UNIVERSIDAD CATÓLICA DE CUENCA

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SERVICIOS TECNOLÓGICOS EN EL GADIPCS SUSCAL, USANDO COMO REFERENCIA LA NORMA ISO/IEC 27002:2016

TRABAJO DE TITULACIÓN PREVIO

A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: DIANA JAKELINE ZAMORA POMAQUIZA.

DIRECTOR: ING. DANNY PATRICIO ANDRADE CÁRDENAS.

CAÑAR - ECUADOR

2023

DIOS, PATRIA, CULTURA Y DESARROLLO

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE INFORMÁTICA, CIENCIAS DE LA COMPUTACIÓN E INNOVACIÓN TECNOLÓGICA

CARRERA DE INGENIERÍA EN SISTEMAS DE INFORMACIÓN

AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SERVICIOS TECNOLÓGICOS EN EL GADIPCS SUSCAL, USANDO COMO REFERENCIA LA NORMA ISO/IEC 27002:2016

TRABAJO DE TITULACIÓN PREVIO

A LA OBTENCIÓN DEL TÍTULO DE INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR: DIANA JAKELINE ZAMORA POMAQUIZA.

DIRECTOR: ING. DANNY PATRICIO ANDRADE CÁRDENAS.

CAÑAR - ECUADOR

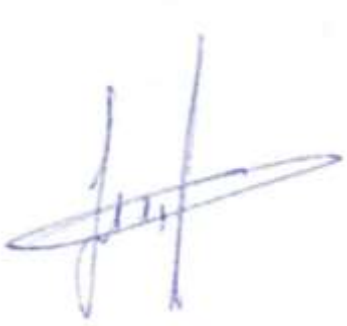
2023

DIOS, PATRIA, CULTURA Y DESARROLLO

DECLARACIÓN

Yo, Diana Jakeline Zamora Pomaquiza, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluyen en este documento.

La Universidad Católica de Cuenca extensión Cañar puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y la Normativa actual de la institución.

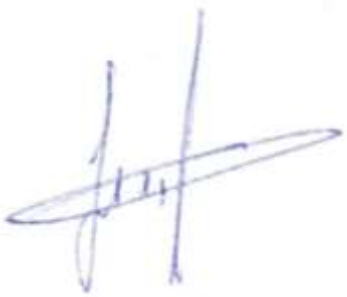


Zamora Pomaquiza Diana Jakeline

C.I: **0302867742**

RESPONSABILIDAD

“La responsabilidad del contenido de esta tesis de grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Universidad Católica de Cuenca Extensión Cañar”.



Zamora Pomaquiza Diana Jakeline

C.I: **302867742**

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por la Estudiante Diana Jakeline Zamora Pomaquiza, bajo mi supervisión.

_____

Ing. Danny Andrade Cárdenas, Mgs.

DIRECTOR DEL TRABAJO INVESTIGATIVO

UNIVERSIDAD CATÓLICA DE CUENCA EXTENSION CAÑAR

DEDICATORIA

A mis padres, de manera especial a mi madre Mélida Pomaquiza por su apoyo y comprensión incondicional.

Este logro no habría sido posible sin su apoyo constante, palabras de aliento a lo largo de esta trayectoria. Gracias por haberme inculcado, el esfuerzo y la perseverancia, dedico esta tesis con todo mi cariño, gracias por ser mi guía a lo largo de esta travesía académica.

A todos los que han hecho posible la realización de este trabajo. por su compañía, su apoyo y su ánimo. Gracias por estar siempre ahí para mí, y por hacerme reír y disfrutar de la vida.

AGRADECIMIENTO

A Dios por haberme dado la fortaleza para cumplir con cada una de mis metas.

Agradezco a mis padres, Rolando Zamora y Mélida Pomaquiza, a mi tía Mercedes Pomaquiza, por su amor, apoyo y comprensión incondicionales. Impulsándome así a alcanzar mis metas, gracias por su apoyo financiero y emocional, lo que me ha permitido concentrarme en mi educación, quiero dedicarles este trabajo como testimonio de gratitud y sacrificio, este logro es su logro y lo celebro en su honor; sin ustedes nada de esto hubiera sido posible.

Agradezco a BTS, porque mediante su música y sus mensajes me han servido como fuente constante de inspiración en mi vida, pudiendo así encontrar consuelo en mis mejores y peores momentos. Además, la dedicación y el compromiso de BTS con su arte y con sus seguidores ha sido un ejemplo de perseverancia y excelencia. Con su duro trabajo y enfoque en la autenticidad son lecciones que he llevado conmigo a lo largo de todo este proceso.

Agradezco a mi amiga Michaelle Narváez, quien ha sido mi apoyo infinito, tus palabras de ánimo y de aliento me han impulsado a superar y perseverar en este viaje académico, en momentos de duda siempre estabas para recordarme mi capacidad. Sin ti este camino hubiera sido más difícil. Gracias por ser una amiga muy increíble y formar parte de esta etapa tan importante de mi vida.

Agradezco a la Universidad Católica de Cuenca extensión Cañar, por la oportunidad de estudiar y realizar esta investigación. Gracias por brindarme los recursos y el apoyo necesarios para alcanzar mis metas.

A los docentes de la Carrera de Ingeniería de Sistemas de Información, les agradezco por su dedicación y compromiso con la educación.

De manera especial, deseo expresar mi agradecimiento al Ing. Danny Patricio Andrade Cárdenas, Mgs., director de mi trabajo de titulación. Gracias por por su guía, apoyo y paciencia durante todo el proceso de investigación y redacción de esta tesis. Su orientación ha sido fundamental para el desarrollo de este trabajo.

RESUMEN

En el marco del proyecto, se propone efectuar una auditoria de seguridad, abarcando aspectos físicos y lógicos, de los sistemas tecnológicos del GADIPCS Suscal. El propósito primordial es identificar vulnerabilidades que comprometen la solidez de los servicios tecnológicos institucionales. El proyecto se inició estableciendo un marco teórico con los ítems relacionadas al tema de investigación. Posteriormente, se definieron y ejecutaron las fases de la auditoría. Para diagnosticar la postura de seguridad actual de la municipalidad, se aplicó una entrevista y una prueba de cumplimiento (Check list) alineada a la norma ISO 27002. A fin de evaluar la adhesión a controles o políticas de seguridad, se recurrió al check list. Con base en esta, se elaboró una matriz de riesgos que permitió discernir los niveles de exposición resultantes de la falta de implementación de ciertos controles. Al concluir, se generó un informe de la evaluación, en el cual se especifican las observaciones identificadas acompañadas de sus correspondientes sugerencias de mejora.

***Palabras Clave*:** norma ISO 27002, matriz de riesgos, auditoría de seguridad, vulnerabilidades, fases de auditoría.

ABSTRACT

As part of the project, it is proposed to conduct a security audit covering both physical and logical aspects of the Autonomous Decentralized Intercultural and Participative Decentralized Government of the Suscal canton (GADIPCS by its Spanish acronym) technological systems. The primary purpose is to identify vulnerabilities that compromise the robustness of institutional technological services. The project began by establishing a theoretical framework with the items related to the research topic. Subsequently, the audit phases were defined and executed. In order to diagnose the current security posture of the municipality, an interview and a compliance test (Checklist) aligned to the ISO 27002 standard were applied. The checklist was used to assess adherence to security controls or policies. Based on the checklist, a risk matrix was developed to discern the levels of exposure resulting from the lack of implementation of specific controls. At the end of the assessment, an evaluation report was generated, specifying the observations identified and their corresponding suggestions for improvement.

Keywords: ISO 27002 standard, risk matrix, security audit, vulnerabilities, audit phases

Índice de Ilustraciones

Índice de tablas

ÍNDICE

INTRODUCCIÓN

La tecnología y la información han tomado un papel central en las operaciones de instituciones gubernamentales en todo el mundo. La seguridad de estos sistemas tecnológicos, tanto a nivel físico como lógico, se ha convertido en un imperativo para garantizar la eficiencia operativa, la protección de datos sensibles y el cumplimiento normativo. La norma ISO/IEC 27002:2016 es un estándar internacional que proporciona las mejores prácticas para la gestión de la seguridad de la información. Incluye recomendaciones para establecer políticas de seguridad, organizar la seguridad de la información, gestionar activos, controlar el acceso, asegurar los sistemas de criptografía, garantizar la seguridad física, gestionar incidentes de seguridad y realizar revisiones de la seguridad de la información, entre otras áreas. En esencia, establece las pautas para que las organizaciones implementen, mantengan y mejoren continuamente la seguridad de su información.

El propósito de esta investigación es realizar una auditoría exhaustiva de la seguridad física y lógica de los servicios tecnológicos en el GADIPCS Suscal, con el propósito de determinar posibles áreas de perfeccionamiento y asegurar la adhesión a las pautas establecidas en la norma ISO/IEC 27002:2016. Así, se busca apoyar el refuerzo de las capacidades de seguridad de la información de GADIPCS Suscal, un paso vital para para salvaguardar la solidez, accesibilidad y privacidad de sus datos.

A continuación, se ofrece un resumen conciso de los capítulos incluidos en el documento:

Capítulo I: Hace mención al marco referencial, mismo que abarca la explicación del problema de investigación, antecedentes, objetivos, limitaciones y delimitaciones.

Capítulo II: Incluye una sección teórica en la que se introducen y explican ideas y términos asociados con la auditoría en el ámbito informático.

CAPÍTULO I

MARCO DE REFERENCIA

1. Descripción de la situación Problemática

El departamento de Tecnologías de la Información (TI) es un área crítica en las organizaciones gubernamentales, públicas y privadas que manejan información sensible y confidencial. El Gobierno Autónomo Descentralizado Intercultural y Participativo (GADIPCS) del cantón Suscal perteneciente a la provincia de Cañar - Ecuador, cuenta con un departamento de TI encargado de gestionar y mantener sus sistemas de información. Sin embargo, existe una falta de evaluación regular de la seguridad física y lógica de los servicios tecnológicos del departamento de TI del GADIPCS Suscal.

Esta falta de evaluación puede resultar en la exposición de información confidencial y privada a riesgos de seguridad informática, así como la falta de eficiencia y efectividad en los procesos de la organización. Por lo tanto, es necesario realizar una auditoría informática en el departamento de TI del GADIPCS Suscal para evaluar y optimizar sus recursos informáticos, además de presentar propuestas de acciones que pueden reducir riesgos.

1.1. Formulación del Problema

El Gobierno Autónomo Descentralizado Intercultural y Participativo (GADIPCS) del cantón Suscal perteneciente a la provincia de Cañar depende cada vez más de sus servicios tecnológicos para desempeñar sus funciones. Sin embargo, la seguridad física y lógica de estos servicios podría no estar adecuadamente asegurada, lo que podría poner en riesgo la solidez de la información y la efectividad de los de los servicios proporcionados por GADIPCS Suscal.

En base a esta premisa, se formulan las siguientes cuestiones:

- ¿Cuál es el estado actual de la seguridad física y lógica de los servicios tecnológicos en GADIPCS Suscal?
- ¿Qué áreas de la seguridad de los servicios tecnológicos en GADIPCS Suscal necesitan ser mejoradas para cumplir con la norma ISO/IEC 27002:2016?
- ¿Qué acciones específicas se pueden tomar para mejorar la seguridad de los servicios tecnológicos en GADIPCS Suscal de acuerdo con la norma ISO/IEC 27002:2016?

1.2. Antecedentes de la investigación

García (2019), en su trabajo titulado "Auditoría Informática basada en el marco de referencia Cobit 4.1 aplicada al área de calidad del departamento de tecnología del Banco Diners Club del Ecuador, en el periodo de enero – diciembre del año 2018". Utiliza la herramienta Cobit Quickstart, con el fin de establecer la situación actual del área determinada, es así que se concluye que se debe generar un plan de mejora continua, gestionando las necesidades de acuerdo a las normas y políticas de calidad. Este documento sirve para analizar las normas que conducen a llevar de mejor manera los procesos y aplicarlos en la investigación, tomando en cuenta la herramienta que el autor utiliza, para en este caso evaluar los procesos del GADIPCS de Suscal.

