	Un servidor DNS permite transferencias de zona.
------	Respuesta de marca de tiempo ICMP.	**Medio**	La información ICMP, como la máscara de red y la marca de tiempo, se permite desde hosts arbitrarios.

Servicio	Vulnerabilidad	Riesgo	Observación
------	Respuesta de marca de tiempo TCP.	**Bajo**	El host remoto respondió con una marca de tiempo TCP. La respuesta de marca de tiempo TCP se puede utilizar para aproximar el tiempo de actividad del host remoto, lo que podría ayudar a nuevos ataques. Además, algunos sistemas operativos pueden tener huellas dactilares en función del comportamiento de sus marcas de tiempo TCP.

Tabla 8 Matriz de escaneo de vulnerabilidades con la herramienta NEXPOSE

El escaneo realizado con Nexpose encontró los siguientes resultados:

- Se determinó que no se requiere la firma SMB habilitada, en un servidor se expone a la organización a riesgos importantes de seguridad, especialmente los ataques conocidos como man-in-the-middle. Estos ataques pueden poner en peligro la integridad y la confidencialidad de los datos transmitidos entre el cliente y el servidor. La firma SMB es una medida crucial para proteger la comunicación SMB, asegurando que los mensajes no puedan ser modificados durante el tránsito.
- La vulnerabilidad CVE-2023-5517 en el software ISC BIND subraya la necesidad de manejar con cuidado las configuraciones avanzadas del DNS, como la redirección de respuestas NXDOMAIN, sobre todo en entornos que gestionan consultas de forma inversa para direcciones IP privadas. Realizar actualizaciones y emplear una configuración segura son acciones importantes para reducir los riesgos.
- Se encontró CVE-2023-4408 en el software ISC BIND originado por los mensajes de gran tamaño DNS, lo genera una sobrecarga excesiva en la

CPU y puede ocasionar la caída del servicio en caso de gravedad. Actualizar el programa, establecer límites en el tamaño de los mensajes DNS y supervisar el tráfico son pasos fundamentales para gestionar este riesgo.

- Existen transferencias de zonas DNS sin restricciones, debido a ajustes de configuración inadecuados, que permiten a cualquier host solicitar y recibir una copia completa de la base de datos DNS de una zona. Esta vulnerabilidad puede exponer información de carácter confidencial sobre la infraestructura de red, facilitando así posibles ataques.
- Para reducir este riesgo, es fundamental limitar las transferencias de zona únicamente a servidores autorizados, además de aplicar medidas adicionales de seguridad, como autenticación y monitoreo.

2.10.2 Desarrollo de Implementación

Dentro de esta fase se definió el diseño y el alcance del SGSI, el cual es fundamental para posteriormente guiarse en base a dichos objetivos y delimitar nuestro SGSI. Adicionalmente se establecen recomendaciones del alcance y políticas de seguridad con sus respectivos objetivos, determinar una metodología para la gestión de riesgos y por último elaborar la declaración de aplicabilidad de acuerdo a los controles que serán aplicados:

2.10.2.1 Modelo o diseño del SGSI

Dentro de la metodología, se desarrolló un Modelo de Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001. El modelo tiene como objetivo, verificar que los riesgos de seguridad de la información sean gestionados y minimizados por el Departamento de Sistemas y Recursos Tecnológicos del GAD-LIBERTAD. Los aspectos más importantes que del sistema de gestión son:

- Definir Alcance del SGSI
- Definir Política de seguridad de la información
- Metodología de Gestión de Riesgos
- Declaración de Aplicabilidad

2.10.2.2 Alcance del SGSI

El alcance del SGSI se definió en base al contexto de la organización y las características del departamento de Sistemas y Recursos Tecnológicos, de igual forma se tuvo en cuenta los aspectos más importantes de la organización, como sus activos, unidades organizativas, limitaciones objetivos y recursos (véase la documentación completa del alcance en el anexo 2). Se recomiendan los siguientes objetivos y procesos que deberá tener el alcance del SGSI:

Objetivo, alcance y usuarios

El objetivo del alcance es definir claramente los límites del Sistema de Gestión de Seguridad de la Información (SGSI) en el Departamento de Sistemas y Recursos Tecnológicos del GAD Municipal de La Libertad y garantizar la protección de activos del mismo. Los usuarios o subdivisiones que tienen acceso a la documentación del alcance del SGSI para su revisión, son los siguientes:

- Jefa del Departamento
- Área Técnica
- Área de Desarrollo
- Bases de Datos
- Área de Redes
- Programadores e ingenieros

Procesos y servicios del alcance

El departamento de Sistemas determinará el alcance del SGSI según los servicios y sistemas involucrados en los procesos de manejo de información. Se recomienda que el alcance incluya los siguientes procesos:

- **Gestión de activos:** Es uno de los aspectos fundamentales, donde se definirán las responsabilidades que tiene el personal con los activos a su disposición, además de analizar y gestionar los riesgos y vulnerabilidades potenciales.
- **Control de acceso:** La verificación de identidad de los empleados antes de ingresar es necesaria para mantener la confidencialidad e integridad de la información. Los procedimientos implementados deben asegurar un

desempeño apropiado y eficiente. Es fundamental contar con procesos sólidos y bien estructurados que garanticen un funcionamiento óptimo y sin contratiempos.

- **Gestión de Incidentes:** La respuesta ante cualquier eventualidad relacionada con la seguridad de la información, debe ser debidamente gestionada. Es fundamental establecer procedimientos y políticas para garantizar la resolución de problemas y la continuidad del proceso.
- **Gestión de recursos humanos:** El compromiso y capacitación adecuada del personal asegurará un mejor control de los recursos e información durante el empleo o la transición.
- **Manejo de Operaciones y Comunicaciones:** Característica fundamental para garantizar la disponibilidad, acceso a la información y el buen funcionamiento de los sistemas de información, incluso ante posibles incidentes, además se tienen en cuenta procesos como gestión de respaldo y recuperación de datos, se establecerán procedimientos que permitan garantizar un correcto desempeño.
- **Gestión de Servidores:** Respectivo control de los servidores web y bases de datos que alojan aplicaciones y servicios municipales que presentan un riesgo crítico para el Departamento de Sistemas.

2.10.2.3 Política del SGSI

Declaración de la política

La siguiente política de seguridad de la información estará basada en las buenas prácticas y recomendaciones de la norma ISO 27001 y servirá de apoyo para la implementación del SGSI en un futuro:

Establecer buenas prácticas de seguridad de la información centrados en la protección de datos valiosos que se utilizan en diferentes procesos y operaciones, junto con equipo o personal capacitado y con conocimiento en la seguridad de la información. Para garantizar la integridad, confidencialidad, disponibilidad y continuidad de los procesos que respaldan los objetivos de la entidad.

Objetivos

- Determinar controles y un procedimiento formal de Gestión de Seguridad de la Información para prevenir riesgos, el cual forma parte integral del proceso de Gestión y control de Riesgos.
- Determinar y reglamentar los procedimientos necesarios para la operación del Sistema de Gestión de la Seguridad de la Información (SGSI) en el Departamento de Sistemas y Recursos Tecnológicos de la entidad, con el fin de asegurar la ejecución de las actividades requeridas y proteger la información contra amenazas.
- Promover una cultura de seguridad que permita reducir el riesgo de los datos e información, facilitando el monitoreo, control de amenazas, y aplicación de procedimientos que salvaguarden la confidencialidad, integridad y disponibilidad de la información.

Compromiso para la implementación de la alta dirección

La alta gerencia de la organización reconoce que la información es uno de sus activos más valiosos, por lo tanto, debe comprometerse a establecer, implementar y gestionar un Sistema de Seguridad de la Información que incluye un plan de continuidad y recuperación ante desastres. Para demostrar el compromiso, la alta gerencia debe:

- Revisar y aprobar la política de seguridad de la información desarrollada.
- Asegurar la política sea comunicada a todos los empleados de la compañía.
- Garantizar la asignación de los recursos necesarios para implementar y mantener la política de Seguridad de la Información.

2.10.2.4 Metodología para la gestión de Riesgos

Un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la norma ISO 27001 se enfoca en proteger la información de la organización mediante la gestión apropiada de los riesgos asociados. La gestión de riesgos es un componente importante de un SGSI, ya que permite a la organización identificar, evaluar y abordar los riesgos de seguridad de la información de forma apropiada. La elección

de una metodología de gestión de riesgos es un paso fundamental en la implementación de un SGSI.

El análisis de riesgos tiene como finalidad establecer un orden de prioridad de los riesgos asociados a los procesos y activos que forman parte del alcance del SGSI, de modo que puedan ser gestionados de manera efectiva. En esta etapa, se deben identificar las amenazas que afectan a cada uno de los procesos de negocio y activos de información, así como la probabilidad de que dichas amenazas se materialicen. Esta información permitirá estimar el impacto que tendría cualquier falla de seguridad dentro de la organización [7].

Una metodología bien seleccionada no solo garantiza la identificación y el tratamiento adecuados de los riesgos de seguridad de la información, sino que también contribuye a la mejora continua del sistema de gestión y al cumplimiento normativo. Al considerar factores como la naturaleza de la organización, los recursos disponibles y los requisitos regulatorios, las organizaciones pueden elegir la metodología más apropiada para sus necesidades específicas y asegurar la protección efectiva de sus activos de información.

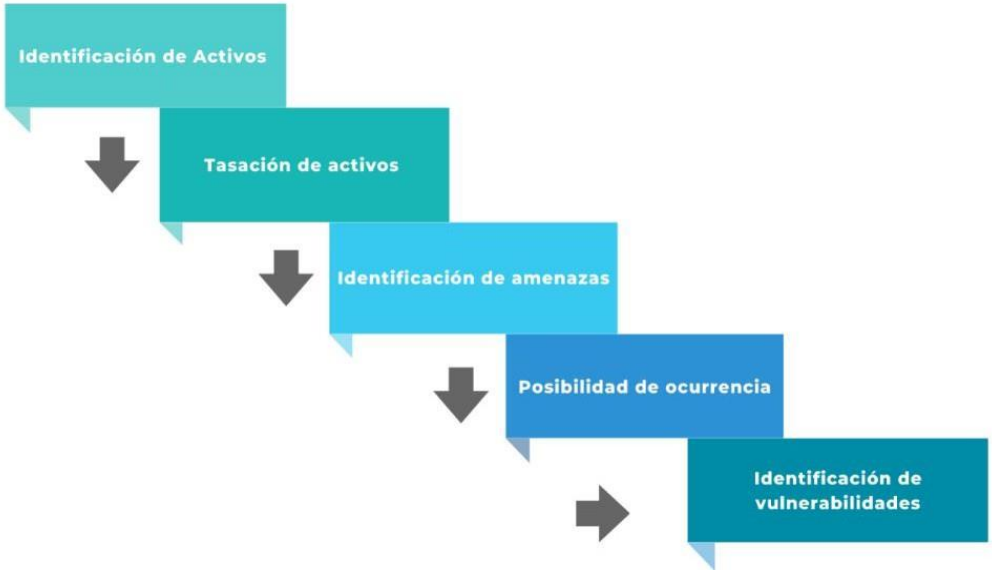

Figura 17. Metodología de Gestión de Riesgos [17]

2.10.2.5 Identificación e inventario de Activos

En esta etapa, es importante realizar un inventario detallado de los activos informáticos, llevar un registro detallado y accesible de los recursos informáticos de la empresa es esencial. Este inventario nos permite conocer en todo momento el estado de cada equipo, lo que facilita la toma de decisiones y la resolución de problemas. Tanto el hardware como el software deben estar debidamente registrados, ya que esta información es crucial para el correcto funcionamiento y mantenimiento de la infraestructura tecnológica [11].

En una organización es importante contar con un sistema de inventario bien detallado, debido a que la gestión eficiente de los recursos informáticos es fundamental para la toma de decisiones y la operación diaria de la organización. Emplear este trabajo permitirá llevar a cabo un análisis y evaluación de los riesgos, identificando las amenazas, vulnerabilidades e impacto potencial para el departamento de Sistemas y Recursos Tecnológicos.

INVENTARIO DE ACTIVOS 'DEPARTAMENTO DE SISTEMAS Y RECURSOS TECNOLÓGICOS'				
Categoría	**Nombre Activo**	**Cantidad**	**Estado**	**Custodio**
Equipos y medios de comunicación	Torres de Comunicación	6	Regular	Jefa del departamento
Equipos y medios de comunicación	Nano Station MS Ubiquiti	5	Regular	Jefa del departamento
Equipos y medios de comunicación	Access Point Wireless Ubiquiti Rocket	8	Regular	Jefa del departamento
Equipos y medios de comunicación	Antenas de Comunicación	10	Bueno	Jefa del departamento
Equipos y medios de comunicación	Radio Walkie Talkie	4	Bueno	Jefa del departamento
Equipos electrónicos	CPU	21	Bueno	Empleados del departamento
Equipos electrónicos	Monitores	27	Bueno	Empleados del departamento
Equipos electrónicos	Mouse	18	Bueno	Empleados del departamento

INVENTARIO DE ACTIVOS 'DEPARTAMENTO DE SISTEMAS Y RECURSOS TECNOLÓGICOS'				
Equipos electrónicos	Laptops	3	Bueno	Empleados del departamento
Equipos electrónicos	Teclados	18	Bueno	Empleados del departamento
Equipos electrónicos	Switch	38	Bueno	Jefa del departamento
Equipos electrónicos	Teléfonos VPLP-SIP IP-PHONE	3	Bueno	Jefa del departamento
Equipos electrónicos	U.P.S 1000 VA o Sistema de Alimentación Ininterrumpida	11	Bueno	Jefa del departamento
Equipos electrónicos	Rack 12 UR de Pared – Gabinetes de Rack	3	Bueno	Jefa del departamento
Equipos electrónicos	Multitoma PDU para Rack 9	1	Bueno	Jefa del departamento
Equipos electrónicos	Módulo de Batería	1	Bueno	Jefa del departamento
Equipos electrónicos	Servidores	8	Bueno	Jefa del departamento
Equipos electrónicos	Impresoras	9	Bueno	Jefa del departamento
Equipos electrónicos	SEAGATE de expansión - Discos duros	7	Bueno	Empleado del departamento
Equipos de oficina y administración	Proyector EPSON	3	Bueno	Jefa del departamento
Equipos de oficina y administración	Compresor	1	Bueno	Jefa del departamento
Equipos de seguridad, vigilancia y control	Cámaras de Seguridad	17	Bueno	Jefa del departamento

Tabla 9. Inventario de Activos

2.10.2.6 Identificación de Amenazas

Una vez realizado el inventario de activos, es importante elaborar una matriz de amenazas y riesgos (externos – internos). Este proceso permite identificar, evaluar y mitigar posibles peligros que puedan comprometer la integridad, confidencialidad y disponibilidad de los recursos informáticos, especialmente en el departamento de Sistemas del municipio. La matriz de amenazas y riesgos facilita priorizar los esfuerzos de seguridad, permitiendo a los responsables del departamento y a la dirección centrarse en las áreas más vulnerables y con mayor impacto potencial.

