UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

Tema: "Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo"

Trabajo de Integración Curricular previo a la obtención del título de Ingeniera en Ciencias de la Computación

AUTORA: Murillo Ruano Leidy Tamara

TUTOR: Ing. Yandún Velasteguí Marco Antonio, MSc.

Tulcán, 2023.

CERTIFICADO DEL TUTOR

Certifico que la estudiante Murillo Ruano Leidy Tamara con el número de cédula 0401968995, ha elaborado el Trabajo de Integración Curricular: "Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo".

Este trabajo se sujeta a las normas y metodología dispuesta en el Reglamento de la Unidad de Integración Curricular, Titulación e Incorporación de la UPEC, por lo tanto, autorizo la presentación de la sustentación para la calificación respectiva.

Firmado electrónicamente por:
MARCO ANTONIO
YANDUN VELASTEGUI

_____

Ing. Yandún Velasteguí Marco Antonio MSc.

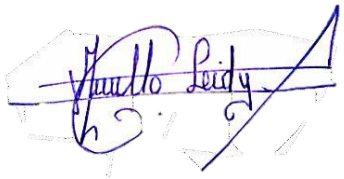
TUTOR

Tulcán, noviembre de 2023

AUTORÍA DE TRABAJO

El presente trabajo de Integración Curricular constituye un requisito previo para la obtención del título de Ingeniera en la Carrera de computación de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Murillo Ruano Leidy Tamara con cédula de identidad 0401968995 declaro que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.



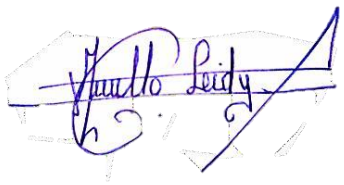
Murillo Ruano Leidy Tamara

AUTORA

Tulcán, noviembre de 2023

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Yo, Murillo Ruano Leidy Tamara declaro ser autora de los criterios emitidos en el Trabajo de Integración Curricular: "Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo" y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes de posibles reclamos o acciones legales.



Murillo Ruano Leidy Tamara

AUTORA

Tulcán, noviembre de 2023

AGRADECIMIENTO

Agradezco a la Universidad Politécnica Estatal Del Carchi Facultad de Industrias Agropecuarias y Ciencias Ambientales, cuna de pericia y profesionalidad, que me haya admitido en una institución tan prestigiosa y responsable.

Debo agradece de manera especial y sincera al MSc. Marco Yandún por haberme permitido realizar esta tesis, bajo su apoyo, confianza y capacidad para orientar mis ideas, las que han contribuido al desarrollo de mi tesis, como también a mi formación investigadora. Las ideas propias siempre enmarcadas en su orientación y rigurosidad, lo cual no habría sido posible sin su oportuna participación.

Al Departamento de Sistemas del Gobierno Autónomo descentralizado del Cantón Espejo (GADME) a cargo del Ing. Clever Pozo y administrativos del área, por su colaboración indispensable para la realización del proyecto de investigación.

Leidy Tamara Murillo Ruano

DEDICATORIA

Primordialmente dedico este trabajo a Dios, que me ha dado la paz para afrontar todas las dificultades de este proceso y alcanzar mis objetivos.

A mis padres Marcos y Yolanda, por sus brillantes ejemplos de trabajo duro y dedicación, su compañía que me brindan siempre y por depositar toda su confianza en mí, su amor y la calidez de familia a la cual amo.

A mi hermana Tania la mayor fuente de inspiración, pues ella fue el principal cimiento para la construcción de mi vida profesional, que gracias a sus virtudes infinitas y gran corazón me llevan a admirarla cada día más.