Una auditoría informática realizada por García (2020), analiza las normas ISO 27001, 27001 y el marco de trabajo COBIT 2019, utiliza un enfoque mixto para realizar el trabajo de investigación. Aplicando tanto una encuesta como una entrevista a los encargados del departamento de TI para recabar información, de esta forma concluye que la organización no lleva de manera adecuada las normas de seguridad informática. Este trabajo permite así analizar las preguntas realizadas al departamento de TI de las

encuestas y entrevistas, siendo estas una línea base para realizar las encuestas a las responsables del departamento de TI del GADIPCS de Suscal.

Abellán & Pardo (2020) realizan una auditoría a la "Sindicatura de Comptes de la Comunidad Valenciana en España", utilizando un análisis documental, determinan las políticas de seguridad informática de la compañía con el fin de consolidar los procesos que se realizan en el área de TI. Así los autores ultiman que las herramientas que la organización utiliza se deben monitorear constantemente basándose en normas de ciberseguridad.

Este documento sirve de guía para realizar las fases de la auditoría en el departamento de TI del GADIPCS de Suscal.

Así mismo, Morán (2022), realiza una revisión tecnológica empleando el estándar COBIT 2019 en el departamento de TI de la Congregación de Hermanas Dominicanas de la Inmaculada Concepción en la ciudad de Quito. Con el propósito de salvaguardar la información, el autor realiza un inventario de los sistemas y los softwares utilizados. De esta manera este documento sirve de referencia para analizar el marco de referencia COBIT 2019, este análisis será utilizado en la investigación para realizar una matriz comparativa de los marcos de la auditoría informática.

1.3. Fundamentación del estudio

La tecnología de la información es fundamental para el funcionamiento de cualquier organización gubernamental, especialmente para aquellas que manejan información sensible y confidencial. En este sentido, el Gobierno Autónomo Descentralizado Intercultural y Participativo (GADIPCS) del cantón Suscal de la provincia de Cañar cuenta con un departamento de TI encargado de gestionar y mantener sus sistemas de información.

No obstante, es importante señalar que hoy en día existe un aumento significativo en los riesgos de seguridad informática, tales como el robo de datos, el malware, el phishing, entre otros. De igual manera, el riesgo de errores humanos, la insuficiencia y deficiencia en las operaciones de la organización también pueden influir notablemente en la eficacia y la capacidad de respuesta del departamento de TI del GADIPCS Suscal.

Por lo tanto, es fundamental llevar a cabo una auditoría informática para evaluar y mejorar la seguridad, eficiencia y efectividad de los sistemas de información utilizados por el departamento de TI del GADIPCS Suscal. Esta evaluación permitirá identificar posibles riesgos y vulnerabilidades, y proponer medidas y acciones necesarias para asegurar la protección de los datos, mejorar la eficiencia y efectividad en los procesos, y garantizar el cumplimiento normativo de la organización.

1.4. Objetivos

1.4.1. Objetivo General

Realizar una auditoría de la seguridad física y lógica de los servicios tecnológicos en el GADIPCS Suscal, usando como referencia la norma ISO/IEC 27002:2016

1.4.2. Objetivos Específicos

- Efectuar una investigación conceptual sobre las normas y metodologías relacionadas a la auditoria informática
- Realizar una planificación de la auditoría de la seguridad física y lógica de los servicios tecnológicos del GADIPCS en base a la norma ISO 27002:2016

- Identificación de posibles brechas de seguridad y vulnerabilidades, y recomendación de medidas de mitigación para proteger los activos de información críticos.
- Creación de un informe de auditoría con los hallazgos de la revisión y las sugerencias pertinentes.

1.5. Limitaciones

- Falta de recursos y personal con la formación adecuada para llevar a cabo la auditoría en conformidad con la norma ISO/IEC 27002:2016.
- Resistencia por parte del personal que no entienda la importancia de la auditoría de seguridad o que vea el proceso como una amenaza para su posición.
- Acceso a la información, debido a restricciones legales, de privacidad o simplemente porque la información no es accesible o resulta complicada de obtener.

1.6. Delimitaciones

La presente investigación se elaborará en beneficio del El Gobierno Autónomo Descentralizado Intercultural y Participativo (GADIPCS) del cantón Suscal perteneciente a la provincia de Cañar. Se entrevistará a ciertos miembros del personal, es decir los encargados de supervisar la protección o los encargados de los servicios tecnológicos. El tiempo para llevar a cabo el desarrollo de la auditoría será de 3 meses.

CAPÍTULO II

MARCO TEÓRICO

2.1. Gestión de Seguridad de la Información

Se trata de un grupo de directrices y procedimientos para la administración sistemática de los esfuerzos de una entidad para minimizar y gestionar los riesgos a sus activos de información. (Solano, Ardila, & Ardila, 2022)

De acuerdo con Vega (2021):

El objetivo principal de la gestión de la seguridad de la información es garantizar la confidencialidad, integridad y disponibilidad de los datos y sistemas de información de una organización. Estos tres elementos se conocen como el "Triángulo CIA" tal como se visualiza en la ilustración Nº 1.:

Ilustración 1: *Triangulo CIA;* ***Fuente****: obtenido de https://juancenteno.info/cia/*

1. **Confidencialidad:** Hace alusión a salvaguardar los datos evitando que individuos o grupos sin permiso puedan acceder a ellos.

2. **Integridad**: Se refiere a asegurar que los datos son exactos y completos, sin haber sufrido alteraciones de manera no autorizada.

3. **Disponibilidad**: hace referencia que los datos y los sistemas están accesibles para los usuarios autorizados cuando lo necesiten.

2.1.1. Seguridad Informática

La seguridad informática es el campo que, apoyándose en directrices y reglamentos tanto internos como externos de una organización, tiene como objetivo salvaguardar la integridad y confidencialidad de los datos almacenados en sistemas digitales. Esta protección se establece frente a diversas amenazas, reduciendo las vulnerabilidades tanto de índole física como digital a las que estos sistemas puedan estar sujetos. (Baca Urbina, 2016)

2.1.2. Vulnerabilidades, Riesgo y Amenazas

En un mundo cada vez más interconectado, entender la seguridad es fundamental. La terminología puede ser confusa, pero al dividir la seguridad en tres conceptos clave: vulnerabilidades, riesgo y amenazas, podemos empezar a desglosar las complejidades de este tema. Las **vulnerabilidades** son debilidades que pueden ser explotadas por agentes maliciosos; las **amenazas** son los posibles ataques o eventos que aprovechan esas vulnerabilidades; y el **riesgo** es la probabilidad y el impacto potencial de que esas amenazas se materialicen.

2.1.2.1. Vulnerabilidad

Es un suceso o acción que da lugar a la realización de una amenaza. La vulnerabilidad se presenta cuando la protección es insuficiente para prevenir que una amenaza se materialice. (Baca Urbina, 2016)

2.1.2.2. Riesgo

El riesgo representa la probabilidad de que ocurra un incidente crucial. Al evaluarlo, podemos determinar las medidas necesarias para minimizar la amenaza y mantenerla dentro de límites aceptables.

Estos riesgos se contrarrestan con la implantación de controles, es decir medidas que se deben llevar a cabo para cumplir con dicho objetivo.

- **Riesgos Lógicos:**

  Los riesgos vinculados a la tecnología de los sistemas de información impactan directamente en su software y pueden ser complicados de identificar. Las perturbaciones que generan en la operación habitual del sistema pueden causar daños que no se pueden remediar en el sistema. (Collado, 2015)

- **Riesgos Físicos**

  "Se engloban en este punto aquellos riesgos, de alguna manera, pueden impactar la continuidad de los procesos empresariales de la organización al comprometer la disponibilidad de la información, que es su recurso más valioso" (Collado, 2015, pág. 56)

2.1.2.3. Amenazas

Las amenazas de un sistema informático pueden ser explotadas desde un atacante remoto mediante la utilización de un troyano, o a través de software malicioso que compromete las defensas del sistema, facilitando la infiltración de agentes malintencionados. (Collado, 2015)

2.2. Norma ISO/IEC 27001

El estándar ISO 27001 es una referencia global en lo que respecta a la administración de la seguridad informática. Proporciona las directrices y procedimientos

óptimos para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) dentro de cualquier entidad. El propósito principal de la ISO 27001 es asegurar la privacidad, coherencia y acceso oportuno a los datos, además de administrar eficientemente los riesgos asociados con la protección de dicha información.(nqa, 2019).

La implementación de la norma ISO 27001 ayuda a las organizaciones a establecer un marco sólido para proteger la información confidencial y gestionar los riesgos de seguridad de la información. También proporciona confianza a los clientes y socios comerciales, demostrando el compromiso de la organización con la seguridad de la información y las mejores prácticas reconocidas internacionalmente. (Quizhpe, 2017)

2.3. Norma ISO/IEC 27002:2016

"Proporciona directrices para normas organizacionales de seguridad de la información y para las prácticas de gestión de seguridad de la información, incluyendo la selección, implementación y gestión de los controles, teniendo en cuenta los riesgos del entorno de seguridad de la información de una determinada organización" (INTECO, 2023, pág. 1).

- **Beneficios de la norma**

  La norma ISO/IEC 27002, al proporcionar directrices y mejores prácticas para la gestión de la seguridad de la información, ofrece una serie de beneficios para las organizaciones (Méndez Gálvez, 2020). Estos beneficios incluyen:

- Incremento en la conciencia sobre la protección de datos;
- Refuerzo en la gestión de activos e información valiosa;
- Proporciona un marco para establecer controles y políticas;
- Permite detectar y solucionar vulnerabilidades;

- Minimiza el peligro de incurrir en faltas por no establecer un SGSI o por no definir políticas adecuadas;
- Se posiciona como un valor agregado en el mercado, atrayendo a clientes que aprecian dicha certificación;
- Conduce a una organización más estructurada con procedimientos y estrategias bien articulados;
- Ayuda a reducir gastos previniendo episodios de fallos en la seguridad informática;
- Asegura el cumplimiento de leyes y otras normativas pertinentes.

2.4. Seguridad física y lógica

2.4.1. Seguridad física

Se refiere a las medidas de protección diseñadas para prevenir el acceso físico no autorizado a recursos sensibles, tales como equipos informáticos, redes, y bases de datos. Las medidas de seguridad física pueden incluir cerraduras, sistemas de alarma, cámaras de vigilancia, control de acceso con tarjetas de identificación o biométricos, guardias de seguridad, vallas, y otras barreras físicas. También puede implicar medidas de protección contra desastres naturales o accidentes, como incendios, inundaciones, o cortes de energía (Medrano Padilla, 2022)

2.4.2. Seguridad lógica

Postigo (2020) define a la seguridad lógica como las medidas de protección que limitan el acceso a los recursos de información a través de software, datos o transmisión de red. Esto implica el uso de firewalls, software antivirus, encriptación, autenticación de usuarios, control de acceso basado en roles, y otras técnicas de seguridad de TI. El objetivo es proteger la integridad, confidencialidad y disponibilidad de los datos y

prevenir ataques cibernéticos, como el malware, el phishing, el hacking, o la denegación de servicio.

2.5. Auditoría Informática

La revisión de sistemas informáticos, comúnmente llamada evaluación de sistemas de información o auditoría de TI, es un proceso que evalúa y examina la infraestructura de tecnología de la información de una organización, las operaciones de TI y los procesos de control de información para determinar si son eficientes, efectivos, seguros y en cumplimiento de las políticas, estándares, leyes y regulaciones establecidos (Imbaquingo, Díaz, Saltos, & Arciniega, 2020)

2.5.1. Auditoría de la seguridad física

La auditoría de la seguridad física es un proceso que evalúa y examina las medidas y controles de seguridad implementados para proteger los activos físicos de una organización. Estos activos pueden incluir instalaciones, edificios, equipos, recursos humanos y cualquier otro elemento físico que sea importante para la operación y continuidad del negocio.