Este enfoque ayuda a crear un entorno seguro, minimizando las interrupciones y los daños causados por incidentes de seguridad. Además, una matriz bien diseñada sirve como base para desarrollar políticas, procedimientos y controles de seguridad, asegurando una gestión eficaz de los riesgos a los que está expuesta la organización.

AMENAZA INTERNA	RIESGO INTERNO
Daños intencionales a equipos informáticos.	Pérdida de equipos y datos críticos
Hurto por parte de funcionarios.	Pérdida económica y alto costo de reemplazo
Malware interno dentro del departamento.	Riesgo de pérdida de datos, seguridad de los sistemas puede estar comprometida.
Suplantación de identidad.	Robo de información de carácter confidencial, pérdida de confianza de los usuarios.
Errores de configuración en equipos electrónicos como switch, routers, etc.	Brechas de seguridad y pérdida de datos, interrupción de servicios críticos
Falta de actualización de software en activos.	Activos expuestos a ataques informáticos.
Descuido en la gestión de contraseñas, contraseñas débiles y que no se cambian con regularidad.	Accesos no autorizados, suplantación de usuarios y robo de datos.

AMENAZA EXTERNA	RIESGO EXTERNO
Ataques Informáticos.	Seguridad de los sistemas puede estar comprometida, robo de datos, alteración de información y denegación de servicios.
Phishing	Acceso no autorizado, pérdida de información sensible.
Desastres Naturales	Destrucción y daños en la Infraestructura, interrupción de servicios por mucho tiempo
Cortes de luz y del suministro eléctrico.	Servicios críticos pueden estar caídos por breves períodos de tiempo, daños en equipos eléctricos.
Proveedores externos.	Dependencia crítica, demoras por fallas en los proveedores, cadenas de suministros bajas.
Espionaje Industrial.	Robo de información confidencial, pérdida de ventaja competitiva.

Tabla 10. Matriz de Amenazas y Riesgos

2.10.2.7 Probabilidad de Ocurrencia y Valoración de Activos

Para la valoración de activos, se evaluará el nivel de impacto o afectación que podría tener sobre el activo específico, al modificar alguno de sus componentes o recursos de información. La puntuación se asigna de acuerdo con los requisitos establecidos en la norma ISO 27001, relacionados con los requerimientos de confidencialidad, integridad y disponibilidad, con el fin de cuantificar el impacto dentro de su respectivo proceso.[7] La siguiente tabla describe los requisitos de confidencialidad, integridad y disponibilidad que se deben asignar a cada uno de los activos, en función de su nivel de impacto: alto, medio o bajo, según su comportamiento dentro del proceso:

REQUISITO	NIVEL DE VALORACIÓN		
	BAJO	MEDIO	ALTO
Confidencialidad	Esta información está disponible para el público en general y su acceso no tiene ningún efecto significativo en el resultado del proceso.	Esta información es de uso exclusivo interno o de circulación limitada, y su acceso por parte de personas no autorizadas no afectaría considerablemente el resultado ni pondría en riesgo a la empresa.	Esta información es de carácter secreto y de máxima confidencialidad. Si personas no autorizadas acceden a ella, el impacto final sobre el proceso o los resultados de la empresa sería sumamente grave.
Integridad	Las aplicaciones empresariales pueden sobrellevar un poco de daño o modificación sin autorización, sin afectar significativamente a la empresa.	El daño o modificación no autorizada a las aplicaciones empresariales es notable, y tiene un impacto considerable en la organización.	Cualquier daño o modificación no autorizada es crítica para la empresa, y puede causar consecuencias graves o incluso la pérdida total de la aplicación o sistema empresarial.

REQUISITO	NIVEL DE VALORACIÓN		
	BAJO	MEDIO	ALTO
Disponibilidad	El activo puede permanecer inaccesible hasta por un día sin mayores problemas.	Podemos aceptar que el activo no esté disponible durante medio día como máximo, pero no más de un día.	No es aceptable que el activo no esté accesible por más de unas pocas horas (4 horas) o incluso menos.

Tabla 11. Matriz de nivel de valoración de activos [7]

Una vez determinado los requisitos para el nivel de valoración de los activos, se utiliza la tabla para cada uno de los activos que tenemos en nuestro inventario, haciendo la siguiente correspondencia, 1 es igual a 'bajo', 2 es igual a 'medio' y 3 es igual 'alto' siendo la valoración total del activo la suma de todos los valores en relación a su disponibilidad, integridad y confidencialidad, tal como se observa a continuación:

ACTIVOS DE EQUIPOS Y MEDIOS DE COMUNICACIÓN

Activos	Confidencialidad	Disponibilidad	Integridad	Total
Torres de Comunicación	1	3	2	6
Nano Station MS Ubiquiti	1	2	2	5
Access Point Wireless Ubiquiti Rocket	1	3	2	6
Antena de Comunicación Ubiquiti 5GHz 25DBI	1	3	2	6

Activos	Confidencialidad	Disponibilidad	Integridad	Total
Radio Walkie Talkie	1	2	1	4

Tabla 12. Valoración de activos de equipos y medios de comunicación

ACTIVOS DE EQUIPOS ELECTRÓNICOS

Activos	Confidencialidad	Disponibilidad	Integridad	Total
CPU, Monitores	2	3	2	7
Laptops	2	2	2	6
Mouse y Teclados	1	2	1	4
Switch 24 puertos	2	3	2	7
Teléfonos VPLP-SIP IP-PHONE	1	3	2	6
U.P.S 1000 VA o Sistema de Alimentación Ininterrumpida	1	3	2	6
Rack 12 UR de Pared – Gabinetes de Rack	1	2	1	4
Multitoma PDU para Rack 9	1	2	1	4
Módulos de Batería	1	3	1	5
Network Video Recorder HDMI, USB	2	3	2	7
Servidores	3	3	3	9
Impresoras Multifunción – Escáneres Fujitsu	1	2	2	5

Activos	Confidencialidad	Disponibilidad	Integridad	Total
SEAGATE de expansión - Discos duros	3	2	2	7

Tabla 13. Valoración de activos de equipos electrónicos

ACTIVOS EQUIPOS DE OFICINA Y SEGURIDAD (VIGILANCIA Y CONTROL)

Activos	Confidencialidad	Disponibilidad	Integridad	Total
Proyectores EPSON	1	2	1	4
Central Telefónica	2	3	3	8
Split de Pared y Compresor	1	2	1	4
Cámaras de Seguridad	2	3	3	8

Tabla 14. Valoración de activos de equipos de oficina y seguridad

2.10.2.8 Identificación de Amenazas y Vulnerabilidades para los activos informáticos

El análisis de riesgo es uno de los pasos más importantes para implementar un sistema de gestión de seguridad de la información, ya que permite examinar de manera correcta cada uno de los procesos, actividades y demás tareas de la organización que podría estar en riesgo, además de determinar las necesidades de seguridad, las vulnerabilidades potenciales y las amenazas a las que se enfrenta. Por lo tanto, el resultado obtenido de todo este proceso de análisis de riesgos es la información sobre la situación actual de la empresa en términos de sus niveles de seguridad, los controles implementados y los riesgos existentes [45].

AMENAZA	VULNERABILIDAD
Fuego	Ausencia de sistemas de prevención de incendios. Falta de procesos para revisar y mantener estos sistemas.
Condiciones climáticas desfavorables	Altas temperaturas en verano, fallas en equipos por altas temperaturas.
Desastres naturales	Infraestructura no preparada para inundaciones, terremotos, etc. Faltas de copias de seguridad en otros sitios.
Eventos importantes del medio ambiente	Es probable que uno se vea afectado por obras o eventos que sucedan en el área cercana, como manifestaciones o disturbios públicos.
Interrupción de fuentes de alimentación	Probabilidad de interrupciones del suministro eléctrico.
Interrupción de redes de comunicación	La dependencia en un solo proveedor de internet puede ser problemática, ya que no hay respaldo si surge algún problema. La infraestructura de comunicación carece de la debida protección.
Modificación de la información	Falta de controles de acceso adecuados, medidas de autenticación y contraseñas de acceso débiles.
Espionaje	Exposición de información confidencial de la organización. Productos y servicios

AMENAZA	VULNERABILIDAD
	pueden ser utilizados por la competencia, intercepción de señales.
Manipulación de hardware y software	Acceso sin restricciones a servidores y equipos clave, ausencia de controles para administrar cambios del software.
Software Malicioso	Antivirus inexistentes y sistema de detección de intrusos desactualizado, falta de políticas para descargar o navegación.
Ingeniería Social	Capacitación necesaria para empleados en seguridad de la información, políticas débiles en relación a la verificación de identidad.
Pérdida de datos	La falta de mecanismos de seguridad para preservar y restaurar la información es preocupante. Falta de cifrado en datos o información sensible.

Tabla 15. Matriz de descripción de amenazas y vulnerabilidades de los activos

Según Helena Alemán en su trabajo de titulación 'Metodología para la implementación de un SGSI en la fundación universitaria Juan de Castellanos, bajo la norma ISO 27001:2005' una vez identificadas las posibles amenazas y vulnerabilidades de los activos informáticos, se procederá a evaluar el nivel de riesgo, el cual se establecerá en función de los activos cuyo valor de nivel de impacto sean mayor o igual a 5, teniendo en cuenta que [7]:

Nivel de riesgo= Nivel de Amenaza X Nivel de vulnerabilidad X Nivel de impacto

El nivel de vulnerabilidad y el nivel de amenaza se los puede calificar en una escala de 0 a 3, respectivamente:

- 0 = no aplica
- 1 = bajo
- 2 = medio
- 3 = alto

Dentro de la siguiente tabla se establecieron los activos en función de su valor de impacto, dentro del activo informático de los servidores, se determinó que presentan un riesgo alto de acuerdo al análisis de vulnerabilidades realizado previamente, por lo que se creó un apartado solo del servidor, donde se realizaron las pruebas respectivas. Solo se agregaron las amenazas y vulnerabilidades más importantes con respecto al servidor, para una visión más detallada dirigirse a la sección de **ejecución de análisis de vulnerabilidades**.

ACTIVO	AMENAZA	VULNERABILIDAD	NIVEL DE IMPACTO	NIVEL AMENAZA	NIVEL VULNERABILIDAD	NIVEL DE RIESGO
Torres de Comunicación -- Antena de Comunicación Ubiquiti 5GHz 25DBI	Desastres Naturales	Perdida de información por falta de copias de seguridad	6	2	3	36
	Interrupción de fuentes de alimentación	Fallas en el suministro eléctrico				
Nano Station MS Ubiquiti -- Access Point Wireless Ubiquiti Rocket	Recalentamiento	Problemas en la alimentación eléctrica	5	2	2	20
	Interrupción de redes de comunicación	Infraestructura carece de mantenimiento y actualización				
Computadoras, CPU, laptops	Software malicioso	Antivirus inexistentes, falta de actualización de sistemas operativos	7	3	3	63
	Ingeniería social	Falta de capacitación del personal y empleados, verificación de identidad nula				
	Virus	Mal uso del internet, inexistentes restricciones para navegar en la red				

ACTIVO	AMENAZA	VULNERABILIDAD	NIVEL DE IMPACTO	NIVEL AMENAZA	NIVEL VULNERABILIDAD	NIVEL DE RIESGO
	Modificación de la información	Falta de controles de acceso adecuados, medidas de autenticación y contraseñas de acceso débiles				
Switch	Sobrecarga de recursos	Falta de monitoreo y falta de balance de cargas	7	3	2	42
	Rendimiento bajo (Daño irreparable)	Falta de mantenimiento a los equipos o reemplazo de los mismos				
Sistema de Alimentación Ininterrumpida – Módulos de batería	Hardware defectuoso	Componentes del UPS obsoletos, no existe redundancia en sistemas importantes	6	2	2	24
	Fallos en las baterías	Tiempo de vida útil cumplido, falta de pruebas en las baterías adquiridas				
	Sobrecalentamiento	No existe suficiente ventilación en lugar físico del equipo, sobrecarga del sistema				

ACTIVO	AMENAZA	VULNERABILIDAD	NIVEL DE IMPACTO	NIVEL AMENAZA	NIVEL VULNERABILIDAD	NIVEL DE RIESGO
Teléfonos VPLP-SIP IP-PHONE -- Central Telefónica	Pérdida de conexión	Configuración de central telefónica inadecuada	7	1	2	14
Impresora Multifunción	Componentes defectuosos	Vida útil del equipo corta	5	2	1	10
	Cabezales dañados	Falta de mantenimiento a los equipos				
	Cartuchos incompatibles	Falta de control de recursos				
Router	Intermitencia y caída de la red	Configuración del equipo incorrecta	5	2	2	20
	Pérdida económica por daño del equipo	No existe mantenimiento alguno en los equipos				
Network Video Recorder	Daños físicos	Ataques a las cámaras, lo que ocasiona falta de funcionamiento	8	2	2	32

ACTIVO	AMENAZA	VULNERABILIDAD	NIVEL DE IMPACTO	NIVEL AMENAZA	NIVEL VULNERABILIDAD	NIVEL DE RIESGO
HDMI, USB -- Cámaras de Seguridad	Pérdida de conexión	Caída de la imagen en vivo y de las grabaciones				
Servidor Secundario	Robo de información	Ausencia de calidad de servicio, caída de la red y servicios a fines	9	3	3	72
	Ataques Informáticos	Baja protección contra malware	9	3	3	
		No actualizar el software con regularidad y aplicación de parches	9	3	3	

Tabla 16. Activos más importantes para la obtención de nivel de riesgo

2.10.2.9 Aplicabilidad de Objetivos de Control

Siguiendo las buenas prácticas establecidas en la Norma ISO 27001, se elaboró una nueva matriz donde se agregó una columna donde indica el 'Objetivo de Control' correspondiente. Esto permitió elegir el dominio en función de cumplir con las condiciones de evaluación descritas en la tabla 16 y así realizar un tratamiento de las amenazas de cada activo. La selección adecuada de los objetivos de control garantiza que todos los aspectos de los activos de información de la organización, que fueron valorados con algún grado de riesgo, queden cubiertos y sean auditados en un futuro. A continuación, se presenta la columna "Objetivo de control" que contiene los dominios relacionados con las amenazas detalladas para cada activo informático.

Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Objetivos de Control
Torres de Comunicación -- Antena de Comunicación Ubiquiti 5GHz 25DBI	Desastres Naturales	Perdida de información por falta de copias de seguridad	36	A.11 Seguridad Física y del Entorno A.13 Seguridad en las Comunicaciones
	Interrupción de fuentes de alimentación	Fallas en el suministro eléctrico		
Nano Station MS Ubiquiti --	Recalentamiento	Problemas en la alimentación eléctrica	20	A.12 Seguridad de

Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Objetivos de Control
Access Point Wireless Ubiquiti Rocket	Interrupción de redes de comunicación	Infraestructura carece de mantenimiento y actualización		las Operaciones A.13 Seguridad en las Comunicaciones
Computadoras, CPU, laptops	Software malicioso	Antivirus inexistentes, falta de actualización de sistemas operativos	63	A.5 Políticas de Seguridad de la Información A.9 Control de Acceso A.10 Criptografía A.14 Adquisición, desarrollo y Mantenimiento de los sistemas de información.
	Ingeniería social	Falta de capacitación del personal y empleados, verificación de identidad nula		
	Virus	Mal uso del internet, inexistentes restricciones para navegar en la red		
Switch	Sobrecarga de recursos	Falta de monitoreo y falta de balance de cargas	42	A.13 Seguridad en las

Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Objetivos de Control
	Rendimiento bajo (Daño irreparable)	Falta de mantenimiento a los equipos o reemplazo de los mismos		Comunicaciones A.8 Gestión de Activos A.11 Seguridad Física y del Entorno
Sistema de Alimentación Ininterrumpida – Módulos de batería	Hardware defectuoso	Componentes del UPS obsoletos, no existe redundancia en sistemas importantes	24	A.11 Seguridad Física y del entorno A.16 Gestión de Incidentes en Seguridad de la Información
	Fallos en las baterías	Tiempo de vida útil cumplido, falta de pruebas en las baterías adquiridas		
	Sobrecalentamiento	No existe suficiente ventilación en lugar físico del equipo, sobrecarga del sistema		
Teléfonos VPLP-SIP IP-PHONE -- Central Telefónica	Pérdida de conexión	Configuración de central telefónica inadecuada	14	A.13 Seguridad en las Comunicaciones

Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Objetivos de Control
				A.11 Seguridad Física y del entorno
Impresora Multifunción	Componentes defectuosos	Vida útil del equipo corta	10	A.5 Políticas de Seguridad de la Información A.6 Organización de Seguridad de la Información A.9 Control de Acceso A.10 Criptografía
	Cabezales dañados	Falta de mantenimiento a los equipos		
	Cartuchos incompatibles	Falta de control de recursos		
Router	Intermitencia y caída de la red	Configuración del equipo incorrecta	20	A.13 Seguridad en las Comunicaciones A.8 Gestión de Activos A.11 Seguridad Física y del Entorno
	Pérdida económica por daño del equipo	No existe mantenimiento alguno en los equipos		
Network Video Recorder HDMI, USB --	Daños físicos	Ataques a las cámaras, lo que ocasiona falta de funcionamiento	32	A.11 Seguridad Física y del Entorno

Activo	Amenaza	Vulnerabilidad	Nivel de Riesgo	Objetivos de Control
Cámaras de Seguridad	Pérdida de conexión	Caída de la imagen en vivo y de las grabaciones		
Servidor Secundario	Robo de información	Ausencia de calidad de servicio, caída de la red y servicios a fines	72	A.9 Control de Acceso A.11 Seguridad Física y del Entorno A.13 Seguridad en las Comunicaciones
	Ataques Informáticos	Baja protección contra malware		
		No actualizar el software con regularidad y aplicación de parches		

Tabla 17. Matriz de Objetivos de control

2.10.2.10 Declaración de Aplicabilidad

El objetivo de la elaboración de la Declaración de Aplicabilidad es fundamental para definir qué controles son los adecuados para aplicar en el Departamento de Sistemas y recursos tecnológicos, con su respectiva justificación. De esta manera, se busca garantizar la seguridad de la información y la protección de los sistemas de la entidad. Es importante destacar que los objetivos y controles enumerados en la tabla están alineados con los controles del anexo A de la norma ISO/IEC 27002:2013, es decir, las cláusulas del 5 al 18, y se deben aplicar a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Cada control detallado para el Departamento de Sistemas de la entidad es importante para garantizar la seguridad de la información y proteger los sistemas de la entidad, también verificar que se implementen de manera efectiva y se realicen

evaluaciones periódicas. La elaboración de la Declaración de Aplicabilidad es un proceso importante que debe ser realizado con la mayor atención y cuidado posible. Es necesario que se realice una evaluación de los riesgos y amenazas que pueden afectar a la entidad, para establecer los controles adecuados que permitan minimizarlos y garantizar la seguridad de la información.

A continuación, se detallan los objetivos de control para el Departamento de Sistemas del GAD-LIBERTAD:

A.5 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN				
A.5.1 DIRECTRICES DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI	**NO**	
A.5.1.1	Políticas para la Seguridad de la Información.	X		Es fundamental elaborar un documento donde se establezcan políticas de seguridad, debido a que el departamento de sistemas maneja información y éste es uno de los activos más importantes, el documento debe ser aprobado y publicado por el departamento de Sistemas.
A.5.1.2	Revisión de las Políticas de Seguridad de la Información.	X		Es importante realizar revisiones constantes de las políticas de seguridad de la información, para garantizar su eficacia.

Tabla 18. Matriz controles Políticas de Seguridad

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN				
A.6.1 ORGANIZACIÓN INTERNA				
SECCIÓN	CONTROLES ISO 27001	APLICABILIDAD		JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN
		SI	NO	
A.6.1.1	Roles de seguridad de la información y responsabilidades de seguridad de la información.	X		Es importante que todas las responsabilidades sean definidas y asignadas, para que la toma de decisiones sea efectiva.
A.6.1.2	Separación de tareas.	X		Separar las diferentes funciones de permisos administrativos de acceso a sistemas o áreas restringidas, evitando que las responsabilidades recaigan sobre una sola persona. Asignar perfil de acuerdo con las responsabilidades.
A.6.1.3	Contacto con autoridades.	X		Mantener contacto con las autoridades pertinentes, para reportar de forma óptima incidentes de seguridad de la información.
A.6.1.4	Contacto con grupos de intereses especiales.	X		El jefe del departamento de sistemas debe mantener contacto con otros departamentos del GAD-LIBERTAD
A.6.1.5	Seguridad de la Información en la gestión de proyectos.	X		El área de desarrollo de proyectos debe cumplir con reglas correspondientes a la seguridad de la información y elaborar una evaluación de

				riesgo al comienzo de cualquier proyecto.
A.6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO				
A.6.2.1	Políticas de dispositivos Móviles.	X		Establecer una política y medidas de seguridad para protección contra riesgos con el uso de dispositivos móviles.
A.6.2.2	Teletrabajo.	X		Si se accede a la información desde lugares de teletrabajo o si se procesa o almacena información, se debe garantizar su protección.

Tabla 19. Matriz controles Organización de la Seguridad de la Información

Se recomienda aplicar los controles A.7 del anexo A relacionado con la seguridad ligada a recursos humanos, sin embargo, el Departamento de Sistemas será el encargado de definir el procedimiento que consideren necesario para la contratación o desvinculación del personal:

A.7 SEGURIDAD LIGADA A RECURSOS HUMANOS				
A.7.1 ANTES DEL EMPLEO				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI	**NO**	
A.7.1.1	Verificación de antecedentes.	X		Los solicitantes de empleo deben cumplir con leyes, normas, regulaciones y principios éticos para la idoneidad del trabajo. La revisión es necesaria con miras en requisitos del negocio.

A.7 SEGURIDAD LIGADA A RECURSOS HUMANOS				
A.7.1.2	Términos y condiciones de la relación laboral.	X		Asegurarse que los empleados cumplan las condiciones relacionadas con la seguridad de la información. En caso de que el departamento no cumpla con este control se darán las debidas recomendaciones.
A.7.2 DURANTE EL EMPLEO				
A.7.2.1	Responsabilidades de gestión.	X		Debe realizarse de forma periódica una capacitación al personal del departamento de Sistemas, así garantizar la seguridad de la información.
A.7.2.2	Concientización, educación y formación en seguridad de la información.			
A.7.2.3	Proceso de medidas disciplinarias.			
A.7.3 FINALIZACIÓN O CAMBIO DE RELACIÓN LABORAL O EMPLEO				
A.7.3.1	Responsabilidades en la desvinculación.	X		Se deben tener en cuenta las responsabilidades correspondientes a la desvinculación laboral. Además de la devolución completa de los activos de información.

Tabla 20. Matriz de Seguridad Ligada a Recursos humanos

A.8 GESTIÓN DE ACTIVOS				
A.8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EX CLUSIÓN**
		SI	**NO**	
A.8.1.1	Inventario de activos.	X		Identificación de activos de información y responsabilidades sobre los mismos, con objetivo de evaluar medidas de protección de cada activo, basado en una gestión de riesgos.
A.8.1.2	Propiedad de los activos.	X		Establecer que todos los activos del departamento tengan un propietario y cumplan con las políticas establecidas.
A.8.1.3	Uso aceptable de los activos.	X		Es importante que se realicen normas para el uso aceptable de los activos informáticos. Y así documentar el uso apropiado basado en la seguridad de la información.
A.8.1.4	Proceso de devolución de activos	X		Control para que los empleados, devuelvan los activos de información una vez finalizado el periodo de utilización.
A.8.2 CLASIFICACIÓN DE LA INFORMACIÓN				
A.8.2.1	Clasificación de la información	X		Es fundamental que el departamento de Sistemas, elabore un plan para la clasificación de la información de acuerdo a su valor, dentro de la empresa.
A.8.2.2	Etiquetado de la información.	X		Se debe desarrollar un conjunto adecuado de procedimientos para etiquetar la información. Así asegurar el manejo

				adecuado de los activos de información.
A.8.2.3	Manipulado de la información	X		Se busca garantizar la protección del activo a través del procedimiento de gestión de activos.
A.8.3 MANIPULACIÓN DE SOPORTES				
A.8.3.1	Gestión de soportes extraíbles.	X		Se debe implementar una política para evitar la propagación de Malware o virus informáticos y evitar la pérdida de información.
A.8.3.2	Eliminación de soportes.	X		Los soportes deben eliminarse de forma segura cuando ya no vayan a ser necesarios.
A.8.3.3	Soportes físicos en tránsito.	X		Es fundamental custodiar la información para evitar acceso no autorizado o corrupción en el transporte.

Tabla 21. Matriz de la Gestión de Activos

A.9 CONTROL DE ACCESO				
A.9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESO				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EX CLUSIÓN**
		SI	**NO**	
A.9.1.1	Política de control de acceso.	X		El departamento de sistemas debe establecer roles y perfiles de acceso de acuerdo a las diferentes funciones del cargo. Establecer política de control de acceso.
A.9.1.2	Acceso a las redes y a los servicios de red.	X		Se debe proporcionar a los usuarios el acceso a las redes y a los servicios en red para los cuales tengan autorización debida.

A.9.2 GESTIÓN DEL ACCESO DE USUARIOS				
A.9.2.1	Registro y baja de usuarios.	X		Es fundamental implementar procesos que permitan asignar y revocar derechos de acceso, cuando el empleado inicie o termine su vinculación laboral.
A.9.2.2	Gestión de acceso a los usuarios.			
A.9.2.3	Gestión de privilegios de acceso.	X		El departamento de Sistemas debe establecer roles y perfiles de acceso, cuando se inicie el empleado y cuando finalice su período.
A.9.2.4	Gestión de la información de autenticación secreta de autenticación de usuarios.	X		Se busca verificar la identidad de los usuarios que hacen uso de los sistemas del departamento, por medio de autenticación.
A.9.2.5	Revisión de los derechos de acceso de usuario.	X		Es importante que quienes estén a cargo de la gestión de la información se aseguren de que los permisos otorgados estén en línea con las responsabilidades de cada puesto.
A.9.2.6	Retirada o reasignación de los derechos de acceso.	X		En caso de finalización de cargo, se deben retirar los activos de información y revocar toda clase de permisos y contraseñas.
A.9.3 RESPONSABILIDADES DEL USUARIO				
A.9.3.1	Uso de las contraseñas de autenticación.	X		Los usuarios deben establecer contraseñas fuertes y seguras para evitar vulnerabilidades a los sistemas de información.

A.9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES				
A.9.4.1	Restricción del acceso a la información.	X		Los responsables de los activos de información deben validar que los derechos de acceso sean acordes a su función, que están establecidas en las políticas ya definidas.
A.9.4.2	Procedimientos seguros de inicio de sesión.			
A.9.4.3	Sistema de gestión de contraseñas.	X		Se deben establecer cambios de contraseñas de forma periódica, además de registrar todas contraseñas y rechazar contraseñas similares
A.9.4.4	Uso de utilidades con privilegios del sistema	X		Se debe restringir y controlar el uso de utilidades que puedan ser capaces de invalidar los controles del sistema.
A.9.4.5	Control de acceso al código fuente de los programas.	X		Es importante limitar el acceso a los códigos fuente para evitar que los programas y sus elementos sean manipulados o divulgados.

Tabla 22. Matriz de Control de Acceso

A.10 CRIPTOGRAFÍA				
A.10.1 CONTROLES CRIPTOGRÁFCOS				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EX CLUSIÓN**
		SI	**NO**	
A.10.1.1	Política de uso de los controles criptográficos.	X		El departamento de Sistemas debe establecer normas para el uso de la criptografía y garantizar la protección de la información.
A.10.1.2	Gestión de claves.	X		Las directrices para la encriptación tienen que incluir la administración de las contraseñas, las cuales deben estar conectadas con la

				protección, la duración y el ciclo de vida.