Durante una auditoría de seguridad física, se llevan a cabo las siguientes actividades:

1. **Evaluación de controles de acceso**: Se revisan los sistemas de control de acceso físico, como cerraduras, tarjetas de acceso, controles biométricos, cámaras de vigilancia, y se verifica si están funcionando correctamente y si se aplican adecuadamente.
2. **Revisión de políticas y procedimientos**: Se examinan las políticas y procedimientos relacionados con la seguridad física, como la gestión de visitantes, el manejo de llaves, los procedimientos de respuesta a emergencias y

la protección de activos valiosos. Se verifica si están actualizados y si se siguen adecuadamente.

3. **Inspección de instalaciones**: Se realiza una evaluación física de las instalaciones para identificar posibles vulnerabilidades, como puntos débiles en la seguridad perimetral, deficiencias en el diseño de la infraestructura física, acceso no autorizado a áreas restringidas, entre otros.

4. **Análisis de sistemas de vigilancia**: Se evalúa la efectividad de los sistemas de vigilancia, como cámaras de seguridad, alarmas de intrusión, sistemas de detección de incendios y sistemas de monitoreo. Se verifica su funcionamiento, cobertura y capacidad para detectar y responder a incidentes.

5. **Verificación de seguridad de activos físicos**: Se evalúa la protección y resguardo de los activos físicos críticos, como equipos, archivos físicos, datos en papel, recursos humanos y otros elementos valiosos. Se verifica si se aplican medidas de seguridad adecuadas, como protección contra incendios, sistemas de respaldo de energía, procedimientos de manejo de datos sensibles, entre otros.

6. **Evaluación de capacitación y concienciación**: Se analiza la capacitación y concienciación en seguridad física proporcionada a los empleados, como la seguridad en la manipulación de activos, la gestión de visitantes y la respuesta a situaciones de emergencia (Dipaz, 2019)

2.5.2. Auditoría de la seguridad lógica

Olortegui (2019) define a la auditoría de la seguridad lógica es un proceso que evalúa y examina los controles y medidas implementados para proteger los activos de información y los sistemas de información de una organización. El objetivo principal de esta auditoría es asegurar la confidencialidad, integridad y disponibilidad de la

información, así como garantizar el cumplimiento de las políticas y regulaciones relacionadas con la seguridad de la información.

2.6. Técnicas de la auditoría informática

Las herramientas de la auditoria Informática, se definen como el conjunto de elementos que permiten analizar de mejor manera una evaluación exhaustiva y sistemática de los sistemas de información de una empresa.

- **Cuestionarios:** Permiten recabar información sobre el departamento de TI para exponer un informe.
- **Entrevistas:** Esta técnica obtiene información más a detalle con la persona entrevistada (Sánchez Supe, 2022, pág. 17)
- **Herramientas de auditoría de cumplimiento**: permiten evaluar el cumplimiento de las políticas y regulaciones de seguridad de la información, y verificar que los controles y medidas de seguridad implementados por la organización cumplan con los estándares de seguridad y privacidad establecidos (2021, pág. 60).

2.7. Proceso de la Auditoria

Para realizar una auditoría, es esencial establecer las etapas de desarrollo en función del logro de los objetivos del proyecto.

"Independientemente del tipo de control que se aplique, llevar a cabo una auditoría es tener en cuenta un proceso sistemático que cuenta con cuatro fases fundamentales: Planeación, Ejecución, Comunicación de resultados y Seguimiento."

Las fases de la Auditoria son las siguientes:

2.7.1. Planeación

Durante la etapa de planificación, se reúnen diversos recursos esenciales para establecer la estrategia de auditoría que guiará la fase de ejecución. En esta etapa, es crucial que el auditor adquiera un entendimiento y visión general de la entidad a auditar, lo que le permitirá determinar cómo llevará a cabo el análisis de la gestión de dicha entidad. (Alayon, 2014)

2.7.2. Ejecución

Durante la etapa de ejecución, el auditor lleva a cabo la estrategia que fue diseñada en la fase previa, reflejada en el memorando de planificación y en los programas de trabajo. En esta etapa, se reúne la evidencia necesaria que permitirá al auditor formar una opinión sobre la gestión de la organización. (Alayon, 2014)

2.7.3. Comunicación de resultados

Después de finalizar la etapa de ejecución, se ordenan los documentos de la auditoría relacionados con las herramientas de recolección de datos. Estos incluyen los hallazgos de las entrevistas, listas de verificación, cuestionarios y también los resultados del análisis de riesgo de cada proceso auditado. (Camacho, 2016)

2.8. Análisis y gestión de riesgos de seguridad informática

2.8.1. Análisis de riesgos

El análisis de riesgos es un proceso continuo que evalúa la probabilidad y gravedad de eventos peligrosos en sistemas informáticos. Busca identificar vulnerabilidades y amenazas, para luego establecer controles de seguridad basados

en estos hallazgos, con el fin de minimizar amenazas o reducir su impacto en la organización. (Leon, 2007).

2.8.2. Gestión de Riesgos

La administración de riesgos es un proceso que identifica, examina, evalúa y categoriza el riesgo, con el objetivo de establecer estrategias que permitan mitigarlos. (Parra Moreno, 2012).

Este procedimiento permite a las entidades comprender con mayor claridad el estado actual de su seguridad, facilitando la toma de decisiones sobre las acciones requeridas para reducir o prevenir posibles riesgos.

CAPÍTULO III

3. ESQUEMA METODOLÓGICO

3.1. Enfoque de la investigación

La investigación que se llevará a cabo tendrá como objetivo principal realizar una auditoría exhaustiva de la seguridad en el GADIPCS Suscal, centrándose específicamente en las dimensiones física y lógica de sus servicios tecnológicos. Para lograr un análisis completo y detallado, se adoptará un enfoque mixto. Esto significa que se combinarán técnicas cuantitativas y cualitativas para recopilar, analizar e interpretar datos. La utilización del enfoque mixto permitirá abordar la problemática desde diferentes ángulos, ofreciendo una visión más completa y una comprensión más profunda de la situación actual de la seguridad en la entidad.

Como marco de referencia para llevar a cabo esta auditoría, se utilizará la norma ISO/IEC 27002:2016. Esta norma internacional proporciona las mejores prácticas y directrices para la implementación de controles de seguridad de la información, lo que facilitará la identificación de áreas de mejora, potenciales vulnerabilidades y recomendaciones pertinentes para reforzar la seguridad de los servicios tecnológicos del GADIPCS Suscal.

3.2. Nivel de la investigación

La investigación que se llevará a cabo busca auditar de manera detallada las dimensiones física y lógica de la seguridad en los servicios tecnológicos del GADIPCS Suscal. Adoptando un enfoque descriptivo, el estudio se centrará en reconocer, examinar y detallar las características y prácticas de seguridad existentes en la entidad.

Esta metodología permitirá obtener un panorama nítido y detallado de la postura de seguridad actual de la organización.

3.3. Población y muestra

La entidad objeto de estudio es la empresa pública municipal GADIPCS Suscal. Dentro de este universo, se focalizará en el personal del departamento de TI para conformar la muestra seleccionada.

El grupo de estudio es limitado, dado que no se tiene claridad sobre cuántos individuos trabajan en la entidad.

3.4. Métodos de investigación

En este estudio, se empleará el método deductivo, iniciará con un análisis general de los datos y procederá hacia una evaluación más granular, con el propósito de alcanzar de manera precisa los objetivos planteados.

3.4.1. Estrategias de Implementación

Durante la realización de este proyecto, se abordarán las tres etapas cruciales de la auditoría: Planeación, Ejecución e Informe Final. Adicionalmente, utilizaremos la norma ISO 27002 como marco de referencia, lo que facilitará la comprobación del cumplimiento de los protocolos de seguridad, tanto lógicos como físicos.

A continuación, se detallan las acciones a llevar a cabo en cada etapa.

3.4.1.1. Fase de Planeación

Durante esta etapa, se busca entender profundamente la estructura y cultura de la organización, así como diagnosticar su estado actual, considerando

sus metas, desafíos y el contexto en el que opera. Esta comprensión será esencial para las fases posteriores del proyecto.

Las etapas que se planean abordar incluyen:

- **Revisión preliminar**

  Se recolectará información esencial sobre la organización para una comprensión completa.

- **Definición de objetivos, alcance y programa de auditoria**

  En esta etapa, se fija la meta y los límites de la auditoría, delineando las tareas a desarrollar en cada etapa del proceso de revisión.

3.4.1.2. Fase de Ejecución

En esta etapa, se procede a analizar los controles de seguridad en vigor. Posteriormente, se realizan evaluaciones técnicas para detectar posibles brechas de seguridad. Al concluir el análisis, se examinan los hallazgos con el objetivo de identificar amenaza que podrían ser explotados.

3.4.1.3. Fase de Comunicación de Resultados

Al concluir, se compone un documento con las sugerencias pertinentes para minimizar los riesgos asociados.

3.5. Técnicas e instrumentos de recolección

Para llevar a cabo una investigación profunda y obtener información relevante, se implementarán diversas técnicas que abordarán tanto fuentes primarias como secundarias (Revisiones Bibliográficas, Entrevista, Observación, etc). Adicionalmente, se llevará a cabo una prueba de cumplimiento (Check list) basada en la norma ISO 27002.

3.6. Tratamiento de la información

Se seleccionarán y adaptarán adecuadamente según las necesidades específicas de la investigación, y se tomarán las precauciones necesarias para asegurar que la información recopilada sea precisa y se pueda confiar en ella.

3.7. Resultados

Conforme a la metodología de auditoría delineada anteriormente, procederemos a ejecutar secuencialmente cada etapa propuestas.

3.8. FASE DE PLANEACIÓN

3.8.1. Revisión Preliminar

Todos los datos presentados en esta sección derivan de fuentes primarias, específicamente de documentos y declaraciones aportadas por los directivos y empleados del Gobierno Autónomo Descentralizado Intercultural del Cantón Suscal.

3.8.1.1. Descripción general de la Empresa

"El Gobierno Autónomo Descentralizado Municipal Intercultural y Participativo del Cantón Suscal desde su creación, en esta nueva etapa de autonomía y autodeterminación ha mejorado de manera sustantiva la calidad de los servicios públicos volviéndolos más accesibles con criterios de equidad e igualdad. El desafío ha sido una constate para romper las barreras discriminatorias, de injusticia social". (Gobierno Autónomo Descentralizado Municipal Intercultural y Participativo del Cantón Suscal, 2022)

Por lo tanto, ha sido necesario enfrentar desafíos ideológicos, políticos y administrativos para reducir las desigualdades entre quienes poseen y quienes carecen de todo.

Como táctica, se han unificado ideas, perspectivas y determinación política con una perspectiva de derechos para establecer un objetivo unificado: el desarrollo sostenible y sustentable del Nuevo Suscal.

Misión

> "El GADIPCS será un organismo que promoverá el desarrollo sustentable y sostenible en el cantón, empleando adecuadamente los recursos físicos, humanos, económicos contando con herramientas como la planificación participativa, misma que permite brindar un tratamiento equitativo a las diferentes dificultades que se vinculen y competan al gobierno local. Realizar una adecuada rendición de cuentas, misma que contará una participación activa de la ciudadanía urbana y de las comunidades rurales, lo que contribuirá a fortalecer el bienestar social, material, espiritual, cultural en la población, lo cual llevará a un adecuado progreso del cantón Suscal."