Tabla 23. Matriz de controles de Criptografía

A.11 SEGURIDAD FÍSICA Y DEL AMBIENTE				
A.11.1 ÁREAS SEGURAS				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EX CLUSIÓN**
		SI	**NO**	
A.11.1.1	Perímetro de seguridad física.	X		Es importante restringir el acceso a las áreas que contienen información delicada y solo permitir que las personas con funciones correspondientes tengan acceso a ellas. Este punto ya está cubierto por el Municipio.
A.11.1.2	Controles físicos de entrada.	X		La entidad ya tiene cubierto este punto, con biométricos que verifican la persona que ingresa al departamento, sin embargo, debe aplicarse el control.
A.11.1.3	Seguridad de oficinas, despachos e instalaciones.	X		El acceso a áreas que manejan información como servidores y base de datos, está restringida y solo personal autorizado puede ingresar.
A.11.1.4	Protección contra amenazas externas y del ambiente	X		Elaborar políticas de protección física contra factores externos, el encargado de elaborar será el Departamento de Sistemas.
A.11.1.5	El trabajo en las áreas seguras.	X		Se deben diseñar procedimientos para el trabajo en áreas seguras, donde la información sea

				más sensible, como evitar el uso de dispositivos móviles.
A.11.1.6	Áreas de acceso público, de entrega y de carga.	X		El departamento de sistemas se maneja en una parte aislada de la entidad, además de tener un control de acceso a toda persona que ingresa al departamento, sea colaborador o no.
A.11.2 SEGURIDAD DE LOS EQUIPOS				
A.11.2.1	Emplazamiento y protección de equipos.	X		Es importante delimitar un espacio protegido para colocar los equipos y reducir la posibilidad de riesgos ambientales o ingresos no autorizados.
A.11.2.2	Instalaciones de suministro.	X		Es fundamental que los equipos estén resguardados de posibles interrupciones de energía y otros trastornos provocados por fallas en las instalaciones de abastecimiento.
A.11.2.3	Seguridad del cableado.	X		Es necesario proteger el cableado eléctrico y de telecomunicaciones que transmite información para evitar interferencias o daños en los servicios de información.
A.11.2.4	Mantenimiento de los equipos.	X		Es necesario establecer pautas para el mantenimiento de los equipos que aseguren su disponibilidad.
A.11.2.5	Retirada de materiales de propiedad de la empresa.	X		Las pautas para proteger los activos deben contemplar la identificación del personal tanto interno como externo que tiene la autorización para

				retirarlos, así como el período durante el cual se retirarán y la verificación de que se devuelvan correctamente.
A.11.2.6	Seguridad de los equipos fuera de las instalaciones.		X	Mantener un registro de custodia de los activos que abandonan la entidad y realizar evaluaciones de riesgo para instalaciones donde serán usados. No hacen uso de laptops u otro dispositivo adicional al que ya tienen.
A.11.2.7	Reutilización o eliminación segura de equipos	X		Es importante contar con directrices para la eliminación y reutilización de equipos que aseguren que la información sea eliminada de manera irreversible, ya sea mediante la destrucción o la sobre escritura, para evitar su recuperación.
A.11.2.8	Equipo de usuario desatendido.		X	Los empleados deben asegurarse de que los equipos desatendidos cumplen con la protección adecuada. El departamento ya cumple con este apartado.
A.11.2.9	Política de puesto de trabajo despejado y pantalla limpia.	X		Los empleados del departamento de sistemas deben comprender completamente las normas en relación al uso de los dispositivos, la privacidad de la información, la gestión de contraseñas y las sesiones.

Tabla 24. Matriz de Seguridad Física y del Ambiente

A.12 SEGURIDAD DE LAS OPERACIONES				
A.12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI	**NO**	
A.12.1.1	Procedimientos documentados de operación.	X		Elaborar procedimientos y documentarlos para las labores de operación de forma que se garantice la seguridad.
A.12.1.2	Gestión de cambios.	X		Es importante registrar cualquier modificación en los procedimientos. La información documentada debe incluir detalles como la identificación, planificación, evaluación del impacto, y otros aspectos relevantes.
A.12.1.3	Gestión de capacidades.	X		El gerente departamental debe ser el responsable de supervisar el uso de los activos del departamento de Sistemas y de planificar la capacidad, para garantizar el rendimiento requerido.
A.12.1.4	Separación de los recursos para desarrollo, prueba y producción.	X		Es necesario que el departamento de sistemas divida los entornos de desarrollo de los entornos de producción con el fin de prevenir interrupciones o errores en el servicio.
A.12.2 PROTECCIÓN CONTRA EL SOFTWARE MALICIOSO (MALWARE)				
A.12.2.1	Controles contra el código malicioso.	X		Es importante asegurar la protección de la información mediante la implementación de normas y medidas de seguridad que prohíban el uso de programas no

				autorizados, detecten su presencia y limiten el acceso a páginas web maliciosas.
A.12.3 COPIAS DE SEGURIDAD				
A.12.3.1	Copias de seguridad de la información.	X		Es importante hacer respaldos de la información, software y sistema y revisarlos regularmente según la política de copias de seguridad establecida.
A.12.4 REGISTROS Y SUPERVISIÓN				
A.12.4.1	Registro de eventos.	X		Es necesario establecer reglas claras para registrar, almacenar y acceder a la información de las actividades, a fin de manejarlas de forma efectiva.
A.12.4.2	Protección de la información del registro.	X		Es necesario asignar a cada empleado un usuario y contraseña para garantizar la seguridad en el acceso a la información y tareas asignadas, con el objetivo de establecer un adecuado control de protección de datos.
A.12.4.3	Registros de administración y operación.	X		Se deben controlar y proteger los registros de los usuarios privilegiados como los administradores, para regular sus actividades.
A.12.4.4	Sincronización del reloj.	X		Es necesario que los relojes de los equipos del departamento de Sistemas estén sincronizados para cumplir con las normativas y mantener una medida uniforme.

A.12.5 CONTROL DEL SOFTWARE EN EXPLOTACIÓN				
A.12.5.1	Instalación del software en explotación.	X		Sólo aquellos empleados que estén autorizados dentro del departamento de sistemas tienen la capacidad de instalar o desinstalar programas en los equipos de la empresa.
A.12.6 GESTIÓN DE VULNERABILIDAD TÉCNICA				
A.12.6.1	Gestión de las vulnerabilidades técnicas.	X		Es necesario disponer de controles adecuados para manejar las vulnerabilidades técnicas identificadas en la matriz de riesgos.
A.12.6.2	Restricción en la instalación de software.	X		Se deben establecer y aplicar reglas que rijan la instalación de software por parte de los usuarios.
A.12.7 CONSIDERACIONES SOBRE LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN				
A.12.7.1	Controles de auditoría de sistemas de información	X		Las auditorías requeridas, se deben planificar y coordinar con la dirección ejecutiva.

Tabla 25. Matriz de Seguridad de las Operaciones

A.13 SEGURIDAD DE LAS COMUNICACIONES				
A.13.1 GESTIÓN DE LA SEGURIDAD DE REDES				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI	**NO**	
A.13.1.1	Controles de red.	X		Para garantizar el correcto funcionamiento de las redes de

				información se deben establecer controles y procedimientos para asegurar la configuración de los dispositivos
A.13.1.2	Seguridad de los servicios de red.	X		Es importante determinar y gestionar los servicios de red mediante controles adecuados.
A.13.1.3	Segregación en redes.	X		La red está segmentada correctamente, sin embargo, el control debe ser aplicado para una mejor seguridad.
A.13.2 INTERCAMBIO DE INFORMACIÓN				
A.13.2.1	Políticas y procedimientos de intercambio de información.	X		Es necesario implementar medidas oficiales, procesos y regulaciones que salvaguarden el intercambio de datos a través de cualquier medio de comunicación y establecer pactos para garantizar la seguridad de la información empresarial.
A.13.2.2	Acuerdo de intercambio de información.			
A.13.2.3	Mensajería electrónica	X		Es importante garantizar la seguridad de toda la información relacionada con la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o no revelación.		X	No aplica, ya que la información que se maneja en el departamento de Sistemas es ajena a terceras personas y se maneja internamente en la entidad.

Tabla 26. Matriz de Seguridad de las Comunicaciones

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN				
A.14.1 REQUISITOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EX CLUSIÓN**
		SI	**NO**	
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información.	X		Cuando un gerente adquiere nuevos sistemas de información o realiza cambios en los sistemas existentes, es importante que documente los requisitos de seguridad en el documento de especificaciones de requerimientos de seguridad.
A.14.1.2	Asegurar los servicios de aplicaciones en redes públicas.	X		La información que está relacionada con aplicaciones que pasa a través de redes públicas debe ser protegida de cualquier actividad fraudulenta.
A.14.1.3	Protección de las transacciones de servicios de aplicaciones.		X	No se aplica el control, no entra dentro de los objetivos del proyecto.
A.14.2 SEGURIDAD DE DESARROLLO Y EN LOS PROCESOS DE SOPORTE				
A.14.2.1	Política de desarrollo seguro.	X		Es importante establecer e implementar normas en la empresa para el desarrollo de los sistemas y aplicaciones.
A.14.2.2	Procedimiento de control de cambios en sistemas.	X		Es importante registrar las modificaciones efectuadas en los procesos con el fin de prevenir errores en el software y en los sistemas de información.

A.14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativos.	X		Cuando se realicen cambios en los sistemas operativos o las aplicaciones deben pasar por un proceso de revisión para garantizar que no existen efectos adversos.
A.14.2.4	Restricciones a los cambios en los paquetes de software	X		Verificar en las políticas que exista directrices para realización de cambios en el software.
A.14.2.5	Principios de ingeniería de sistemas seguros.		X	Establecer principios de ingeniería y entregar documentación pertinente no entra dentro de los objetivos de nuestro proyecto. Sin embargo, es importante que el departamento cuente con la aplicabilidad de este control.
A.14.2.6	Entorno de desarrollo seguro.	X		Es necesario establecer un entorno de desarrollo seguro que garantice la protección apropiada de los procesos y procedimientos proporcionados a todos los trabajadores.
A.14.2.7	Externalización del desarrollo de software.		X	El departamento de sistemas no trabaja con áreas externas de desarrollo de software.
A.14.2.8	Pruebas funcionales de seguridad de sistemas.	X		Es necesario llevar a cabo pruebas en los sistemas con el fin de confirmar y planificar minuciosamente las acciones que garanticen un funcionamiento óptimo durante todo el proceso de desarrollo del software.
A.14.2.9	Pruebas de aceptación de sistemas.	X		Es importante implementar planes de evaluación y normas correspondientes para

				sistemas de información recién creados, actualizados o mejorados. De esta manera se puede reducir el peligro y prevenir debilidades.
A.14.3 DATOS DE PRUEBA				
A.14.3.1	Protección de los datos de prueba.		X	No se aplica el control, no entra dentro de los objetivos del proyecto. El departamento de sistemas es el mayor encargado en estos controles.

Tabla 27. Matriz de Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

A.15 RELACIÓN CON PROVEEDORES				
A.15.1 SEGURIDAD EN LAS RELACIONES CON PROVEEDORES				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI	**NO**	
A.15.1.1	Política de seguridad de la información en relaciones con los proveedores.		X	Es fundamental que el departamento de sistemas controle el acceso a los proveedores y se debe exigir el cumplimiento de las políticas de seguridad existentes. Por motivos de información confidencial, no se elaborará dicha política.
A.15.1.2	Requisitos de seguridad en contratos con terceros.	X		Los requisitos relacionados con la seguridad de la información deben acordarse con los proveedores.
A.15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones.	X		Los acuerdos con los proveedores deben incluir requisitos para hacer frente a riesgos de seguridad de la información relacionados con las

				tecnologías de la información.
A.15.2 GESTIÓN DE LA PROVISIÓN DE SERVICIOS DEL PROVEEDOR				
A.15.2.1	Control y revisión de la provisión de servicios del proveedor.		X	No se aplica el control, no entra dentro de los objetivos del proyecto. El departamento de sistemas es el encargado de estos controles.
A.15.2.2	Gestión de cambios en la provisión del servicio del proveedor.			

Tabla 28. Matriz de Relación con los Proveedores

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN				
A.16.1 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y MEJORAS				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI	**NO**	
A.16.1.1	Responsabilidades y procedimientos.	X		Garantizar una respuesta efectiva y puntual ante incidentes de seguridad de la información es crucial. Para lograrlo, es necesario establecer claras responsabilidades y procedimientos de gestión adecuada.
A.16.1.2	Notificación de los eventos de seguridad de la información.	X		Establecer los canales de comunicación para todos los eventos o incidentes ocurridos en el departamento de sistemas. Es

				importante que los usuarios estén familiarizados con los mecanismos de notificación.
A.16.1.3	Reporte de puntos débiles de la seguridad.		X	El área técnica del departamento es el encargado de llevar a cabo estas actividades.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información.			
A.16.1.5	Respuesta a incidentes de seguridad de la información.	X		Establecer un procedimiento de respuesta de incidentes de seguridad.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información.	X		El aprendizaje adquirido al investigar y solucionar problemas de seguridad informática debe aplicarse para disminuir la posibilidad o las consecuencias de futuros incidentes.
A.16.1.7	Recopilación de evidencias.	X		Es necesario recolectar y preservar las pruebas de los incidentes de seguridad informática.

Tabla 29. Matriz para la Gestión de Incidentes

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO				
A.17.1 MANTENER LA SEGURIDAD DE LA INFORMACIÓN				
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**		**JUSTIFICACIÓN DE APLICABILIDAD/EX CLUSIÓN**
		SI	**NO**	
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	X		Se requiere mantener al día los manuales que contienen el plan de emergencia para cada uno de los servicios del departamento de Sistemas

				para garantizar la continuidad de las operaciones en caso de algún contratiempo.
A.17.1.2	Implementar la continuidad de la seguridad de la información		X	El departamento de sistemas debe documentar, mantener procesos y controles para asegurar el nivel requerido de seguridad de la información. Sin embargo, no entra de los objetivos del proyecto elaborar un documento que verifique la continuidad de procesos.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.		X	Comprobación de controles establecidos, no está establecido en los objetivos del proyecto.
A.17.2 REDUNDANCIAS				
A.17.2.1	Disponibilidad de los recursos de tratamiento de la información.	X		Se requiere incorporar mecanismos o procedimientos que garanticen la accesibilidad, autenticidad y privacidad de los datos y los sistemas informáticos, con el fin de minimizar peligros.

Tabla 30. Matriz de Continuidad del Negocio

A.18 CUMPLIMIENTO			
A.18.1 CUMPLIMIENTO DE LOS REQUISITOS LEGALES			
SECCIÓN	**CONTROLES ISO 27001**	**APLICABILIDAD**	**JUSTIFICACIÓN DE APLICABILIDAD/EXCLUSIÓN**
		SI / **NO**	

A.18.1.1	Identificación de la legislación aplicable.		X	No se tomará en cuenta la norma de cumplimiento, debido a que dentro del alcance del proyecto y los objetivos está establecido que no se llegará a la parte de implementación de un SGSI. Por lo tanto, no se hará énfasis en la revisión de documentación legal.
A.18.1.2	Derechos de propiedad intelectual. (DPI)			
A.18.1.3	Protección de los registros de la organización.			
A.18.1.4	Protección de los datos y privacidad de la información personal.			
A.18.1.6	Regulación de los controles criptográficos.			
A.18.2 REVISONES DE LA SEGURIDAD DE LA INFORMACIÓN				
A.18.2.1	Revisión independiente de la seguridad de la información.		X	No se tomará en cuenta la norma de cumplimiento, debido a que dentro del alcance del proyecto y los objetivos está establecido que no se llegará a la parte de implementación de un SGSI.
A.18.2.2	Cumplimiento de las políticas y normas de seguridad.			
A.18.2.3	Comprobación del cumplimiento técnico.			