- **Visión**

> "Hacia el año 2023 el cantón Suscal de la provincia Cañar, se proyecta como territorio integrado e interconectado, con diferentes actividades productivas y económicas que les otorgan bienestar a sus habitantes, buscando además mejorar las condiciones de vida desde todos los ejes de gestión y articulación; buscando que los actores sociales del territorio participen activamente en las distintas decisiones estratégicas, formulación de propuestas, políticas, planes y proyectos." (Oliva, 2023)

3.8.1.2. Organigrama de la Empresa

El organigrama que se muestra a continuación ha sido aprobado conforme al artículo 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP). Es importante mencionar que, dado que la imagen original proporcionada por la unidad de talento humano del GAD Intercultural Participativo del Cantón Suscal no era nítida, se realizó una reelaboración manual de este.

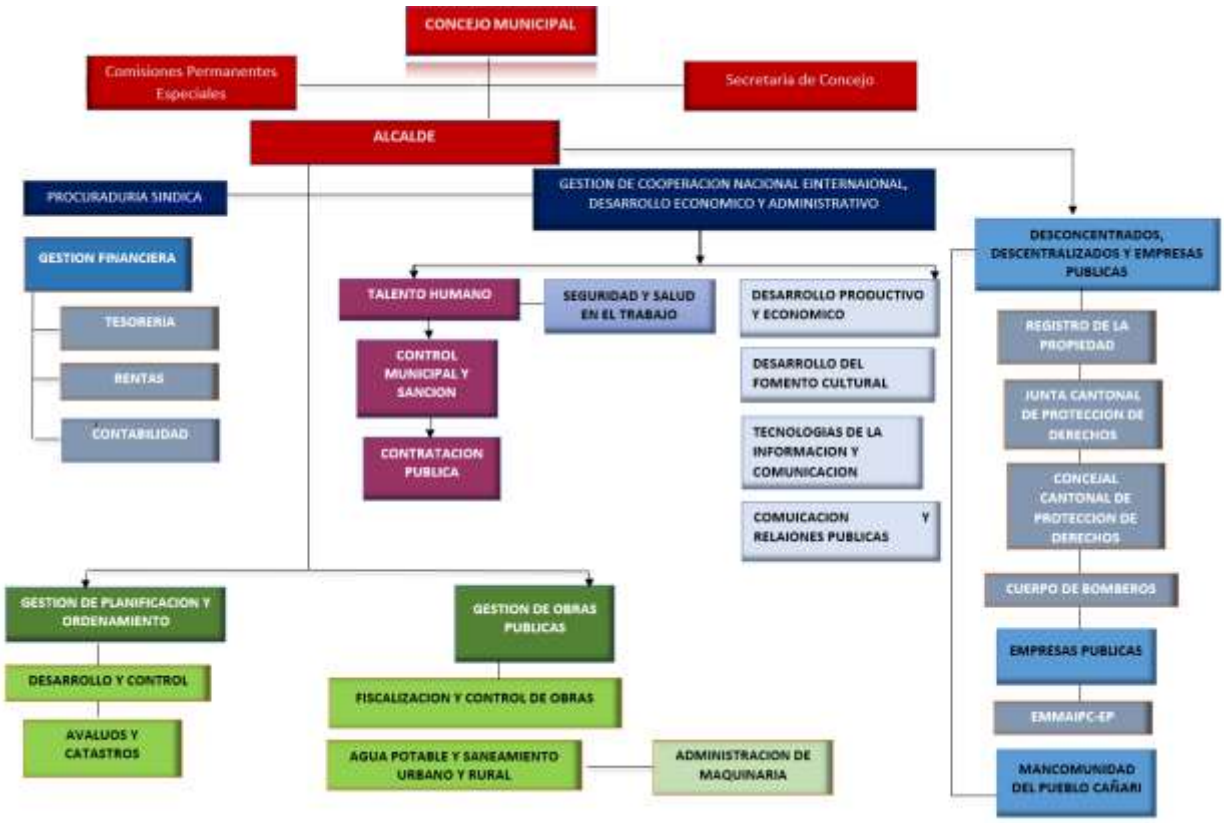


***Ilustración 2**: Organigrama del GAD Suscal*

3.8.2. Definición de objetivos, alcance y programa de auditoria

En esta actividad, se establece el alcance de la auditoría y se delinean los procedimientos específicos para cada fase del proceso.

3.8.2.1. Objetivo de la Auditoria

Evaluar la seguridad física y lógica de los servicios tecnológicos del GADIPCS Suscal mediante técnicas y herramientas de auditoría especializadas,

con la finalidad de identificar vulnerabilidades y avalar la integridad, confidencialidad y disponibilidad de la información y recursos tecnológicos.

3.8.2.2. Alcance de la Auditoria

Se realizará una evaluación integral de la seguridad física y lógica de todos los servicios tecnológicos del GADIPCS Suscal. Esta revisión abordará tanto las medidas y controles de protección física y lógicas de los elementos tecnológicos, como las políticas, procedimientos y configuraciones relacionadas con la seguridad de la información. La intención es identificar posibles vulnerabilidades y ofrecer recomendaciones para fortalecer la protección de los recursos y datos del GADIPCS Suscal. Se emplearán metodologías y herramientas adecuadas para garantizar un análisis exhaustivo y preciso

3.8.2.3. Programa de la Auditoria

Tabla 1: *Programa de Auditoria; Autor: Propio*

	GOBIERNO AUTÓNOMO DESCENTRALIZADO INTERCULTURAL DEL CANTÓN SUSCAL			**Código:** **Versión:** **Emisión:**	
Objetivo del programa	Definir las tareas y los plazos de la auditoría.	**Procedimiento**	Auditoria a la seguridad Fisca y Lógica	**Año**	2023
Proceso	**Dependencia**	**Fase**	**Actividad**	**Fecha I.**	**Fecha F.**
Gestión Tecnológica	Departamento de TI	**Planeación**	Revisión preliminar	28/8/2023	29/8/2023
			Objetivos, alcance y programa de auditoria	30/8/2023	1/9/2023
			Especificación de Controles de la norma ISO 27002	4/9/2023	6/9/2023
			Diseñar las pruebas de cumplimiento (Check List)	6/9/2023	8/9/2023
		Ejecución	Ejecutar Prueba (Aplicar la prueba de cumplimiento (Check List))	8/9/2023	12/9/2023
			Analizar los resultados de la prueba	12/9/2023	15/9/2023
		Informe	Parentación de Hallazgos (Informe F)	15/9/2023	22/9/2023

3.8.2.4. Norma ISO 27002: 2016

La norma ISO/IEC 27001 establece un marco de referencia que comprende 14 dominios y 114 objetivos de control específicos, frecuentemente abordados en auditorías de seguridad de la información. Dentro del contexto de esta investigación, que se centra en una auditoría de seguridad física y lógica, se han seleccionado aquellos dominios intrínsecamente vinculados a estos ámbitos de seguridad para garantizar una evaluación técnica y adecuada de las prácticas y controles existentes, dicha información se puede visualizar en la Tabla Nº 2.

Tabla 2: *Controles físicos y lógicos de la norma ISO 27002; Autor: Propio; Fuete: ISO 27000*

Control	Sección	Controles de Seguridad de la Información
Controles Físicos	**A11**	**Seguridad física y del entorno**
	A11.1	**Áreas seguras**
	A11.1.1	Perímetro de seguridad física
	A11.1.2	Controles físicos de entrada
	A11.1.3	Seguridad de oficinas, despachos y recursos
	A11.1.4	Protección contra las amenazas externas y ambientales
	A11.1.5	El trabajo en áreas seguras
	A11.1.6	Áreas de carga y descarga
	A11.2	**Seguridad de los equipos**
	A11.2.1	Emplazamiento y protección de equipos
	A11.2.2	Instalaciones de suministro
	A11.2.3	Seguridad del cableado
	A11.2.4	Mantenimiento de los equipos
	A11.2.5	Retirada de materiales propiedad de la empresa
	A11.2.6	Seguridad de los equipos fuera de las instalaciones
	A11.2.7	Reutilización o eliminación segura de equipos
	A11.2.8	Equipo de usuario desatendido
	A11.2.9	Política de puesto de trabajo despejado y pantalla limpia
	A9	**Control de acceso**
	A9.1	**Requisitos de negocio para el control de acceso**
	A9.1.1	Política de control de acceso
	A9.1.2	Acceso a las redes y a los servicios de red
	A9.2	**Gestión de acceso de usuario**
	A9.2.1	Registro y baja de usuario
	A9.2.2	Provisión de acceso de usuario

Controles Lógicos	A9.2.3	Gestión de privilegios de acceso
	A9.2.4	Gestión de la información secreta de autenticación de los usuarios
	A9.2.5	Revisión de los derechos de acceso de usuario
	A9.2.6	Retirada o reasignación de los derechos de acceso
	A9.3	**Responsabilidades del usuario**
	A9.3.1	Uso de la información secreta de autenticación
	A9.4	**Control de acceso a sistemas y aplicaciones**
	A9.4.1	Restricción del acceso a la información
	A9.4.2	Procedimientos seguros de inicio de sesión
	A9.4.3	Sistema de gestión de contraseñas

3.8.2.5. Prueba de Cumplimientos ISO 27002 (Check List)

A continuación, se proporciona una lista de verificación detallada basada en la norma ISO/IEC 27002, que comprende distintos dominios, controles específicos y sus correspondientes objetivos de control. Esta lista ha sido diseñada para evaluar y asegurar la conformidad y adecuación de las prácticas y procedimientos implementados por el personal de TI del GADIPCS Suscal, en relación con las recomendaciones y requerimientos de la mencionada norma.

Tabla 3: *Prueba de cumplimiento (Check list) ISO 27002*

Estado y Aplicabilidad de controles de Seguridad de la Información				
Control	**Sección**	**Controles de Seguridad de la Información**	**Si**	**No**
Controles Físicos	**A11**	**Seguridad física y del entorno**		
	A11.1	**Áreas seguras**		
	A11.1.1	Perímetro de seguridad física		
	A11.1.2	Controles físicos de entrada		
	A11.1.3	Seguridad de oficinas, despachos y recursos		
	A11.1.4	Protección contra las amenazas externas y ambientales		
	A11.1.5	El trabajo en áreas seguras		
	A11.1.6	Áreas de carga y descarga		
	A11.2	**Seguridad de los equipos**		
	A11.2.1	Emplazamiento y protección de equipos		
	A11.2.2	Instalaciones de suministro		
	A11.2.3	Seguridad del cableado		
	A11.2.4	Mantenimiento de los equipos		
	A11.2.5	Retirada de materiales propiedad de la empresa		
	A11.2.6	Seguridad de los equipos fuera de las instalaciones		
	A11.2.7	Reutilización o eliminación segura de equipos		
	A11.2.8	Equipo de usuario desatendido		
	A11.2.9	Política de puesto de trabajo despejado y pantalla limpia		
Controles Lógicos	**A9**	**Control de acceso**		
	A9.1	**Requisitos de negocio para el control de acceso**		
	A9.1.1	Política de control de acceso		
	A9.1.2	Acceso a las redes y a los servicios de red		
	A9.2	**Gestión de acceso de usuario**		
	A9.2.1	Registro y baja de usuario		
	A9.2.2	Provisión de acceso de usuario		
	A9.2.3	Gestión de privilegios de acceso		
	A9.2.4	Gestión de la información secreta de autenticación de los usuarios		
	A9.2.5	Revisión de los derechos de acceso de usuario		
	A9.2.6	Retirada o reasignación de los derechos de acceso		
	A9.3	**Responsabilidades del usuario**		
	A9.3.1	Uso de la información secreta de autenticación		
	A9.4	**Control de acceso a sistemas y aplicaciones**		
	A9.4.1	Restricción del acceso a la información		
	A9.4.2	Procedimientos seguros de inicio de sesión		
	A9.4.3	Sistema de gestión de contraseñas		
	A9.4.4	Uso de utilidades con privilegios del sistema		

	A10	**Criptografía**		
	A10.1	**Controles criptográficos**		
	A10.1.1	Política de uso de los controles criptográficos		
	A10.1.2	Gestión de claves		
	A12	**Seguridad de las operaciones**		
	A12.2	**Protección contra el software malicioso (malware)**		
	A12.2.1	Controles contra el código malicioso		
	A12.3	**Copias de seguridad**		
	A12.3.1	Copias de seguridad de la información		
	A12.4	**Registros y supervisión**		
	A12.4.1	Registro de eventos		
	A12.4.2	Protección de la información del registro		
	A12.4.3	Registros de administración y operación		
	A12.4.4	Sincronización del reloj		
	A12.6	**Gestión de la vulnerabilidad técnica**		
	A12.6.1	Gestión de las vulnerabilidades técnicas		
	A12.6.2	Restricción en la instalación de software		
	A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
	A12.7.1	Controles de auditoría de sistemas de información		
	A16	**Gestión de incidentes de seguridad de la información**		
	A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
	A16.1.1	Responsabilidades y procedimientos		
	A16.1.2	Notificación de los eventos de seguridad de la información		
	A16.1.3	Notificación de puntos débiles de la seguridad		
	A16.1.5	Respuesta a incidentes de seguridad de la información		
	A16.1.6	Aprendizaje de los incidentes de seguridad de la información		

CAPÍTULO IV

4. PROPUESTA

4.1. FASE DE EJECUCIÓN

Durante esta etapa, se efectúa una evaluación minuciosa de los dominios, seguida de un análisis de riesgo integral, utilizando enfoques y herramientas especializadas para determinar y cuantificar las potenciales amenazas y vulnerabilidades asociadas a esos dominios.

4.1.1. Evaluación de los Controles basados en la Norma ISO 27002

A continuación, se muestra la lista de verificación con los resultados proporcionados por el equipo de TI del GADIPCS Suscal. Basándonos en esta información, evaluaremos los resultados de cada control que fue seleccionado previamente.

La valoración del riesgo se efectuará basándose en los criterios y escalas especificados en la norma ISO 27005, ponderando simultáneamente el impacto anticipado y la probabilidad de manifestación del evento no deseado.

Impacto: Puede ser valorado en términos cualitativos, como "Bajo" (B), "Medio" (M), "Alto" (A), o en términos cuantitativos, respectivamente (1, 2, 3)

Probabilidad: Al igual que el impacto, la probabilidad puede ser valorada de forma cualitativa o cuantitativa.

Evaluación del Riesgo: Se hace en una matriz de riesgos donde el impacto y la probabilidad se cruzan para proporcionar una valoración general del riesgo (por ejemplo, "Riesgo Bajo" (RB), "Riesgo Medio" (RM), "Riesgo Alto" (RA)). Para la evaluación de la matriz, se emplearán las siglas previamente especificados correspondiente a cada nivel de riesgo.

Riesgo Bajo: Valores 1 a 3.

Riesgo Medio: Valores 4 a 6.

Riesgo Alto: Valores 7 a 9.

Tabla 4: Estado de los controles de seguridad física y lógica (Matriz de Riesgo); Autor: Propio

Estado y Aplicabilidad de controles de Seguridad de la Información								
Control	**Sección**	**Controles de Seguridad de la Información**	**Si**	**No**	**Riesgo**	**Impacto**	**Probabilidad**	**Nivel de Riesgo**
Controles Físicos	**A11**	**Seguridad física y del entorno**						
	A11.1	**Áreas seguras**						
	A11.1.1	Perímetro de seguridad física		X	Daño o sabotaje de activos físicos	M	M	RM
	A11.1.2	Controles físicos de entrada	X		Fallos en sistemas de autenticación	A	B	RB
	A11.1.3	Seguridad de oficinas, despachos y recursos		X	Robo o pérdida de activos, Daño accidental	M	M	RM
	A11.1.4	Protección contra las amenazas externas y ambientales	X		Daño por fenómenos naturales, Exposición a temperaturas extremas	A	B	RB
	A11.1.5	El trabajo en áreas seguras		X	Falta de procedimientos adecuados	M	M	RM
	A11.1.6	Áreas de carga y descarga		X	Manipulación de cargas	B	B	RB
	A11.2	**Seguridad de los equipos**						
	A11.2.1	Emplazamiento y protección de equipos		X	Acceso no autorizado a sistemas y datos corporativos	A	M	RM
	A11.2.2	Instalaciones de suministro	X		Interrupción del suministro eléctrico o de comunicaciones.	A	M	RM
	A11.2.3	Seguridad del cableado	X		Acceso no autorizado o daño al cableado de comunicaciones.	A	M	RM
	A11.2.4	Mantenimiento de los equipos	X		Fallo o malfuncionamiento del equipo	A	M	RM
	A11.2.5	Retirada de materiales propiedad de la empresa		X	Fuga o acceso no autorizado a información confidencial	A	A	RA

	A11.2.6	Seguridad de los equipos fuera de las instalaciones		X	Pérdida, robo o acceso no autorizado a los datos contenidos en equipos	A	M	RM
	A11.2.7	Reutilización o eliminación segura de equipos		X	Recuperación no autorizada de datos de equipos desechados o reutilizados.	M	B	RB
	A11.2.9	Política de puesto de trabajo despejado y pantalla limpia		X	Exposición no autorizada de información confidencial	A	B	RB
Controles Lógicos	**A9**	**Control de acceso**						
	A9.1	**Requisitos de negocio para el control de acceso**						
	A9.1.1	Política de control de acceso		X	Acceso no autorizado a recursos y datos confidenciales	A	M	RM
	A9.1.2	Acceso a las redes y a los servicios de red		X	Acceso no autorizado o compromiso de la infraestructura de red y servicios asociados.	A	M	RM
	A9.2	**Gestión de acceso de usuario**						
	A9.2.1	Registro y baja de usuario		X	Uso indebido de recursos y datos	M	B	RB
	A9.2.2	Provisión de acceso de usuario		X	Exposición, modificación o eliminación no autorizada de datos.	M	M	RM
	A9.2.3	Gestión de privilegios de acceso		X	Abuso o uso indebido de privilegios elevados	A	M	RM
	A9.2.4	Gestión de la información secreta de autenticación de los usuarios		X	Compromiso de la información secreta de autenticación	M	B	RB
	A9.2.5	Revisión de los derechos de acceso de usuario		X	Persistencia de derechos de acceso inapropiados o excesivos para usuarios	M	B	RB
	A9.2.6	Retirada o reasignación de los derechos de acceso		X	Continuidad de derechos de acceso no pertinentes	A	M	RM
	A9.3	**Responsabilidades del usuario**						

	A9.3.1	Uso de la información secreta de autenticación		X	Compromiso de la información secreta de autenticación	M	B	RB
	A9.4	**Control de acceso a sistemas y aplicaciones**						
	A9.4.1	Restricción del acceso a la información	X		Exposición no autorizada o inapropiada de datos sensibles	A	B	RB
	A9.4.2	Procedimientos seguros de inicio de sesión	X		Compromiso de credenciales y acceso no autorizado	M	B	RB
	A9.4.3	Sistema de gestión de contraseñas		X	Falta de almacenamiento seguro y cifrado de contraseñas en el sistema de gestión.	M	M	RM
	A9.4.4	Uso de utilidades con privilegios del sistema		X	Abuso o mal uso de utilidades con privilegios, llevando a cambios no autorizados	A	M	RM
	A10	**Criptografía**						
	A10.1	**Controles criptográficos**						
	A10.1.1	Política de uso de los controles criptográficos		X	Implementación incorrecta o inconsistente de criptografía	M	B	RB
	A10.1.2	Gestión de claves		X	Pérdida, filtración o compromiso de claves criptográficas	A	M	RM
	A12	**Seguridad de las operaciones**						
	A12.2	**Protección contra el software malicioso (malware)**						
	A12.2.1	Controles contra el código malicioso	X		Fallo en la detección o mitigación de código malicioso	A	A	RA
	A12.3	**Copias de seguridad**						
	A12.3.1	Copias de seguridad de la información	X		Fallo de copias de seguridad adecuadas	A	M	RM
	A12.4	**Registros y supervisión**						
	A12.4.1	Registro de eventos		X	Falta de registros adecuados o la incapacidad de conservar y analizar registros	M	B	RB
	A12.4.2	Protección de la información del registro		X	Alteración de los registros	M	B	RB

	A12.4.3	Registros de administración y operación		X	Malas prácticas o acciones maliciosas, comprometiendo la integridad y seguridad de los sistemas y datos.	M	M	RM
	A12.4.4	Sincronización del reloj		X	Desfase o desincronización de los relojes de los sistemas	M	B	RB
	A12.6	**Gestión de la vulnerabilidad técnica**						
	A12.6.1	Gestión de las vulnerabilidades técnicas		X	Fallo en la identificación, evaluación o remediación oportuna de vulnerabilidades técnicas	M	M	RM
	A12.6.2	Restricción en la instalación de software		X	Instalación no autorizada o inadvertida de software malicioso	A	A	RA
	A12.7	**Consideraciones sobre la auditoria de sistemas de información**						
	A12.7.1	Controles de auditoría de sistemas de información	X		Registro de información excesiva o irrelevante, lo que resulta en la omisión de eventos críticos	M	B	RB
	A16	**Gestión de incidentes de seguridad de la información**						
	A16.1	**Gestión de incidentes de seguridad de la información y mejoras**						
	A16.1.1	Responsabilidades y procedimientos		X	Actividad inusual en horarios no laborables	M	M	RM
	A16.1.2	Notificación de los eventos de seguridad de la información	X		Ataques de phishing o spear-phishing	A	M	RM
	A16.1.3	Notificación de puntos débiles de la seguridad		X	Falta de comunicación adecuada o tardía sobre puntos débiles de la seguridad identificados (actualizaciones faltantes)	M	B	RB
	A16.1.5	Respuesta a incidentes de seguridad de la información		X	Respuesta inadecuada (Pérdida de datos, interrupción prolongada de los servicios)	A	M	RM

	A16.1.6	Aprendizaje de los incidentes de seguridad de la información		X	Falta de mejoras continuas en las prácticas y protocolos de seguridad de la organización.	M	M	RM

4.1.2. Análisis General de la prueba de cumplimiento según la norma ISO 27002 (Check List)

A partir de la Tabla Nº 4 proporcionada anteriormente se presenta un análisis general de los controles físicos y lógicos del GADIPCS Suscal en relación con el estado y la aplicabilidad de los controles de seguridad de la información:

Controles Físicos:

- **Seguridad física y del entorno**: Los controles en esta sección están orientados hacia la seguridad física de las instalaciones y equipos. De los controles listados, hay un equilibrio entre controles ya implementados y los que no lo están. Las amenazas identificadas incluyen daño físico, fallos de autenticación, y acceso no autorizado. La mayoría de estos controles tienen un riesgo medio (RM) asociado, lo que indica una necesidad moderada de atención, ya que podrían afectar la integridad de los sistemas y datos.

Controles Lógicos:

- **Control de acceso**: Esta sección se centra en el control de acceso a sistemas y datos. Se observa que muchos de estos controles no están implementados, exponiendo al GADIPCS Suscal a riesgos significativos como acceso no autorizado y compromiso de credenciales. La mayoría de estos controles tienen un nivel de riesgo medio (RM).

- **Criptografía**: Los controles criptográficos son cruciales para asegurar la confidencialidad de los datos. En la matriz presentada, se observa que ambos controles criptográficos no se encuentran implementados. Estos se categorizan con un nivel de riesgo medio (RM). Específicamente, en cuanto a la gestión de

claves, la ausencia de este control puede resultar en la pérdida o compromiso de claves criptográficas.

- **Seguridad de las operaciones**: Esta sección cubre una variedad de controles desde protección contra malware hasta auditoría de sistemas. Una observación importante es la ausencia de la restricción en la instalación de software, lo cual representa un alto riesgo (RA) de instalación no autorizada de software malicioso. Además, es fundamental destacar que varios controles dentro de este dominio han sido catalogados con un nivel de riesgo medio (RM), lo cual indica que aún existen vulnerabilidades que deben ser abordadas para fortalecer la infraestructura y las operaciones de seguridad en el GADIPCS Suscal

- **Gestión de incidentes de seguridad de la información**: Al analizar la matriz proporcionada, se identifica que una parte considerable de los controles, lamentablemente, no ha sido implementada. De estos, algunos han sido catalogados con un nivel de riesgo alto (RA). Asimismo, otros controles han sido etiquetados con un riesgo medio (RM).