Tabla 31. Matriz de Cumplimiento

2.10.3 Desarrollo de Verificación

Aquí se ejecutaron procedimientos de seguimiento y revisión de controles para las políticas sugeridas en la siguiente fase. A continuación, se presentaron formatos elaborados con la finalidad de cumplir con los controles y buenas prácticas de acuerdo a la norma ISO 27001 y garantizar la seguridad de la información en el

Departamento de Sistemas. Estos formatos incluyeron planes de acción, matrices de registros, respaldos, procedimientos de control de accesos, control de mantenimiento, entre otros.

Dentro de los procedimientos de seguimiento y revisión, se recomienda realizar un análisis periódico de los incidentes de seguridad reportados, las vulnerabilidades identificadas y las amenazas emergentes que pudieron impactar los activos de información. En base a ello, deben actualizarse las políticas y controles de seguridad para mantener un nivel de protección adecuado y adaptarse a los cambios del entorno. (Véase los controles aplicables a las políticas dentro del anexo 4)

2.10.4 Desarrollo fase Actuar

El departamento de Sistemas carece actualmente de un marco documentado de políticas de seguridad de la información. Aunque se llevan a cabo diversos procesos para proteger la información, estos apenas cumplen con algunas normas básicas, lo que no garantiza una adecuada seguridad de la información.

Por lo tanto, es fundamental desarrollar políticas de seguridad de la información que estén debidamente documentadas y comunicadas a todas las subdivisiones del Departamento de Sistemas. Este documento debe ser elaborado por personas relacionadas con la gerencia del departamento. Las recomendaciones basadas en ISO 27001 para la creación de políticas se describen a continuación:

2.10.4.1 Políticas de Seguridad conforme a la norma ISO 27001

A.5 Políticas de Seguridad de la información

A.5.1 Directrices de Gestión de Seguridad de la Información

Objetivo: Establecer buenas prácticas de seguridad de la información orientados a la protección de datos utilizados en los diferentes procesos del departamento, y así garantizar la integridad, confidencialidad, disponibilidad de la información.

Normas

- Elaborar documento que establezca las políticas de seguridad de la información, el cual servirá para capacitar al personal del Departamento de Sistemas y Recursos Tecnológicos sobre su adecuada aplicación.

- La documentación deberá ser desarrollada por el departamento de sistemas en conjunto con la alta gerencia de la entidad.
- Posteriormente, este documento será sometido a una revisión periódica, con el fin de que sea aprobado, modificado o desaprobado, según corresponda.
- Determinar los procedimientos necesarios para la operación del SGSI en el departamento de Sistemas, con el objetivo de asegurar la ejecución de actividades requeridas y proteger la información contra amenazas.

Definición de funciones y Responsabilidades de Seguridad

A.6 Organización de la seguridad de la información

A.6.1 Organización Interna

Objetivo: Establecer las funciones y obligaciones relacionadas con la seguridad de la información para todos los miembros del departamento de Sistemas y Recursos Tecnológicos del municipio, garantizando así la protección efectiva de los activos de información y el cumplimiento de los estándares ISO 27001.

Normas (Aplicar Formato 7)

- Definir las funciones y responsabilidades de cada miembro del área de Sistemas y Recursos Tecnológicos.
- Abarcar todas las actividades vinculadas a la protección de la información, detallando los procedimientos específicos de cada cargo.
- Asegurarse que todos los empleados entiendan sus responsabilidades en materia de seguridad y cómo se respaldan en el cumplimiento de los estándares ISO 27001.

A.6.2 Política de Dispositivos Móviles y Teletrabajo

Objetivo: Establecer políticas acerca del uso de dispositivos móviles y el trabajo remoto en el departamento de Sistemas, para garantizar la protección de recursos y el cumplimiento de los estándares de seguridad de la información.

Normas

- Determinar controles que regulen el uso de aparatos móviles, incluyendo teléfonos inteligentes y tablets, para el acceso a la red y la información empresarial.
- Establecer procedimientos para garantizar el acceso remoto a la infraestructura y datos del municipio, incluyendo el uso de redes privadas virtuales, autenticación de múltiples factores y otros sistemas de seguridad.
- Realizar capacitaciones para los trabajadores, enfocados en el aprendizaje de técnicas y peligros relacionados con el uso de dispositivos móviles y el trabajo remoto y así ayudar a promover una cultura de seguridad.
- Diseñar un sistema de gestión de incidentes regulares en dispositivos móviles y trabajo remoto, para garantizar una identificación e intervención oportuna ante posibles peligros o vulnerabilidades.

A.8 Gestión de Activos

A.8.1 Responsabilidad sobre los activos

Establecer un sistema de gestión que facilite la identificación y control efectivo de los recursos tecnológicos del departamento de Sistemas, para garantizar su uso apropiado y la protección de la información de acuerdo a las mejores prácticas y normas de seguridad.

Normas (Aplicar Metodología para la Gestión de Riesgos)

- Todos los activos de carácter físico, digital o de información, deben ser catalogados y almacenados en un registro centralizado.
- El registro debe contener información detallada sobre cada recurso, como su código, descripción, localización, custodio, valor y estado. Asegurando que exista un panorama claro acerca de los recursos utilizados.
- Los activos deben ser identificados, en función de su relevancia para el Departamento y verificar su grado de riesgo. Esto implica analizar la confidencialidad, integridad y accesibilidad de cada uno de estos elementos.
- Establecer reglas para el uso apropiado de los activos, determinar el manejo apropiado de los empleados y un control de devolución de los mismos. Estas

pautas deben abordar temas como el acceso autorizado, limitaciones en el uso personal, mantenimiento y notificación de incidentes.

- Verificar periódicamente el cumplimiento de estas directrices para garantizar su eficacia.

A.8.2 Política del uso Aceptable de Activos

Objetivo: Determinar un conjunto de normas donde se especifique el uso apropiado de los recursos de la organización para salvaguardar la integridad, confidencialidad y accesibilidad de la información en el Departamento de Sistemas y Recursos.

Normas (Aplicar Metodología para la Gestión de Riesgos)

- Solo el personal autorizado está permitido acceder y usar los activos del departamento.
- El acceso a dichos recursos debe limitarse únicamente a los empleados que tengan una necesidad justificada para su utilización.
- Los empleados no deben utilizar los recursos de la empresa para asuntos personales.
- Utilizar los bienes corporativos, como computadoras y laptops, para fines privados puede conllevar problemas de seguridad y disminuir la eficiencia operativa.
- Tomar las precauciones y medidas necesarias para proteger los bienes de la empresa ante cualquier daño, pérdida o robo. Las sanciones serán definidas por el gerente del departamento.
- Seguir lineamientos de mantenimiento e informar de inmediato cualquier fallo o desperfecto en el activo.
- Todo problema de seguridad o debilidad encontrada en los recursos debe ser comunicada de inmediato a la gerencia.
- Garantizar que toda la información se maneje de manera confidencial y solo se utilice para los fines aprobados.
- Acatar los acuerdos organizacionales sobre la protección de datos personales, evitar revelar información sin autorización y seguir los procedimientos para almacenar y eliminar datos de forma segura.

A.9 Política de Control de Acceso

Objetivo: Establecer normas para administrar y vigilar el acceso a los sistemas, programas y datos del departamento de Sistemas, garantizando que solo las personas autorizadas puedan acceder a los recursos requeridos para sus tareas y obligaciones.

Normas (Aplicar Formatos 1 y 6)

- Todas las personas que utilicen el sistema deben identificarse de manera segura, como mediante contraseñas fuertes, autenticación en dos pasos o credenciales digitales.
- Los permisos de acceso deben ser aprobados por las autoridades correspondientes y registrados de manera apropiada.
- Gestionar las identidades de todos los usuarios que acceden a los recursos del departamento.
- Administrar los permisos de acceso de cada persona, asegurando así la seguridad y el control adecuado de los recursos.
- Los privilegios de acceso a sistemas, deben revisarse regularmente para asegurar que los permisos se ajusten a las necesidades actuales del personal.
- Las revisiones de acceso deben realizarse al menos una vez al año y cuando se produzcan cambios importantes en las responsabilidades del personal.
- El ingreso a áreas sensibles, como centros de datos y cuartos de servidores, debe estar limitado solo a personal autorizado y protegido por medidas de seguridad física, como tarjetas de acceso, reconocimiento biométrico o vigilancia de seguridad.
- Todas las visitas de terceros deben ser registradas y estar acompañadas en todo momento por personal autorizado.

A.9.1 Política de Control de acceso a los servidores y a la Red

Objetivo: Determinar normas para regular y supervisar el ingreso a los servidores y la red de la organización, asegurando la protección de los recursos vitales y la información confidencial contra accesos ilegítimos y posibles riesgos.

Normas (Aplicar Formato 1)

- El jefe del Departamento de Sistemas, otorgará el permiso de acceso a los servidores y a la red.
- Para obtener este acceso, se debe presentar una solicitud al departamento de Sistemas del GAD-LIBERTAD.
- Esta solicitud deberá ser aprobada por el jefe del departamento. Es necesario monitorear los accesos de los usuarios a los servidores y sistemas de información, verificando que sean los previamente autorizados por el personal encargado.
- Establecer procedimientos para revocar los privilegios de acceso cuando sea necesario.
- Mantener un registro del acceso a los servidores de archivos y bases de datos.

A.9.3.1 Políticas de Gestión de Contraseñas

Objetivo: Determinar procesos para la generación y uso de contraseñas seguras, con el objetivo de salvaguardar los sistemas y los datos de la empresa contra ingresos no autorizados de terceros.

Normas (Aplicar Formato 2)

- La contraseña debe tener al menos 12 caracteres de los cuales incluir una mezcla de mayúsculas, minúsculas, números y símbolos especiales.
- Evitar el uso de información personal, como nombres de usuario, fechas de nacimiento o palabras comunes para la creación de contraseñas.
- Es importante que las contraseñas se actualicen con frecuencia, cada 90 días aproximadamente.
- Para mantener la seguridad, no se permite volver a usar las últimas cinco contraseñas. El cambio de contraseña debe ser una práctica obligatoria para proteger adecuadamente la información.
- Si el usuario detecta que su contraseña ha sido comprometida, debe informarlo de inmediato a la persona responsable de las cuentas de usuario.

- Las contraseñas de correo electrónico, red, servidores de archivos y bases de datos deben cumplir con los requisitos de uso establecidos.
- Los usuarios no deben permitir que los navegadores web guarden sus contraseñas.
- Se recomienda que los usuarios que manejan sistemas, aplicaciones o información delicada, utilicen gestores de contraseñas según su facilidad de uso.
- Evita anotar o guardar tus contraseñas en sitios visibles, como en el escritorio o documentos sin protección.
- Configurar las cuentas para que se bloqueen automáticamente después de cierto número de intentos fallidos de inicio de sesión (por ejemplo, cinco intentos consecutivos).
- Sólo el personal de soporte, el cual debe ser autorizado podrá desbloquear cuentas bloqueadas, previa verificación de la identidad del usuario.

A.9.4.5 Control de acceso al código fuente de los programas

Objetivo: Elaborar lineamientos para controlar el acceso al código fuente de los sistemas y aplicaciones desarrolladas por el departamento de Sistemas, garantizando que el código no sea vulnerado ni alterado por terceros.

Normas

- El acceso al código fuente debe otorgarse de acuerdo a los privilegios del empleado, dando solo los permisos necesarios para que el personal cumpla con la tarea específica.
- Cada solicitud de acceso debe estar debidamente fundamentada, registrada y autorizada por la persona responsable.
- El sistema recién creado debe pasar por una evaluación exhaustiva, con el fin de detectar y corregir cualquier falla o deficiencia.
- Es necesario diseñar un plan acción para llevar a cabo pruebas en los sistemas de información.
- Cualquier indicio de que el código fuente esté afectado debe notificarse de inmediato al equipo de Seguridad de la Información.

- Es necesario llevar a cabo una evaluación minuciosa y aplicar las acciones correctivas pertinentes para eliminar cualquier riesgo relacionado.

A.10 Política de uso de Controles Criptográficos

Objetivo: Determinar normas que regulen el uso de técnicas de criptografía, con el fin de garantizar la privacidad, integridad y autenticidad de la información, resguardándola de accesos no autorizados y posibles debilidades.

Normas (Aplicar Formato 4)

- Emplear procedimientos de técnicas criptográficas que se ajusten a los estándares de seguridad utilizados.
- Seguir protocolos de seguridad al generar, distribuir, almacenar, renovar y eliminar las claves.
- Utilizar módulos de seguridad de hardware o servicios en la nube para la gestión de claves, con el fin de garantizar su resguardo contra accesos no autorizados y alteraciones.
- Toda información importante como datos personales, financieros y de operaciones, debe estar protegida mediante cifrado cuando se guarda en servidores, bases de datos u otros medios de almacenamiento.
- Utilizar métodos de autenticación robustos y firmas electrónicas para confirmar la identidad y la integridad de las comunicaciones y documentos.
- Establecer procesos de auditoría para evaluar los controles criptográficos, identificar vulnerabilidades y garantizar el cumplimiento de las políticas de seguridad.
- Toda revisión debe documentarse, en caso de cualquier incumplimiento debe corregirse de inmediato.
- Tener un plan establecido para enfrentar eventos de seguridad vinculados a la criptografía, como procedimientos para la revelación de claves criptográficas.

A.11 Política de Seguridad Física y del Ambiente

A.11.1 Áreas Seguras

Objetivo: Determinar procedimientos de protección contra peligros externos y del ambiente, con el fin de garantizar el funcionamiento continuo y la confiabilidad de los sistemas.

Normas (Aplicar Formato 7)

- Contar con medidas de seguridad que restrinjan el acceso únicamente a personal autorizado. En caso de ser necesario incluir tarjetas de identificación, cerraduras electrónicas y sistemas biométricos.
- Los edificios y centros de datos deben estar construidos con materiales resistentes para soportar eventos naturales como temblores e inundaciones.
- Establecer estrategias para la reducción de peligros medioambientales que puedan impactar la seguridad y funcionalidad de los sistemas informáticos.
- El departamento debe contar con sistemas de detección de incendios en todas las áreas principales, como rociadores automáticos y extintores de dióxido de carbono, para evitar daños provocados por el fuego.