  Con base en el análisis, es evidente que el GADIPS Suscal tiene una variedad de riesgos en ambas categorías, físicos y lógicos.

4.2. FASE DE COMUNICACIÓN DE RESULTADOS

En esta última fase, se consolida y sintetiza los datos recopilados durante el proceso de ejecución de la auditoría, proporcionando un fundamento robusto para la estructuración del informe de auditoría final.

4.2.1. Hallazgos

Durante esta fase, se registran meticulosamente las observaciones detectadas en la etapa de ejecución de la auditoría, proporcionando recomendaciones orientadas a

mitigar potenciales vulnerabilidades y optimizar la postura de seguridad de la entidad. A Continuación, se presenta la siguiente matriz.

Tabla 5: Cuadro de Hallazgos de la auditoria a la seguridad física y lógica del GAD Suscal a base de la norma ISO 27002.

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL INTERCULTURAL Y PARTICIPATIVO DEL CANTÓN SUSCAL Cuadro de Hallazgos Evaluación de Check List – Noma ISO 27002							
Control	**Sección**	**Controles de Seguridad de la Información**	**No**	**Riesgo**	**Nivel de R**	**Causa**	**Recomendación**
Controles Físicos	**A11**	**Seguridad física y del entorno**					
	A11.1	**Áreas seguras**					
	A11.1.1	Perímetro de seguridad física	X	Daño o sabotaje de activos físicos	RM	Falta de medidas de seguridad adecuadas en las áreas donde se almacenan activos físicos valiosos, permitiendo el acceso no autorizado.	Al Alcalde, se recomienda Implementar controles físicos más robustos, como sistemas de vigilancia con cámaras, acceso biométrico o tarjetas de acceso, y formar al personal
	A11.1.3	Seguridad de oficinas, despachos y recursos	X	Robo o pérdida de activos, Daño accidental	RM	Deficiencias en la gestión de activos y protocolos de manejo	Al Jefe de Ti, se recomienda fortalecer la seguridad en las oficinas y despachos a través de la instalación de cerraduras electrónicas o sistemas de acceso biométrico en puertas principales y áreas críticas
	A11.1.5	El trabajo en áreas seguras	X	Falta de procedimientos adecuados	RM	La ausencia de directrices claras y procedimientos estandarizados para operar en áreas seguras	Al jefe de Ti, se recomienda desarrollar y documentar procedimientos operativos específicos para trabajar en áreas seguras. Estos procedimientos deben abordar aspectos como la autenticación, el acceso autorizado y la respuesta ante situaciones de emergencia.
	A11.2	**Seguridad de los equipos**					

	A11.2.1	Emplazamiento y protección de equipos	X	Acceso no autorizado a sistemas y datos corporativos	RM	Ubicación inadecuada y medidas de protección insuficientes para los equipos	Al jefe de Ti, se recomienda reubicar equipos críticos y sensibles en áreas designadas con controles de seguridad mejorados, como salas cerradas con acceso controlado.
	A11.2.5	Retirada de materiales propiedad de la empresa	X	Fuga o acceso no autorizado a información confidencial	RA	La inadecuada gestión y supervisión de materiales que son retirados de las instalaciones de la empresa	Al Alcalde, se recomienda establecer un protocolo estricto para la retirada de materiales propiedad de la empresa
	A11.2.6	Seguridad de los equipos fuera de las instalaciones	X	Pérdida, robo o acceso no autorizado a los datos contenidos en equipos	RM	La falta de medidas de protección adecuadas o de procedimientos claros al manejar equipos fuera de las instalaciones	Al jefe de Ti, se recomienda implementar políticas y procedimientos estrictos para el manejo de equipos fuera de las instalaciones
Controles Lógicos	**A9**	**Control de acceso**					
	A9.1	**Requisitos de negocio para el control de acceso**					
	A9.1.1	Política de control de acceso	X	Acceso no autorizado a recursos y datos confidenciales	RM	Política de control de acceso insuficientemente definida o inaplicada	Al jefe de Ti, se recomienda implementar, revisar y fortalecer la política de control de acceso. Debería incluir la definición clara de roles y responsabilidades, asignación de derechos de acceso.
	A9.1.2	Acceso a las redes y a los servicios de red	X	Acceso no autorizado o compromiso de la infraestructura de red y servicios.	RM	La falta de medidas restrictivas y adecuadas en la configuración del acceso a redes y servicios asociados	Al jefe de Ti, se recomienda implementar una solución de detección y prevención de intrusiones (IDPS) en puntos críticos de la infraestructura de red para identificar y mitigar cualquier actividad sospechosa en tiempo real

	A9.2	**Gestión de acceso de usuario**					
	A9.2.2	Provisión de acceso de usuario	X	Exposición, modificación o eliminación no autorizada de datos.	RM	La asignación indiscriminada o poco rigurosa de privilegios de usuario puede llevar a que individuos tengan acceso indebido a información crítica.	Al jefe de Ti, se recomienda iimplementar un proceso sistemático para la asignación y revisión de derechos de acceso basado en el principio de mínimo privilegio.
	A9.2.3	Gestión de privilegios de acceso	X	Abuso o uso indebido de privilegios elevados	RM	La falta de monitoreo, revisión y controles adecuados sobre las cuentas con privilegios elevados puede llevar a abusos o manipulaciones malintencionadas de datos	Al jefe de Ti, se recomienda establecer un protocolo estricto para la gestión de privilegios de acceso.
	A9.2.6	Retirada o reasignación de los derechos de acceso	X	Continuidad de derechos de acceso no pertinentes	RM	La persistencia de derechos de acceso a sistemas o datos luego de que estos ya no son pertinentes para un usuario	Al jefe de Ti, se recomienda implementar un proceso automatizado de revisión y revalidación de derechos de acceso en intervalos regulares.
	A9.4	**Control de acceso a sistemas y aplicaciones**					
	A9.4.3	Sistema de gestión de contraseñas	X	Falta de almacenamiento seguro y cifrado de contraseñas en el sistema de gestión.	RM	El no emplear métodos adecuados para el almacenamiento de contraseñas, como el uso de algoritmos de cifrado débiles	Se recomienda al jefe de implementar un sistema robusto de gestión de contraseñas que utilice técnicas modernas de almacenamiento seguro.
	A9.4.4	Uso de utilidades con privilegios del sistema	X	Abuso o mal uso de utilidades con privilegios, llevando a cambios no autorizados	RM	Falta de controles adecuados, capacitación insuficiente sobre la importancia y responsabilidad que conlleva el uso de estas utilidades.	Al jefe de Ti, se recomienda establecer una política estricta y claramente definida sobre el uso de utilidades con privilegios del sistema.

	A10	**Criptografía**					
	A10.1	**Controles criptográficos**					
	A10.1.2	Gestión de claves	X	Pérdida, filtración o compromiso de claves criptográficas	RM	Falta de procedimientos adecuados para el almacenamiento seguro de claves, la transmisión no cifrada de claves entre sistemas.	Para fortalecer la gestión de claves criptográficas, al Jefe de Ti, se recomienda establecer un protocolo riguroso que incluya: Almacenamiento seguro, Accesos restringido, Backus Seguro, etc.
	A12	**Seguridad de las operaciones**					
	A12.4	**Registros y supervisión**					
	A12.4.3	Registros de administración y operación	X	Malas prácticas o acciones maliciosas, comprometiendo la integridad y seguridad de los sistemas y datos.	RM	Falta de protocolos adecuados y de formación en seguridad para el personal	Al Jefe de Ti, se recomienda establecer protocolos estrictos de monitoreo y auditoría para las actividades en sistemas y redes, asegurando que se detecten y se aborden rápidamente cualquier acción inusual.
	A12.6	**Gestión de la vulnerabilidad técnica**					
	A12.6.1	Gestión de las vulnerabilidades técnicas	X	Fallo en la identificación, evaluación o remediación oportuna de vulnerabilidades técnicas	RM	Deficiencias en los procesos de escaneo y revisión de sistemas, falta de herramientas actualizadas de detección de vulnerabilidades	Al Jefe de Ti, se recomienda implementar un programa robusto y periódico de escaneo de vulnerabilidades con herramientas actualizadas, establecer un equipo dedicado a la evaluación y priorización de riesgos asociados a las vulnerabilidades
	A12.6.2	Restricción en la instalación de software	X	Instalación no autorizada o inadvertida de	RA	Falta de controles adecuados en la instalación de software	Al Jefe de Ti, se recomienda establecer una política clara de instalación de software que defina qué aplicaciones están permitidas y cuáles no

				software malicioso			
	A16	**Gestión de incidentes de seguridad de la información**					
	A16.1	**Gestión de incidentes de seguridad de la información y mejoras**					
	A16.1.1	Responsabilidades y procedimientos	X	Actividad inusual en horarios no laborables	RM	La falta de restricciones o de definición clara sobre los horarios de acceso permitidos, posible negligencia o desconocimiento por parte del personal	Al jefe de Ti, se recomienda reforzar y clarificar las políticas y procedimientos relacionados con los horarios permitidos de actividad y acceso a los sistemas.
	A16.1.2	Notificación de los eventos de seguridad de la información		Ataques de phishing o spear-phishing	RM	Caer en las tácticas ingeniería social que engañan a los usuarios para que revelen información confidencial	Al Jefe de Ti, se recomienda iimplementar un sistema proactivo de notificación que alerte a los usuarios sobre campañas de phishing y actualizaciones de seguridad.
	A16.1.5	Respuesta a incidentes de seguridad de la información	X	Respuesta inadecuada (Pérdida de datos, interrupción prolongada de los servicios)	RM	Falta de un protocolo establecido, falta de capacitación del personal o recursos insuficientes para manejar incidentes de seguridad de manera efectiva.	Al jefe de Ti, se recomienda establecer y mantener un plan de respuesta a incidentes que detalle las acciones específicas a seguir en caso de diferentes tipos de incidentes de seguridad.
	A16.1.6	Aprendizaje de los incidentes de seguridad de la información	X	Falta de mejoras continuas en las prácticas y protocolos de seguridad de la organización.	RM	No realizar revisiones periódicas y análisis post-incidente, y no incorporar lecciones aprendidas en las políticas establecidas.	Después de cada incidente de seguridad, al jefe de Ti, se recomienda llevar a cabo un análisis detallado para comprender las causas subyacentes y las circunstancias que llevaron al incidente.

4.3. FASE INFORME FINAL DE AUDITORIA

El presente informe final de auditoría se centra en la evaluación integral realizada sobre las medidas de seguridad física y lógica implementadas en el GADIPCS Suscal. A través de este documento, se ofrece un panorama claro de los hallazgos, análisis y recomendaciones orientadas a fortalecer y optimizar los protocolos y sistemas de seguridad.

8 DE SEPTIEMBRE 2023

" AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SERVICIOS TECNOLÓGICOS EN EL GADIPCS SUSCAL, USANDO COMO REFERENCIA LA NORMA ISO/IEC 27002:2016"

Auditoria de **Controles Fisiocs y Logicos** en el **GADIPCS**		Informe Final	2023
Equipo de Auditoria			
Auditor certificacion	DIANA JAKELINE ZAMORA POMAQUIZA	Auditor	
Gestor de Auditoria			
Gestor Cerficiacion			
Director			
ING. Danny Andrade		Director	

Auditoria de Controles Físicos y Lógicos en el GADIPCS1 de enero de 2023

1. RESUMEN EJECUTIVO

1.1. Objetivo

El propósito primordial de esta iniciativa de auditoría es llevar a cabo un análisis pormenorizado y riguroso sobre la adecuación y efectividad de los protocolos y procedimientos asociados a la “Seguridad Física y Lógica de los servicios tecnológicos del GADIPCS SUSCAL”, fundamentando dicho análisis en los estándares y criterios estipulados en la normativa ISO/IEC 27002:2016.

1.2. Alcance

Este alcance asegura una evaluación exhaustiva que abarca tanto aspectos físicos como lógicos, alineados a una norma internacionalmente reconocida.

El alcance de la auditoría cubre lo siguiente:

- **Infraestructura Física:**
  - Inspección de los mecanismos de control de acceso físico
  - Revisión de las medidas de protección contra amenazas físicas.
- **Seguridad Lógica:**
  - Evaluación de los controles de acceso lógico al sistema.
  - Revisión de la gestión de contraseñas y políticas de autenticación.
- **Gestión de la Seguridad:**
  - Evaluación de la política y procedimientos de seguridad de la información.
- **Cumplimiento de la Norma ISO/IEC 27002:2016:**
  - Comparación de las prácticas y procedimientos actuales con los requerimientos de la norma.
  - Identificación de áreas de mejora y áreas de no conformidad.

- **Evaluación de Riesgos:**
  - Identificación y análisis de riesgos relacionados con la seguridad física y lógica.
  - Propuestas de mitigación y planes de mejora basados en la evaluación de riesgos.

1.3.Metodología

Para el desarrollo del presente informe se basó en las fases de la auditoria las cuales se mencionan a continuación.

- **Planeación**

  En esta etapa, se efectuó un análisis del estado actual de la entidad con el propósito de diagnosticar la seguridad, tanto física como lógica, y establecer el programa de auditoría.

- **Ejecución**

  Durante esta fase, se llevó a cabo una evaluación exhaustiva de los controles de seguridad estipulados en la norma ISO/IEC 27002. Para ello, se empleó una lista de verificación detallada, diseñada específicamente para analizar y cotejar cada control y subcontrol establecido por la mencionada normativa. Esta herramienta permitió identificar el nivel de cumplimiento, posibles brechas y áreas de mejora en relación con los estándares de seguridad definidos por ISO/IEC 27002 dentro de la organización.

- **Comunicación de Resultados**

  Se elabora un informe detallado que documenta los hallazgos surgidos a lo largo del proceso de auditoría. Este informe incluye una evaluación minuciosa de las desviaciones, inconsistencias y áreas de mejora

identificadas en comparación con los criterios de auditoría establecidos. Además, se categorizan y priorizan los hallazgos según su impacto y relevancia para la organización.

1.4.Opinión de auditoría y principales hallazgos/observaciones

Limitaciones: Dado que no se pudo llevar a cabo nuestro encargo de auditoría según lo planeado, debido a < El tiempo disponible para completar la auditoría, Falta de información requerida >, no expresamos una opinión general sobre el sistema de control <las actividades/procesos auditados> según se describe en los objetivos y alcance del encargo de auditoría.

Resultados Positivos: A partir de las evidencias obtenidas y las evaluaciones realizadas durante nuestra auditoría, y conforme a los objetivos y alcance definidos para este proceso de revisión, se ha determinado que algunos controles de seguridad implementados, tanto físicos como lógicos, son confiables y se alinean adecuadamente con los estándares establecidos por la norma ISO 27002.

Resultados Negativos: A partir de las evidencias obtenidas y las evaluaciones realizadas durante nuestra auditoría, y conforme a los objetivos y alcance definidos para este proceso de revisión, concluimos que los controles de seguridad tanto físicas como lógicas que no se cumplen en la organización, no proporciona una seguridad razonable en cuanto al logro de los objetivos institucionales, debido a que sus activos quedan expuestos a amenazas y la materialización de la misma puede conllevar resultados desfavorables.

2. INFORME COMPLETO

2.1. Introducción

La era digital ha posicionado a la tecnología y la información en el epicentro de las operaciones institucionales a nivel global. En este contexto, las entidades gubernamentales, como el GADIPCS Suscal, enfrentan el desafío de garantizar una gestión segura y eficiente de sus sistemas tecnológicos. La seguridad, tanto en el ámbito físico como en el lógico, no solo es esencial para la eficiencia operativa, sino también para la salvaguarda de datos críticos y el cumplimiento de marcos normativos. Entre las normativas destacadas, la ISO/IEC 27002:2016 emerge como un estándar internacional que brinda una hoja de ruta de mejores prácticas en gestión de la seguridad de la información. Esta investigación se orienta a auditar la seguridad de los servicios tecnológicos del GADIPCS Suscal, alineándose con las directrices de dicho estándar, con la visión de reforzar sus capacidades de seguridad y, por ende, resguardar la integridad, confidencialidad y disponibilidad de su patrimonio informativo.

2.2. Hallazgos

A continuación, se presentan los hallazgos más significativos identificados durante la etapa de ejecución de la auditoría. Además, se ofrece la sugerencia adecuada que se debería considerar para atenuar los riesgos asociados.

2.3. Controles Físicos

Los controles físicos representan un conjunto de directrices y mejores prácticas destinadas a proteger los activos de información contra amenazas físicas. Estos controles buscan asegurar que los activos y la información estén

resguardados de daños físicos, accesos no autorizados, robos, y desastres naturales o provocados por el hombre.

2.3.1. Seguridad Física y del Entorno

2.3.1.1. Áreas Seguras

- **Perímetro de Seguridad**

  Después de aplicar la lista de verificación (check list) para el objetivo de control dentro del dominio "Seguridad física y del entorno", conforme a las directrices establecidas en la norma ISO/IEC 27002, se ha identificado que el área de TIC del GADIPCS no satisface adecuadamente los requerimientos de dicho control. Esta deficiencia conlleva un nivel elevado de vulnerabilidad, potenciando la probabilidad de que amenazas externas e internas puedan materializarse y comprometer la integridad, disponibilidad y confidencialidad de los activos de información y recursos tecnológicos de la entidad.

  Conclusión

  En virtud de la evaluación realizada, es evidente que la estructura actual de seguridad física y del entorno en el área de TIC del GADIPCS presenta lagunas significativas en comparación con los estándares de la norma ISO/IEC 27002. Esta situación no solo deja a la entidad en una posición vulnerable frente a amenazas potenciales, sino que también subraya la necesidad urgente de reforzar y actualizar las medidas de seguridad.

Recomendación

Al jefe de TI, se recomienda implementar

Medidas de Seguridad Física: Es esencial llevar a cabo una revisión exhaustiva y actualización de las medidas de seguridad física en el área de TIC del GADIPCS. También se debe realizar una:

Evaluación del Entorno Actual: Realizar un análisis de riesgos específico para identificar las áreas más vulnerables y determinar las amenazas específicas asociadas con el entorno físico actual.

- **Seguridad de Oficina, Despacho y Recursos**

  Con respecto a la evolución para el objetivo de control "Seguridad de Oficina, Despacho y Recursos", basada en parámetros y criterios específicos establecidos por la norma ISO/IEC 27002, se ha llegado a determinar que el área de TIC del GADIPCS presenta deficiencias en su conformidad con dicho objetivo. Esto indica que hay aspectos específicos relacionados con la seguridad y gestión de recursos, espacios de oficina y despacho que no están siendo manejados adecuadamente o que requieren mejoras. Las deficiencias detectadas pueden involucrar áreas como protocolos de seguridad, sistemas de monitoreo, gestión de acceso o incluso capacitación del personal en las mejores prácticas.

Conclusión

Esta situación crea vulnerabilidades que podrían comprometer la seguridad y operatividad de los sistemas y datos de la entidad. Es crucial que el GADIPCS reconozca estas áreas de oportunidad y priorice acciones correctivas para salvaguardar la integridad de sus activos informáticos

Recomendación

Al alcalde, se recomienda fortalecer la seguridad en las oficinas y despachos a través de la instalación de cerraduras electrónicas o sistemas de acceso biométrico en puertas principales y áreas críticas.

- **El trabajo en áreas Seguras**

  Otro de los objetivos de control del dominio Seguridad Física y del entorno con nivel de riesgo medio, lo que implica una serie de consideraciones. Este nivel de riesgo indica que, aunque se han implementado algunas medidas de seguridad, aún existen áreas de vulnerabilidad o deficiencias en el sistema o proceso. Estas deficiencias, si no se tratan adecuadamente, podrían ser aprovechadas por actores malintencionados o dar lugar a incidentes no deseados, poniendo en riesgo la integridad, confidencialidad y disponibilidad de la información o recursos.

  Conclusiones

  Aunque no hay amenazas críticas inmediatas, las deficiencias detectadas requieren intervención para garantizar una seguridad alineada con las mejores prácticas internacionales.

Recomendaciones

Al jefe de TI, se recomienda la implementación de controles adicionales, conforme a la norma ISO/IEC 27002, tales como: Reforzar los protocolos de acceso a áreas seguras, Mejorar las infraestructuras físicas de seguridad, Establecer protocolos de respuesta rápida ante posibles incidentes de seguridad. Estas medidas son esenciales para mitigar el nivel de riesgo medio identificado en el área de trabajo en zonas seguras.

Al alcalde se recomienda considerar la capacitación continua del personal en las mejores prácticas de seguridad y realizar auditorías periódicas para asegurar la conformidad y eficacia de los controles implementados.

2.3.1.2. Seguridad de los equipos

- **Retirada de Materiales propiedad de la Empresa**

Este objetivo de control es unos de los más críticos de acuerdo al análisis realizado, al no contar con el control “retirada de materiales propiedad de la empresa” la entidad queda expuesto a que se presente fugas o accesos no autorizados a los datos confidenciales.

Conclusión

Es evidente que la ausencia de este objetivo de control crítico sitúa a la entidad en una posición de alta vulnerabilidad. Es esencial atender esta carencia de inmediato para salvaguardar la integridad y confidencialidad de los recursos de información de la entidad.

Recomendación

Al jefe de TI, se recomienda implementar medidas de seguridad robustas como: Registro detallada, Protocolo de verificación, Sistema de Alerta, etc.

De la misma manera, se recomienda al jefe de TI revisar y fortalecer las políticas y procedimientos actuales.

Al jefe de TI se recomienda también llevar a cabo capacitaciones regulares para el personal con el objetivo de prevenir accesos no autorizados y garantizar la protección adecuada de los datos confidenciales de la entidad.

2.4. Controles Lógicos

2.4.1. Control de Acceso

2.4.1.1. Requisitos de negocio para el control de acceso

Los objetivos de control con mayor nivel de riesgo son los siguientes.

- **Política de control de acceso**

Con base en el análisis efectuado en el dominio "Control de Acceso", se ha determinado que el departamento de TIC presenta una vulnerabilidad significativa debido a la falta de un documento formal que defina las políticas para el control de accesos a la infraestructura y sistemas tecnológicos. Esta ausencia puede comprometer la seguridad y confidencialidad de los datos y recursos tecnológicos, haciendo esencial la pronta implementación de políticas y procedimientos adecuados en esta área.

Conclusión

En el análisis efectuado en el dominio "Control de Acceso", se ha determinado que el departamento de TIC presenta una vulnerabilidad significativa debido a la falta de un documento formal que defina las políticas para el control de accesos a la infraestructura y sistemas tecnológicos. Esta ausencia puede comprometer la seguridad y confidencialidad de los datos y recursos tecnológicos, haciendo esencial la pronta implementación de políticas y procedimientos adecuados en esta área.

Recomendación

Al jefe de TI se recomienda, elaborar y aprobar un documento oficial que defina claramente las políticas y procedimientos de control de acceso a la infraestructura y sistemas tecnológicos. De la misma manera se recomienda, implementar mecanismos de autenticación, como contraseñas complejas, autenticación de dos factores o reconocimiento biométrico.

2.4.1.2. Gestión de acceso de usuario

- **Gestión de Privilegio de acceso**

  Con base en la evaluación técnica efectuada, se ha identificado que el mencionado objetivo de control no está operativamente activo ni implementado en el departamento de TIC. Esta deficiencia puede dar lugar a situaciones donde los privilegios se utilicen indebidamente, facilitando actos maliciosos como la alteración o manipulación no autorizada de datos.