A.11.2 Seguridad de los equipos

Objetivo: Establecer lineamentos para asegurar la protección física de los equipos en el departamento de Sistemas y Recursos Tecnológicos, con el fin de protegerlos de accesos no permitidos, daños, robos y otros riesgos.

Normas (Aplicar Formato 8)

- Elaborar un manual de mantenimiento de equipos informáticos, a cargo del departamento de Sistema, el cual se actualizará cada cierto tiempo. Para garantizar el correcto funcionamiento, control de protección de la información y prolongar su vida útil.
- El departamento de Sistemas, será responsable de verificar la seguridad de los equipos informáticos ante cualquier eventualidad imprevista. Para ello, se creará un documento que detalle los procedimientos a seguir en caso de incidentes.

- Desarrollar un plan de mejora continua en la gestión de la información, con el fin de mantener una pantalla limpia y salvaguardar la información crítica del departamento de Sistemas.

A.12 Seguridad de las operaciones

A.12.2 Política de Protección contra software malicioso (Malware)

Objetivo: Emplear normas para salvaguardar los datos de la empresa, protegiéndolos de software dañino y asegurar la confidencialidad, integridad y accesibilidad de la información.

Normas (Aplicar Formato 12)

- El uso de antivirus debe estar aprobado previamente por el Departamento de Sistemas. La instalación de otro tipo de antivirus está prohibida a menos que existe una autorización previa.
- Es fundamental que el antivirus se instale en todos los dispositivos del departamento, desde los servidores hasta las computadoras de los empleados.
- Mantener actualizado el antivirus es importante para garantizar una protección eficaz contra las nuevas amenazas que puedan surgir.
- Configurar el firewall, para permitir únicamente el tráfico de red indispensable para las operaciones de la organización. Todo el tráfico que no sea esencial debe bloquearse, con el fin de disminuir posibles ataques.
- El antivirus debe tener la capacidad de gestionar los servicios. Los usuarios no deben abrir correos electrónicos de origen dudoso.
- Siempre se debe escanear con el antivirus los dispositivos de almacenamiento interno y externo.
- En caso de que una computadora se infecte, se debe desconectar de la red y limpiarla por personal calificado.
- Evitar el uso de medios de almacenamiento y carpetas compartidas con acceso de lectura y escritura, para disminuir el riesgo de que se introduzcan y ejecuten archivos dañinos en la red.

A.12.3 Política de Copias de Seguridad

Objetivo: Determinar un procedimiento relacionado con el respaldo de datos, para asegurar la continuidad de procesos y garantizar la recuperación rápida de la información en caso de pérdida o daño.

Normas (Aplicar Formato 5)

- Recopilar información importante del departamento de sistemas como, programas, bases de datos y archivos de usuario.
- Establecer redundancia en otros servidores y localizaciones, en caso de que existan algún desastre natural, estar protegidos con copias de seguridad fuera de la entidad.
- Determinar un tiempo específico para realizar las copias de seguridad, teniendo en cuenta su importancia y susceptibilidad a cambios.
- La rotación de las copias de seguridad debe ser fundamental, para asegurar que las antiguas se eliminen o archiven de forma segura.
- Establecer un plan de recuperación ante incidentes, que indique los pasos a seguir en caso de pérdida de datos, incluyendo la restauración de las copias de seguridad y reanudación de operaciones.

A.12.4 Política de Control de Software

Objetivo: Establecer políticas para el control de software dentro de la organización, con el fin de asegurar la seguridad, integridad, y eficiencia de los recursos informáticos.

Normas (Aplicar Formato 9)

- Realizar una lista de programas informáticos utilizados dentro de la empresa, incluyendo sistemas operativos, aplicaciones y herramientas.
- Elaborar un registro del software usado en la organización, incluyendo información como nombres, versiones, licencias y fechas de instalación.
- Establecer un sistema de control de licencias de software para asegurar el uso y cumplimiento de los términos de las mismas.

- Utilizar herramientas de monitoreo de software, para la detección del uso de software no autorizado o desactualizado.
- Establecer un proceso seguro para eliminar el software que ya no se necesita o que está obsoleto.
- Implementar medidas de seguridad física y digital para proteger el software y los datos de la organización.

A.13 Seguridad de las Comunicaciones

A.13.1 Política de Gestión de Seguridad en las redes y Servidores

Objetivo: Establecer políticas de gestión de seguridad en redes y servidores de la empresa, para reducir los riesgos de ciberataques y asegurar la continuidad de las actividades empresariales.

Normas (Aplicar formato 1)

- Monitorización de las redes LAN dentro y fuera del departamento de TI.
- Verificar el uso adecuado de seguridad y funcionamiento NAT en el direccionamiento IP.
- Control del uso apropiado de antivirus y firewall en los equipos.
- El firewall debe tener reglas restrictivas que bloqueen el tráfico de red, permitiendo solo lo necesario para los servicios requeridos.
- Monitorizar los puertos abiertos en los servidores para detectar amenazas y corregirlas de inmediato por el personal de Redes.
- Seguimiento de los puertos abiertos para identificar actividad de servicios y evitar accesos no autorizados al servidor.
- Cerrar los puertos innecesarios no utilizados para prevenir intrusiones en el servidor.
- Análisis de vulnerabilidades en servidores y estaciones de trabajo para detectar posibles riesgos a la seguridad de la información.

A.13.2 Política del Uso de Correo Electrónico

Objetivo: Establecer normas para el uso del correo electrónico dentro de la empresa, fomentando el uso ético de este medio de comunicación y así resguardar la información confidencial de la organización.

Normas (Aplicar Formato 3)

- Los correos electrónicos asignados a los empleados del departamento, deben utilizarse únicamente para asuntos laborales relacionados con los objetivos de la organización.
- Comunicar la política de uso de correo electrónico a todo el personal de la organización.
- Brindar capacitaciones recurrentes acerca de la política de uso de correo electrónico y las mejores prácticas para un uso responsable.
- Establecer vías de comunicación para que el personal pueda reportar infracciones de la política de uso de correo electrónico.
- El correo electrónico proporcionado a los trabajadores del departamento, pertenecen al GAD-LIBERTAD. Estos recursos son de uso exclusivo de la empresa y no deben ser utilizados para fines personales.
- Aplicar medidas correctivas a quienes no cumplan con la política de uso de correo electrónico.

A.13.3 Política de Intercambio de Información y Recursos compartidos

Objetivo: Definir lineamientos para compartir información dentro del departamento de sistemas, para proteger los recursos de información y mejora de las operaciones laborales.

Normas (Aplicar Formato 6)

- Definir canales de comunicación para intercambio de información dentro del departamento de sistemas, como correo electrónico, herramientas de reuniones presenciales.
- Establecer medidas de seguridad para proteger información confidencial durante la transmisión, incluyendo controles de acceso, cifrado y protección contra malware.

- Promover una cultura de transparencia, en el intercambio de información, fomentando la colaboración y el trabajo en equipo.
- Minimizar el uso de canales de comunicación no oficiales, para intercambio de información confidencial.
- Verificar el cumplimiento de la política de intercambio de información y detectar posibles incumplimientos.

A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información

A.14.1 Política para la Gestión de los Sistemas de Información

Objetivo: Definir un marco para la administración de los sistemas de información dentro del departamento de Sistemas, asegurando que se alineen con las metas estratégicas de la organización y optimizar los recursos de los activos informáticos.

Normas (Aplicar Formato 11)

- Es importante realizar un seguimiento constante de los sistemas de información que se encuentran en fase de prueba.
- Crear un directorio de gestión de los sistemas de información, donde se registren y detallen las especificaciones de cada uno de los sistemas desarrollados.
- Organizar un equipo encargado de supervisar y cumplir con las pautas de gestión de los sistemas de información.
- En caso de necesitar recursos para la administración adecuada de dichos sistemas, como personal, presupuesto y herramientas, se le otorgará facilidad de acceso.
- Actualizar los documentos que describen las políticas, los procedimientos y los planes de acción relacionados con la administración de los sistemas de información.

A.14.2 Política de Desarrollo Seguro

Objetivo: Determinar políticas para el ciclo de vida del software, aplicando métodos de identificación, y mitigación de vulnerabilidades, con el fin de proteger los recursos de la organización y entregar productos de software confiables.

Normas (Aplicar Formato 10)

- La seguridad debe ser parte fundamental en todas las fases del proceso de desarrollo de software, desde la etapa inicial hasta su implementación y mantenimiento.
- Cada proyecto de desarrollo debe tener una evaluación de riesgos, lo que permitirá diseñar un plan efectivo para abordarlos y prevenirlos.
- Las pruebas de seguridad como el análisis de vulnerabilidades y prueba de accesos, se realizarán en un período determinado durante el desarrollo y antes de poner en marcha cualquier aplicación o sistema.
- Los problemas de seguridad encontrados deben solucionarse antes de que el software esté listo para ser utilizado.
- El ingreso a los ambientes de desarrollo, pruebas y producción debe estar restringido únicamente a personal autorizado.
- Aplicar técnicas de gestión de acceso para asegurar que solo los usuarios aprobados puedan acceder a los recursos de desarrollo.

A.16 Gestión de Incidentes

Objetivo: Definir procesos para informar, responder y resolver problemas de seguridad en el GAD-LIBERTAD, con el objetivo de reducir el impacto en las actividades de la compañía y perfeccionar continuamente la posición de seguridad.

Normas (Aplicar Formato 13)

- Todos los trabajadores tienen la obligación de informar de inmediato al equipo de Seguridad de la Información sobre cualquier sospecha o confirmación de un evento que pueda afectar la seguridad.
- Los reportes del incidente deben enviarse a través de los canales de comunicación designados, como correo electrónico, o una línea directa para reportar incidentes.
- Todos los eventos reportados deben documentarse en un sistema centralizado de gestión de problemas.

- Los eventos deben categorizarse según su nivel de gravedad y su posible efecto en las actividades de la organización, utilizando una escala establecida previamente (por ejemplo, alto, medio, bajo).
- Es necesario tener un plan establecido para responder a los incidentes, el cual debe contener instrucciones precisas sobre cómo eliminar y restaurar la situación.
- El equipo designado para el tratamiento de incidentes, debe activarse de inmediato para la resolución del problema.

2.10.4.2 Cumplimiento de Normas

El Departamento de Sistemas y Recursos Tecnológicos del GAD-LIBERTAD, será responsable de revisar todos los controles y las mejoras sugeridas previamente. Como objetivo, se elaboró un documento que contiene dichas políticas que servirán como guía para la implementación del SGSI, el documento debe ser actualizado constantemente dentro de la organización y así garantizar la seguridad en el departamento.

Es importante realizar un seguimiento en todas las áreas, asegurando el cumplimiento de los controles y políticas establecidas, con el fin de mantener una adecuada protección de la información. Si alguna política o norma del departamento no se cumple, deberán aplicarse sanciones de acuerdo a su reglamento.

CONCLUSIONES

- La identificación de los activos informáticos y los posibles riesgos en el departamento de Sistemas del GAD-LIBERTAD, permitió obtener una visión clara de la situación actual de la seguridad de la información en la entidad. Al realizar el inventario de los activos tecnológicos, se ha facilitado la identificación de los recursos más críticos y su importancia para el funcionamiento continuo de los procedimientos municipales.
- El análisis de riesgos ha revelado vulnerabilidades y amenazas que podrían comprometer la integridad, disponibilidad y confidencialidad de la información bajo su gestión. Los equipos informáticos como el servidor que fue auditado, muestran falencias y vulnerabilidades que pueden ser explotadas por atacantes, tales como phishing, virus y malware, así como también tener expuesta información que es confidencial para el departamento y poner en riesgo la seguridad de la información.
- Determinar una metodología de gestión de riesgos adaptada al contexto organizacional, es importante para seguir un paso a paso sustentado en algo que ya se realizó, también mejora la capacidad del departamento para abordar los riesgos de forma efectiva, fortalecer la protección de los activos informáticos y fomentar una cultura de seguridad constante, lo que mejora significativamente la seguridad de la información en el departamento de Sistemas.
- La elaboración de la declaración de aplicabilidad, nos ha dado una base firme para el desarrollo de la guía de implementación del Sistema de Gestión de Seguridad de la Información (SGSI). Este proceso permitió determinar qué controles específicos de la norma son relevantes y necesarios para el contexto de la organización, garantizando que las medidas tomadas, se alineen con las mejores prácticas de seguridad de la información.
- Las recomendaciones establecidas en base a la norma ISO 27001, proporcionan una guía clara para el desarrollo de políticas efectivas que se adapten a las necesidades y el contexto del departamento de Sistemas. Esto a su vez, mejora la capacidad del departamento para gestionar riesgos,

proteger información confidencial y responder de manera adecuada a incidentes de seguridad.

- Al adherirse a los lineamientos y sugerencias de la norma ISO 27001, se logró obtener recursos clave, que permitieron fortalecer la protección de la información en la organización. Esta guía de implementación sirve para obtener la certificación y poner en marcha el SGSI, garantizando que todos los elementos de la seguridad informática sean tratados de manera correcta.
- La guía de implementación del SGSI brindó un fundamento para la gestión de la seguridad de la información en el departamento de Sistemas del GAD-LIBERTAD. Además, asegura un progreso constante en sus prácticas de seguridad. Lo que coloca al departamento en una posición más favorable para hacer frente a riesgos y amenazas, garantizando la integridad, confidencialidad y disponibilidad de la información procesada.

RECOMENDACIONES

- En la bibliografía revisada, mencionan que existen 10 fases que deben cumplirse para la implementación de un SGSI, de las cuales, para el desarrollo del proyecto solo se hizo énfasis en 4 de ellas, que son fundamentales a la hora de implementar el SGSI según diversos autores. En caso de solicitar una certificación ISO 27001, es necesario seguir el desarrollo de las 10 fases mencionadas, para asegurar el cumplimiento de todos los requisitos y cumplir con los objetivos propuestos.
- Para un mejor resultado en el análisis de vulnerabilidades al servidor, se recomienda obtener los datos, con otro tipo de herramientas y realizar una comparativa entre los resultados obtenidos. Como por ejemplo utilizar OpenVas para el escaneo de vulnerabilidades y también Net Scan para el escaneo de puertos. Además, el análisis de vulnerabilidades debería ser realizado a todos los servidores de la entidad para un mejor tratamiento en los resultados, sin embargo, por motivos de privacidad y confidencialidad, no se tuvo acceso a todos los servidores de la entidad.
- La metodología de gestión de riesgos utilizada en el proyecto es en base a otros autores con sus respectivos trabajos de investigación, sin embargo, se recomienda realizar una comparativa de otras metodologías de gestión de riesgos como SCRAMM, OCTAVE, NIST SP 800-30, MAGERIT entre otras y en base a ello elegir la más adecuada al contexto del SGSI.
- Dentro de la declaración de aplicabilidad, se utilizaron todos los controles especificados en el anexo A de la ISO 27002, dejando de lado los controles de cumplimiento que están relacionados con el uso de las políticas cumplidas y revisión del SGSI ya establecido, es por ello que, en caso de que la entidad tenga establecido un SGSI y quiera obtener la certificación, se debe hacer uso de la cláusula 18 del anexo A y verificar el funcionamiento del mismo.
- Para el tratamiento de riesgos de los activos se recomienda realizar un mapa de calor donde se determine si el tipo de riesgo es alto, medio o bajo. Es recomendable sustentar su respuesta en base a dicha información.

- Dentro de la metodología de gestión de riesgos, específicamente en el apartado de gestión de activos, se recomienda realizar el mismo procedimiento con los activos relacionados con el software, como sistemas específicos, aplicaciones y herramientas importantes, entre otros.

REFERENCIAS

[1] C. K. Paguay Lema and G. E. Zamora Arana, "Auditoría de la Seguridad Informática basado en la ISO 27001 Sistema de Gestión de Seguridad de la Información para el GAD Municipal de Milagro," *Repositorio de la Universidad Estatal de Milagro*, 2017, Accessed: Apr. 28, 2024. [Online]. Available: http://repositorio.unemi.edu.ec/xmlui/handle/123456789/3845

[2] C. De and I. De Sistemas, "Elaboración de una guía de implementación de un SGSI para la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia - CEDIA," 2022, Accessed: May 29, 2024. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/22091

[3] "Repositorio Institucional de la UNAM." Accessed: Apr. 28, 2024. [Online]. Available: https://repositorio.unam.mx/contenidos/auditoria-informatica-en-los-procesos-administrativos-del-departamento-de-informatica-de-chocolatera-moctezuma-sa-305816?c=B7XgXA&d=false&q=*:*&i=1&v=1&t=search_0&as=0

[4] R. L. Chagmana Pomaquero, "Auditoría informática aplicando la Norma ISO 27001 para optimizar la seguridad de la información en el Departamento de Tic's del Centro de Investigación y Desarrollo FAE.," 2022, Accessed: Apr. 28, 2024. [Online]. Available: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/35566

[5] N. Kelly, B. Molina, and R. Bailón Sánchez Autorizamos A La, "Análisis en seguridad informática y seguridad de la información basado en la norma ISO/IEC 27001- sistemas de gestión de seguridad de la información dirigido a una empresa de servicios financieros," 2015, Accessed: Apr. 30, 2024. [Online]. Available: http://dspace.ups.edu.ec/handle/123456789/10372

[6] "ISO 27001 - Certificado ISO 27001 punto por punto - Presupuesto Online." Accessed: Jun. 01, 2024. [Online]. Available: https://normaiso27001.es/#h3

[7] P. por, A. Novoa, and H. Clara Isabel, "[Metodología para la implementación de un SGSI en la fundación universitaria Juan de Castellanos, bajo la norma

ISO 27001: 2005],” Feb. 2015, Accessed: Jun. 01, 2024. [Online]. Available: https://reunir.unir.net/handle/123456789/3129

[8] I. De Un *et al.*, “ESCUELA POLITÉCNICA NACIONAL FACULTAD DE INGENIERÍA EN SISTEMAS”.

[9] “Implementar ISO 27001 Paso a Paso- 5 ¿Que Documentar y por qué?” Accessed: Jun. 02, 2024. [Online]. Available: https://normaiso27001.es/fase-5-documentacion-del-sgsi/

[10] “Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 | Revista Tecnológica - ESPOL.” Accessed: Apr. 28, 2024. [Online]. Available: https://rte.espol.edu.ec/index.php/tecnologica/article/view/456

[11] N. P. Becerra Arévalo, “Auditoria informática basada en norma ISO 27004 para el control del parque tecnológico de Uniandes Puyo,” 2017, Accessed: Apr. 28, 2024. [Online]. Available: https://dspace.uniandes.edu.ec/handle/123456789/7415

[12] “Plan de Creación de Oportunidades 2021-2025 – Secretaría Nacional de Planificación.” Accessed: Apr. 28, 2024. [Online]. Available: https://www.planificacion.gob.ec/plan-de-creacion-de-oportunidades-2021-2025/

[13] F. Moreno and F. Moreno, “La Libertad,” *www.lalibertad.gob.ec*, Accessed: Jun. 06, 2024. [Online]. Available: http://www.lalibertad.gob.ec/index.php?option=com_content&view=article&id=131&Itemid=76

[14] “Transparencia LOTAIP.” Accessed: Jun. 06, 2024. [Online]. Available: https://www.cpccs.gob.ec/transparencia-lotaip-2/

[15] “Reglamento a Ley Orgánica de Protección de Datos Personales – Ministerio de Telecomunicaciones y de la Sociedad de la Información.” Accessed: Jun. 07, 2024. [Online]. Available: https://www.telecomunicaciones.gob.ec/ley-y-reglamento-de-la-ley-de-proteccion-de-datos-personales/

[16] Ley, “LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES”, Accessed: Jun. 06, 2024. [Online]. Available: www.lexis.com.ec

[17] O. G. Muñoz Pinto, “Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indigena SAC,” 2020, Accessed: Apr. 28, 2024. [Online]. Available: https://repositorio.uta.edu.ec:8443/jspui/handle/123456789/31305

[18] C. DE Ahorro Y Crédito San Francisco Ltda, “UNIVERSIDAD TÉCNICA DE AMBATO”.

[19] F. J. Valencia-Duque and M. Orozco-Alzate, “Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000”, doi: 10.17013/risti.22.73-88.

[20] M. Catherine and O. Quezada, “FACULTAD DE CIENCIA Y TECNOLOGÍA ESCUELA DE INGENIERÍA ELECTRÓNICA Implementación de la norma ISO/IEC 27001 para seguridad del Data Center del GAD Municipal del Cantón Cuenca. Trabajo de graduación previo a la obtención del título de: INGENIERA ELECTRÓNICA Autora,” 2016.

[21] “Diseñar un Sistema de Gestión de la Seguridad de la Información para la Empresa Qwerty S.A a partir de la Norma ISO 27001.” Accessed: Apr. 28, 2024. [Online]. Available: https://repository.unad.edu.co/handle/10596/34624

[22] V. Ejecutiva, “UNIVERSIDAD DE GUADALAJARA”.

[23] P. De Seguridad, “POLITICAS DE SEGURIDAD,” 2017.

[24] J. CHACON and S. RUGEL, “Artículo de Revisión. Teorías, Modelos y Sistemas de Gestión de Calidad,” *Revista ESPACIOS*, vol. 39, no. 50, Dec. 2018.

[25] J. J. Cano, “Seguridad de la Información en Latinoamérica Tendencias 2009.” Accessed: Jun. 16, 2024. [Online]. Available: https://www.acis.org.co/archivos/Revista/110/05investigacion1.pdf

[26] G. R. D. L. C. Rodríguez, R. A. M. Fernández, and A. C. M. D. L. Santos, “Seguridad de la información en el comercio electrónico basado en ISO 27001 : Una revisión sistemática,” *Innovación y Software*, vol. 4, no. 1, pp. 219–236, Mar. 2023, doi: 10.48168/innosoft.s11.a79.

[27] D. Alan Neill and L. Cortez Suárez, “Procesos y Fundamentos de la Investigación Científica,” *J Chem Inf Model*, vol. 53, no. 9, p. 125, 2018, Accessed: Apr. 28, 2024. [Online]. Available: http://repositorio.utmachala.edu.ec/handle/48000/12498

[28] G. P. G. Alban, A. E. V. Arguello, and N. E. C. Molina, “Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción),” *RECIMUNDO*, vol. 4, no. 3, pp. 163–173, Jul. 2020, doi: 10.26820/RECIMUNDO/4.(3).JULIO.2020.163-173.

[29] N. Teodoro and E. Nieto, “Tipos de Investigación,” *Universidad Santo Domingo de Guzmán*, Jun. 2018, Accessed: Apr. 30, 2024. [Online]. Available: http://repositorio.usdg.edu.pe/handle/USDG/34

[30] J. Martínez Ramos, “Sistema de gestión para mejorar la seguridad de la información en la institución servicios industriales de la marina,” *Universidad Nacional del Santa*, 2014, Accessed: Jun. 01, 2024. [Online]. Available: http://repositorio.uns.edu.pe/handle/20.500.14278/1943

[31] “Ciclo PDCA: ¿cuáles son los pasos y cómo funciona? Conoce algunos ejemplos | Blog SYDLE.” Accessed: Apr. 28, 2024. [Online]. Available: https://www.sydle.com/es/blog/ciclo-pdca-61ba2a15876cf6271d556be9

[32] “Nmap: Análisis de puertos y monitorización de redes - ICM.” Accessed: Apr. 28, 2024. [Online]. Available: https://www.icm.es/2022/05/06/nmap-analisis-de-puertos-y-monitorizacion-de-redes/

[33] A. Laura and H. Saucedo, “Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web”.

[34] U. DE Politécnica Cartagena, A. Barquero Pastor Director, M. Dolores Cano Baños Codirector, and I. Alexander Bello Tasic, “Estudio comparativo entre OpenVas y Wazuh,” 2022, Accessed: Apr. 28, 2024. [Online]. Available: https://repositorio.upct.es/handle/10317/11663

[35] M. Pareja Aparicio, “El banco de pruebas Virtual Box para sistemas operativos,” *Manual formativo de ACTA, ISSN 1888-6051, Nº. 60, 2011, págs. 71-77*, no. 60, pp. 71–77, 2011, Accessed: Apr. 28, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=5724679&info=resumen&idioma=SPA

[36] O. I. Moscaiza Moncada, “Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013,” *Universidad Peruana de Ciencias Aplicadas (UPC)*, Feb. 2018, Accessed: Jun. 16, 2024. [Online]. Available: https://repositorioacademico.upc.edu.pe/handle/10757/623063

[37] D. Arturo and A. Mollehuanca, “Diseño de un sistema de gestión de seguridad de información para servicios postales del Perú S.A.,” Oct. 2014, Accessed: Jun. 15, 2024. [Online]. Available: https://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/5677

[38] M. James Navarro and D. Gainza Reyes, “Procedimientos de seguridad informática relativos a los recursos humanos,” *Serie Científica de la Universidad de las Ciencias Informáticas, ISSN-e 2306-2495, Vol. 14, Nº. 7, 2021 (Ejemplar dedicado a: : Julio), págs. 108-122*, vol. 14, no. 7, pp. 108–122, 2021, Accessed: Jun. 16, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8590661&info=resumen&idioma=ENG

[39] F. Mera Amores, “PROPUESTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001. CASO DE ESTUDIO: EMPRESA ALTAC.” Accessed: Jun. 16, 2024. [Online]. Available:

https://repositorio.puce.edu.ec/server/api/core/bitstreams/2795b614-d9ee-4206-8695-05395d184ddd/content

[40] “PROTOTIPO DE SISTEMA EXPERTO PARA LA GENERACIÓN DE NORMAS, POLÍTICAS Y PROCEDIMIENTOS DE SEGURIDAD BASADOS EN LAS NORMAS ISO 17799 E ISO 27001 DENTRO DE UN ENTORNO ORGANIZACIONAL ‘PSEP’ | Revista Vínculos.” Accessed: Jun. 16, 2024. [Online]. Available: https://revistas.udistrital.edu.co/index.php/vinculos/article/view/4108

[41] “Controles del Anexo A de ISO 27001: guía completa actualizada a la versión de 2022.” Accessed: Jun. 16, 2024. [Online]. Available: https://www.escuelaeuropeaexcelencia.com/2023/03/controles-del-anexo-a-de-iso-27001-guia-completa-actualizada-a-la-version-de-2022/

[42] “SGSI.” Accessed: Jun. 16, 2024. [Online]. Available: https://www.iso27000.es/sgsi.html

[43] “Propuesta de un Modelo de un Sistema de Gestión de Calidad en Seguridad | Eumednet.” Accessed: Jun. 16, 2024. [Online]. Available: https://www.eumed.net/rev/rilco/05/gestion-instituciones.html

[44] I. M. Angel and Z. Sanchez, “Análisis comparativo sobre las herramientas de Seguridad Informática Open Source: Nessus y Snort.,” 2022, Accessed: Jun. 13, 2024. [Online]. Available: http://dspace.utb.edu.ec/handle/49000/11622

[45] S. De, G. De, S. De, L. A. Información En, L. A. Municipalidad, and D. De Pira, “Sistema de gestión de seguridad de la información en la municipalidad distrital de pira aplicando la norma iso/iec 27001:2013,” *Universidad Católica Los Ángeles de Chimbote*, Jul. 2019, Accessed: Jun. 05, 2024. [Online]. Available: https://repositorio.uladech.edu.pe/handle/20.500.13032/11993

ANEXOS

Anexo 1: Árbol de Problemas

Anexo 2: Formulario Entrevista y Encuesta

Formulario de la entrevista

Objetivo: Verificar el grado de conocimiento y cumplimiento de las políticas de seguridad de la información por parte del personal del departamento de TI.

Preguntas para el encuestado	Respuestas
1. ¿Existen políticas que gestionen la seguridad de la información actualmente?	
2. ¿Se presentan riesgos informáticos en la empresa y cuál es el más constante?	
3. ¿Los usuarios se encuentran capacitados para el uso de los recursos tecnológicos?	
4. ¿Los sistemas informáticos han sido víctimas de robo de información?	
5. ¿Existen controles sobre el acceso al personal interno y externo al equipamiento y sistemas que maneja dentro de la institución?	
6. ¿Cuál es el proceso que se lleva a cabo para la gestión y administración de los activos informáticos de la empresa?	
7. ¿Se realizan tareas de monitoreo a los sistemas de información con los empleados del departamento?	
8. ¿Usted conoce acerca de algún Sistema de Gestión de Seguridad de la Información (SGSI)?	.

9. ¿Cree usted que se debería realizar una Auditoría Informática dentro del departamento de TI?	

Formulario de la Encuesta

Objetivo: Verificar el grado de conocimiento, cumplimiento y eficacia de las políticas de seguridad de la información establecidas en el departamento de TI, en línea con los requisitos y principios de la norma ISO/IEC 27001.

1.- ¿Con que políticas de seguridad para la gestión de la información cuenta actualmente el departamento de TI?