Conclusión

De acuerdo al resultado obtenido, es fundamental abordar este vacío para garantizar la integridad y confidencialidad de los datos manejados dentro de ese departamento.

Recomendación

Al jefe de TI se recomienda, implementar un sistema de gestión de acceso robusto y basado en roles, acompañado de políticas y procedimientos claros que determinen los niveles de acceso a la información y a los sistemas tecnológicos.

Al jefe de TI se recomienda, llevar a cabo revisiones periódicas de los privilegios otorgados, y ofrecer capacitaciones regulares al personal del departamento de TIC sobre la importancia y responsabilidad que conlleva el acceso adecuado a los datos y recursos.

2.4.1.3.Control de Acceso a Sistemas y Aplicaciones

- **Sistema de Gestión de Contraseñas**

  El control referente a la gestión basada en roles y acceso diferenciado es crucial. Establece mecanismos que garantizan que únicamente los individuos con las autorizaciones pertinentes, basadas en sus roles y responsabilidades, accedan a información específica. El análisis condujo a la identificación de una deficiencia en el departamento de TIC del GADIPDS en lo que respecta a este mecanismo de control, lo cual puede comprometer la seguridad y confidencialidad de los datos gestionados.

Conclusión

Tras el análisis realizado, es evidente que el departamento de TIC del GADIPDS presenta deficiencias en la implementación del presente control. Es imperativo fortalecer este control para salvaguardar los activos informativos y mantener una gestión adecuada del acceso a los datos.

Recomendación

Al jefe de TI se recomienda, implementar una política de contraseñas que exija la creación de contraseñas complejas, combinando letras, números y símbolos.

Al jefe de TI se recomienda, revisar y actualizar periódicamente los roles y responsabilidades de los usuarios, garantizando que el acceso concedido sea el mínimo necesario acorde a sus funciones.

2.4.2. Criptografía

2.4.2.1. Controles Criptográficos

- **Gestión de claves**

En el análisis realizado se evidencia la falta de implementación de este control, Esta carencia puede culminar en vulnerabilidades significativas, como la exposición, pérdida o filtrado de credenciales de acceso, comprometiendo la seguridad de la infraestructura y la integridad de la información.

Conclusión

Se destaca que la no implementación de este control conlleva a potenciales brechas de seguridad, especialmente en lo que concierne a la comprometida gestión de credenciales. Es esencial priorizar acciones para subsanar esta carencia y preservar la seguridad de la Información.

Recomendación

~~Se recomienda al jefe de TI,~~Al jefe de TI se recomienda, la inmediata implementación y establecimiento de políticas y procedimientos relacionados con la gestión de credenciales, garantizando así que solo el personal autorizado tenga acceso a los sistemas y datos pertinentes.

2.4.3. Seguridad de las Operaciones

2.4.3.1. Protección contra el software malicioso (malware)

- **Restricción en la Instalación de Software**

El departamento de TIC aún no ha implementado este control, lo que representa un nivel de riesgo considerable. La falta de restricciones en la instalación de software puede aumentar las vulnerabilidades del sistema y colocar a la organización en una posición vulnerable ante amenazas potenciales.

Conclusión

La carencia de este control en el GADIPDC amplía el riesgo de exposición a amenazas al integrar software de terceros. Esta brecha podría facilitar la incursión no deseada de fallos de seguridad o malware en la infraestructura tecnológica de la entidad.

Recomendación

Al jefe de TI se recomienda, implementar un protocolo de evaluación y validación de software antes de su instalación. Esta medida debería incluir una revisión detallada de la seguridad del software, pruebas en un entorno aislado y obtener garantías del proveedor sobre la integridad y seguridad del producto.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

Tras una detallada revisión teórica de las normativas y metodologías asociadas a la auditoría informática, se destaca la importancia de estas herramientas en la planificación y realización de auditorías en el sector tecnológico. El estudio teórico sobre la auditoría informática fue fundamental para entender y aplicar de manera efectiva las diferentes etapas involucradas en este proceso.

La estructura de la auditoria, fundamentada en la norma ISO 27002, no solo permitió identificar oportunidades de mejora en el GADIPCS, sino que también orienta el camino hacia la implementación de soluciones eficaces para reforzar la seguridad.

A través de la ejecución de una lista de prueba de cumplimiento (Check List) en el proceso de auditoría, se evaluó sistemáticamente el estado de implementación de cada objetivo de control de seguridad, tanto en el ámbito físico como lógico. Los resultados arrojaron que muchos de estos controles no se encontraban implementada adecuadamente, en consecuencia, se identificaron niveles de riesgo categorizados como "Medio" y "Alto". Esta deficiencia compromete la eficacia de la postura de seguridad de la entidad.

Tras el análisis de los controles de seguridad, tanto físicos como lógicos, de acuerdo con la norma ISO 27002, se ha consolidado los hallazgos en un informe de auditoría. Este documento no solo refleja las áreas donde el GADIPCS muestra deficiencias o carencias en su postura de seguridad, sino que también proporciona recomendaciones puntuales diseñadas para mitigar los riesgos identificados.

Recomendaciones

- Mantenerse actualizado con las versiones más recientes de las normas y metodologías, ya que estas pueden evolucionar y adaptarse a los nuevos desafíos de la industria

Recomendación General para el Gobierno Autónomo Descentralizado Municipal Intercultural y Participativo del Cantón Suscal:

- Se recomienda una capacitación integral y continua para todo el personal del GAD Suscal sobre la importancia de la seguridad de la información y cómo deben proceder en sus respectivas áreas de trabajo.
- Adquirir e implementar tecnologías modernas de protección, detección y respuesta a amenazas. Herramientas como sistemas de detección y prevención de intrusiones (IPS), soluciones de cifrado y gestión de contraseñas, etc.
- Las políticas y protocolos existentes deben ser revisados y fortalecidos para garantizar que reflejen las mejores prácticas actuales en seguridad de la información.

Referencias

Aguilera Lopez, P. (2010). *Seguridad Informatica* . Editex.

Alayon, R. (15 de 10 de 2014). *www.oas.org/juridico/PDFs/mesicic4_ven_intro_proc_aud_ges.pdf.* Obtenido de http://www.oas.org/juridico/PDFs/mesicic4_ven_intro_proc_aud_ges.pdf

Baca Urbina, G. (2016). *Introducción a la seguridad informática.* Mexico: Grupo Editoria Patria.

Briceño, E. V. (2021). *SEGURIDAD DE LA INFORMACIÓN.* 3Ciencias.

Camacho, J. G. (1 de 01 de 2016). *AUDITORÍA A LA SEGURIDAD DE LA RED DE DATOS DE LA EMPRESA.* Obtenido de repository.unad.edu.co: https://repository.unad.edu.co/bitstream/handle/10596/11941/1085267906.pdf?sequence=1

Chango, C. D. (01 de 01 de 2020). *repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf.* Obtenido de https://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

Collado, M. V. (2015). *MF0490_3 - Gestión de servicios en el sistema informático.* España: Editorial Elearning, S.L.

Contraloría General de la República del Perú. (01 de 01 de 2021). *doc.contraloria.gob.pe.* Obtenido de doc.contraloria.gob.pe: https://doc.contraloria.gob.pe/normativa/control_posterior/Version_integrada_del_Manual_de_Auditoria_de_Cumplimiento-MAC.pdf

Dipaz, A. V. (01 de 11 de 2019). *repositorio.unsch.edu.pe.* Obtenido de repositorio.unsch.edu.pe: http://repositorio.unsch.edu.pe/bitstream/UNSCH/4027/1/TESIS%20SIS94_Vil.pdf

Gobierno Autónomo Descentralizado Municipal Intercultural y Participativo del Cantón Suscal. (01 de 01 de 2022). *gadsuscal.gob.ec*. Obtenido de https://gadsuscal.gob.ec/

Imbaquingo, D., Díaz, J., Saltos, T., & Arciniega, S. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 427-440.

INTECO. (11 de 04 de 2023). *www.inteco.org*. Obtenido de www.inteco.org: https://www.inteco.org/shop/inte-iso-iec-27002-2016-tecnologia-de-la-informacion-tecnicas-de-seguridad-codigo-de-buenas-practicas-para-controles-de-seguridad-de-la-informacion-1551#attr=

Leon, M. P. (2007). *Introduccion al analisis de riesgo* . Limusa.

Medrano Padilla, J. (01 de 01 de 2022). *ddigital.umss.edu.bo:8080.* Obtenido de ddigital.umss.edu.bo:8080: http://ddigital.umss.edu.bo:8080/jspui/bitstream/123456789/36654/1/Monografia%20Medrano.pdf

Navarro, E. d. (2003). *Manual de outsourcing informático.* España: Ediciones Díaz de Santos.

nqa. (19 de 10 de 2019). *www.nqa.com.* Obtenido de www.nqa.com: https://www.nqa.com/medialibraries/NQA/NQA-Media-

Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Olortegui Laguna, Y. A. (01 de 01 de 2019). *repositorio.unjfsc.edu.pe.* Obtenido de repositorio.unjfsc.edu.pe: http://repositorio.unjfsc.edu.pe/bitstream/handle/20.500.14067/3081/OLORTEGUI%20LAGUNA%20YASSER%20ANGEL.pdf?sequence=1&isAllowed=y

Pallavicini. (02 de 05 de 2023). *www.pallavicini.cl*. Obtenido de www.pallavicini.cl: https://www.pallavicini.cl/seguridad-de-la-informacion-v2

Parra Moreno, D. A. (01 de 01 de 2012). *repository.unimilitar.edu.co.* Obtenido de GESTIÓN DEL RIESGO EN LA SEGURIDAD INFORMÁTICA: "CULTURA DE LA AUTO-SEGURIDAD INFORMÁTICA": https://repository.unimilitar.edu.co/bitstream/handle/10654/6821/ParraMorenoDuverAugusto2012.pdf?sequence=2&isAllowed=y

Postigo, P. A. (2020). *Seguridad informática (Edición 2020).* Madrid: Paraninfo .

Sabillón, R., & Cano, J. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. *Revista lbérica de Sistemas e Tecnologias de Informação*, 33-48.

Sánchez Supe, J. D. (01 de 01 de 2022). *repositorio.uta.edu.ec.* Obtenido de repositorio.uta.edu.ec: https://repositorio.uta.edu.ec/bitstream/123456789/35878/1/T5404i.pdf

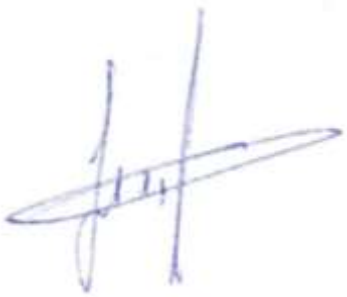
Solano, L. J., Ardila, L. E., & Ardila, H. E. (13 de 08 de 2022). *investigacion.fca.unam.mx.* Obtenido de investigacion.fca.unam.mx: https://investigacion.fca.unam.mx/docs/memorias/2013/2.04.pdf

Universidad Católica de Cuenca	**AUTORIZACIÓN DE PUBLICACIÓN EN EL REPOSITORIO INSTITUCIONAL**

Diana Jakeline Zamora Pomaquiza portador(a) de la cédula de ciudadanía Nº **0302867742** En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"AUDITORÍA DE LA SEGURIDAD FÍSICA Y LÓGICA DE LOS SERVICIOS TECNOLÓGICOS EN EL GADIPCS SUSCAL, USANDO COMO REFERENCIA LA NORMA ISO/IEC 27002:2016"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos y no comerciales. Autorizo además a la Universidad Católica de Cuenca**,** para que realice la publicación de éste trabajo de titulación en el Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Cuenca, **11 de octubre de 2023**

F:



……..

Diana Jakeline Zamora Pomaquiza

C.I. **0302867742**