☐ a) Control de acceso

☐ b) Seguridad de Física

☐ c) Seguridad ambiental

☐ d) Seguridad de la información

☐ e) Ninguna

2.- ¿Se aplica algún proceso o técnica de seguridad para el cuidado y uso de la información?

☐ a) Firewall

☐ b) Control de usuario

☐ c) NAT

☐ d) Ninguno

☐ e) Otro

3.- ¿Se presentan problemas en los equipos de cómputo de la entidad que conlleven a la perdida de la información?

☐ a) Siempre

☐ b) Ocasionalmente

☐ c) Nunca

4.- ¿Cada que tiempo se realizan mantenimientos de tipo preventivo y correctivo de los equipos informáticos de la empresa?

☐ a) 1 vez al mes

☐ b) cada 2 meses

☐ c) Cada 6 meses

☐ d) Anualmente

5.- ¿Se lleva un control adecuado para el inventario de activos informáticos del departamento?

☐ a) Si

☐ b) No

☐ c) Ocasionalmente

6.- ¿Se realizan tareas de monitoreo a los sistemas de información en conjunto con los empleados?

☐ a) Siempre

☐ b) Ocasionalmente

☐ c) Nunca

7.- ¿Los sistemas informáticos que maneja la entidad presentan fallos o irregularidades?

☐ a) Siempre

☐ b) Ocasionalmente

☐ c) Nunca

8.- ¿Cuál es el nivel de conocimiento en seguridad de la información del personal en el Departamento de TI?

☐ a) Bajo

☐ b) Medio

☐ c) Alto

9.- ¿Cada que tiempo se realizan backups o copias de seguridad de la información?

☐ a) Diario

☐ b) Semanalmente

☐ c) Mensualmente

☐ d) Anualmente

☐ e) Otro

10.- ¿Existen fallos en las redes de internet durante la transmisión de datos?

☐ a) Siempre

☐ b) Ocasionalmente

☐ c) Nunca

11.- ¿Con que frecuencia se actualizan los Sistemas Operativos y las aplicaciones?

☐ a) Siempre

☐ b) Ocasionalmente

☐ c) Nunca

Anexo 3: Documento del Alcance del SGSI

DOCUMENTO PARA EL ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Código	
Versión:	
Fecha:	
Elaborado por:	
Aprobado por:	
Nivel de Confidencialidad:	

HISTORIAL DE MODIFICACIONES

Fecha	**Versión**	**Descripción de la Modificación**

Misión del Departamento

Administrar eficientemente los recursos tecnológicos, mediante la utilización de tecnologías de información y la automatización de procesos, a través de la web institucional, servicios informáticos, redes, equipos de computación para el procesamiento automático de datos, acceso a la información y seguridad de los sistemas informáticos, a fin de apoyar de manera eficaz el desarrollo tecnológico y gestión municipal y la toma de decisiones en beneficio de la colectividad del cantón.

Objetivo, alcance y usuarios

El objetivo del alcance es definir claramente los límites del Sistema de Gestión de Seguridad de la Información (SGSI) en el Departamento de Sistemas y Recursos Tecnológicos del GAD Municipal de La Libertad.

El presente documento se aplica a toda la documentación y actividades dentro del SGSI. Los usuarios del documento son los miembros de la dirección de Sistemas y Recursos Tecnológicos y los miembros del equipo del proyecto que integra el SGSI.

- Jefa del Departamento
- Área Técnica
- Área de Desarrollo
- Bases de Datos
- Área de Redes
- Programadores e Ingenieros

Documentos de Referencia

- Norma ISO/IEC 27001, cláusula 4.3
- Guía de Implementación del Sistema de Gestión de Seguridad de la Información, basado en ISO 27001.
- Lista de requisitos legales, normativos, contractuales y de otra índole.

Definición del alcance del SGSI

La organización necesita establecer los límites del sistema de gestión de seguridad de la información (SGSI) para determinar qué información debe protegerse. Esta información debe estar almacenada dentro o fuera del alcance del SGSI. Además, se deben considerar aspectos fundamentales como los activos informáticos, el nivel de organización, los recursos y las áreas que requieren protección y procesamiento interno.

El responsable de definir y delimitar el alcance del SGSI será el/la gerente del Departamento de Sistemas, en conjunto con los directivos de la entidad, de acuerdo a los servicios, procesos y sistemas en los que se maneja información relacionada con la seguridad de activos. Al definir el SGSI, se tendrán en cuenta los siguientes aspectos:

Procesos y Servicios

(Determinar los servicios y/o procesos del departamento que se incluyen en el alcance)

Unidades Organizativas

(Especificar las unidades organizativas o subdivisiones del departamento que tendrán acceso a la documentación)

Ubicaciones

(Determinar las ubicaciones que están incluidas o no dentro del alcance y como es la separación de las demás ubicaciones.)

Limitaciones del Alcance

(Especificar elementos o recursos del departamento que no formarán parte del alcance del SGSI)

Validez del documento

El presente documento será válido hasta (fecha)

El propietario del alcance del SGSI del Departamento de Sistemas y Recursos Tecnológicos es **el/la** (cargo), que debe corroborar el documento y en caso de necesitar una actualización hacerlo respectivamente por lo menos **frecuencia adaptada a la necesidad del departamento.**

(Cargo)

(Nombre)

_____

Firma

Anexo 4: Documentación y Controles de la Fase de Verificación

Formato 1. Control de acceso a los Servidores de archivos y bases de datos

CONTROL DE ACCESO A LOS SERVIDORES

Versión:
Fecha:
Código:

N	Usuario	Correo	Cargo	IP Usuario	IP Servidor	Fecha inicio	Fecha fin	Servicio	Estado (Activo/Inactivo)

Firma responsable **Gerente del Departamento**

Formato 2. Creación de usuarios y contraseñas

FORMATO DE CREACIÓN DE USUARIOS Y CONTRASEÑAS

Fecha:
Departamento:
Nombre del responsable:
Cargo:

Nombre	Cargo	Perfil de Usuario	Nombre de usuario	Dirección IP/ Sistemas Operativo (en caso de Equipos informáticos)	Contraseña	Detalle

Tipos de Solicitud del usuario

☐ Creación de usuarios ☐ Reactivación ☐ Modificación ☐ Eliminación

Perfiles de usuario para creación de contraseñas

-Equipos Informáticos -Correos Institucionales -Sistemas de Información

_____ _____

Firma responsable **Gerente del Departamento**

Formato 3. Informe de Uso de correo Electrónico

INFORME PARA EL USO DE CORREO ELECTRÓNICO

Versión:
Fecha:
Código:

Datos de usuario		**Datos del equipo**		**Seguridad relacionada al correo**
Nombre:	Apellido:	Nombre del equipo:	Dirección IP:	Borrado de Spam: ☐ Sí ☐ No
Cargo:	Correo:	Sistema Operativo:	Características:	Antivirus integrado con correo ☐ Sí ☐ No
Celular:				Medio de respaldo:

Observaciones

_____
_____
_____

_____

Firma del responsable

Formato 4. Registro del uso de Criptografía

REGISTRO DE USO CRIPTOGRÁFICO **Versión:** **Fecha:** **Código:**				
Usuario	**Tipo de datos Protegido**	**Uso de cifrado Sí/No**	**Método Criptográfico Utilizado**	**Frecuencia de uso**

Firma responsable **Gerente del Departamento**

Métodos Criptográficos Utilizados

- AES-256: Se utiliza para cifrar documentos confidenciales y garantizar que únicamente los usuarios autorizados tengan acceso a la información.
- RSA-2048: Se utiliza principalmente para cifrar correos electrónicos. Esto garantiza que la comunicación se mantenga privada, ya que solo se hace accesible para los destinatarios reales.
- SHA-256: Se usa para firmas digitales. Las firmas aseguran la autenticidad y la integridad de los documentos.
- TLS 1.2: Se utiliza para transacciones en línea. El componente garantiza que todos los datos transmitidos estén protegidos y, por lo tanto, todos cifrados.

- PGP: es un componente de cifrado que se usa para comunicaciones externas. La parte protege la comunicación con la información previamente enviada fuera de la organización.

Formato 5. Proceso para realizar respaldo de la Información

CONTROL DE RESPALDO DE INFORMACIÓN (BASES DE DATOS)						
Código: **Versión:** **Fecha Elaboración:**						
Servidor	Nombre Base de datos	Tamaño de la base	Fecha Restauración	Nombre del archivo	Resultado Satisfactorio Si/No	Firma del responsable
Observaciones: _____ _____						

_____ _____

Firma responsable **Gerente del Departamento**

Formato 6. Control para el Acceso a los recursos compartidos

CONTROL DE LOS RECURSOS COMPARTIDOS EN RED **Versión:** **Fecha:** **Código:**	
Datos de responsable	**Datos de Solicitante**
Departamento:	Departamento:
Nombre y Apellido:	Nombre y Apellido:
Teléfono:	Teléfono:
Correo:	Correo:
Datos del Recurso	
Nombre de Servidor:	
Ruta a la cual se quiere acceder:	

Datos del Usuario		
N	Nombres y Apellidos	Permisos Asignados
		☐ Lectura ☐ Escritura ☐ Denegación
		☐ Lectura ☐ Escritura ☐ Denegación
		☐ Lectura ☐ Escritura ☐ Denegación

Firma responsable **Gerente del Departamento**

Formato 7. Documento para la asignación de roles y responsabilidades

ASIGNACIÓN DE ROLES Y RESPONSABILIDADES EN EL DEPARTAMENTO DE SISTEMAS Y RECURSOS TECNOLÓGICOS					
Fecha elaboración: **Versión:** **Código:**					
Nombre	Responsabilidad	Rol	Autoridad	Habilidades	Actividad

Firma responsable **Gerente del Departamento**

Formato 8. Reportes de Mantenimiento de Equipos

REPORTE DE MANTENIMIENTO DE EQUIPOS **Versión:** **Fecha:** **Código:**	
Datos Generales	**Datos del Cliente**
Nombre de la empresa:	**Nombre cliente:**
Responsable del trabajo:	**Responsable:**
Área de trabajo:	**Dirección:**
Dirección:	**Teléfono:**
Correo:	**Correo:**

Descripción			
Cantidad	**Descripción**	**Marca**	**Condiciones Técnicas**

Observaciones del Mantenimiento

Firma responsable **Gerente del Departamento**

Formato 9. Solicitud de instalación de Software

INFORME DE INSTALACIÓN DE SOFTWARE **Versión:** **Fecha:** **Código:**		
Responsable del equipo	**Responsable de la instalación**	**Detalle del Equipo Informático**
Nombre y Apellido:	Nombre y Apellido:	Nombre Equipo:
Cargo:	Cargo:	Marca/Modelo:
Correo:	Correo:	Código del inventario:
Departamento:		
Detalle del Software requerido		
Nombre:		
Versión:		
Fecha instalación:		
Código licencia:		
Base de Datos:		

En caso de solicitar instalación de otro software, escribirlos a continuación:

1. _____
2. _____
3. _____
4. _____

_____ _____

Firma responsable **Gerente del Departamento**

Formato 10. Pruebas de sistemas y software

FORMATO PARA PRUEBAS DE SISTEMAS Y SOFTWARE **Versión:** **Fecha:** **Código:**			
Prueba del Software			
Fecha elaboración		Prerrequisitos de la Prueba	Recursos de la Prueba
Fecha aplicación			
Tipo de prueba			
Código de prueba			
Descripción			
Resultados de la Prueba			
Defectos		Posible solución	
Observaciones			

Firma responsable **Gerente del Departamento**

Formato 11. Directorio de Sistemas de Información

DIRECTORIOS DE SISTEMAS DE INFORMACIÓN **Versión:** **Fecha:** **Código:**	
Característica	**Detalle**
Nombre Sistema	
Nombre del Servicio	
Categoría	
Tipo	
Proveedor	
Estado	
Tipo Licencia	
Fecha expiración licencia	
Plataforma	
Ubicación del servidor de archivos	
Base de Datos	
Responsable Base de Datos	

Firma responsable **Gerente del Departamento**

Formato 12. Informe Utilización de Antivirus en los Equipos

Informe de Utilización de Antivirus **Versión:** **Fecha:** **Código:**	
Características	**Detalle**
Nombre de Equipo	
Dirección IP	
Sistema Operativo	
Usuario del Equipo	
Departamento	
Tipo Licencia	
Protección en tiempo real	
Actualización Automática	
Observaciones	

Firma responsable **Gerente del Departamento**

Formato 13. Procedimiento para la Gestión de Incidentes

DESCRIPCIÓN DE PROCEDIMIENTO	
Actividad	**Detalle**
Detectar y reportar el incidente	**Responsable:** Cualquier funcionario que detecte el incidente.
Categorizar el Incidente	Si se verifica que el informe describe un incidente real, entonces se debe clasificar el incidente dentro de la categoría apropiada: • Virus • Incidente Acceso Físico • Problema de red • Fallo en las comunicaciones • Incidentes humanos • Incidentes con aplicativos • Incidentes con bases de datos
Documentar el incidente	Si el reporte no corresponde a un incidente de seguridad: • Documentar en el formato las razones por las cuales no se considera un incidente de seguridad. • Notificar a quien corresponda para realizar las acciones necesarias de acuerdo con el problema real para resolverlo. • Documentar en la Bitácora de Incidentes de Seguridad de la Información, archiva el formato correspondiente y cierra del incidente.
Definir las acciones correctivas	El área de Seguridad de la Información evalúa si el incidente afecta a la Organización y su nivel de impacto, considerando lo siguiente: a) BAJO: Si el incidente es único y solo afecta a un equipo interno o asociado. b) MEDIO: Si el incidente afecta las operaciones internas, se considera un evento que puede representar una

	amenaza futura, pero no se considera una amenaza grave o inmediata. c) ALTO: En caso de que el incidente sea muy crítico, donde representa una amenaza seria y afecte de manera inmediata a recursos importantes o ponga en riesgo información confidencial, y además involucre a usuarios externos, se considera de alto nivel. Si el incidente se catalogó como de alto o medio nivel, se conforma un equipo para atenderlo, incluyendo a los especialistas identificados en la fase de detección, considerando el tipo de recursos afectados y el nivel de especialización requerido.
Ejecutar plan de acción	• Notifica a los involucrados las medidas a seguir. • Lleva a cabo las acciones registradas según el tipo de incidente identificado y el impacto definido. • Determina el grado de daño causado a los recursos informáticos o información de la Entidad, mediante un análisis exhaustivo de los sistemas afectados y documentando los hallazgos y daños detectados. • Confirma los recursos informáticos, servicios y entidades afectadas directa o indirectamente por el incidente, incluyendo la identificación preliminar de los especialistas (internos / externos) que podrían responder al incidente.