Leidy Tamara Murillo Ruano

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

ÍNDICE DE ANEXOS

RESUMEN

El presente proyecto evaluó la limitada importancia de seguridad informática que mantiene actualmente el Gobierno Autónomo Descentralizado Del Cantón Espejo (GADME), mediante la aplicación de la norma ISO/IEC 27002, se determinó que existen escasos controles que inciden a un aumento en riesgos de dimensiones de seguridad los hallazgos que se obtuvieron son: formación inadecuada, control de acceso lógico deficiente, documentación inadecuada, aplicaciones y software obsoletos, gestión de riesgos de terceros y gestión de vulnerabilidades inadecuada, probar el plan de contingencia del sistema de manera regular, lista de protocolos críticas, uso de un cifrado de datos potente al transmitir información restringida, identificación de dispositivos de red no fiables o no autorizados, la metodología de investigación aplicada en este estudio, fue tipo mixta cualitativa y cuantitativa mediante la utilización de instrumentos como la encuesta y entrevista a los administrativos del departamento de sistema y funcionarios de las diferentes áreas. Se determinó carencias en la planificación estratégica, debilidades en las políticas y procedimientos de seguridad, incumplimiento de regulaciones y leyes, falta de seguridad en la red y sistemas, insuficiente protección de datos, amenazas internas y externa, problemas de continuidad de la institución, como aporte a la solución a estos hallazgos se realiza un plan de contingencia que contempla una matriz de riesgos y medidas a llevarse a cabo antes, durante y después de una contingencia con acciones a corto, mediano y largo plazo.

Palabras claves: Seguridad de procesos, plan de contingencia, matriz de riesgos, ISO/IEC 27002.

ABSTRACT

The present project assessed the limited importance of computer security currently maintained by the "Gobierno Autónomo Descentralizado del Cantón Espejo" (GADME). A thorough application of ISO/IEC 27002 revealed that there are few controls that affect an increase in the risk of safety dimensions. Findings include inadequate training, poor logical access control, inadequate documentation, obsolete applications and software, third-party risk management and deficient vulnerability management, testing the system contingency plan on a regular basis, listing critical protocols, using strong data encryption when transmitting restricted information, identification of unreliable or unauthorized network devices. The research methodology applied in this study was a mixed qualitative and quantitative type through the use of instruments such as the survey and interview of system department administrators and officials from different areas. The outcome of this process was to identify strategic planning gaps, security policy and procedure weaknesses, non-compliance with regulations, insufficient data protection, internal and external threats, and problems with continuity of the institution. Finally, the contingency plan includes a matrix of risks and measures, which should be taken before, during, and after a contingency with short, medium, and long-term actions.

Keywords: Process reliability, contingency plan, risk matrix, ISO/IEC 27002.

INTRODUCCIÓN

El gobierno Descentralizado Municipal del Cantón Espejo es una institución eficiente y organizada que gestiona el desarrollo del cantón, cuyo objetivo es crear un desarrollo social, económico, productivo y vial en un ambiente sano, promoviendo la seguridad y la participación a través de una planificación estratégica integrada, asegurando el progreso, el bienestar y la sostenibilidad de los habitantes del cantón.

Funcionalmente, la Unidad de Administración de Departamentos está directamente vinculada a la Unidad de Sistemas, responsable de la gestión y el funcionamiento de la tecnología, los servicios web y la intranet, así como del cumplimiento de los procesos organizativos y la protección de información confidencial.

La intención de esta investigación fue generar un informe de estrategias de riesgos de la seguridad, a través de una auditoría de seguridad de la información, las organizaciones pueden reducir su exposición a los riesgos de seguridad de la información, prevenir inconvenientes potenciales en sus procesos y realizar mejoras continuas a corto, medio y largo plazo mediante el uso de mecanismos de auditoría de seguridad de la información basados en el análisis de la norma internacional ISO/IEC 27002. La función de la auditoría de seguridad es garantizar que se dé prioridad a la confidencialidad, disponibilidad, integridad y además que existan procesos de seguridad donde su eficacia se refleje en las actividades de gestión del sistema de información.

I. PROBLEMA

1.1 PLANTEAMIENTO DEL PROBLEMA

La tecnología de la información (TI) es un pilar dentro de la sociedad actual debido a la globalización, constantemente se realizan actividades en una empresa la cual debe contar con normas, que garanticen que los datos procesados en los sistemas de información sean privados y seguros. Por lo tanto, es importante realizar una auditoría en este campo con la finalidad de beneficiar a una institución.

Gracias a el ecosistema informático en América latina se lleva a cabo la tendencia de políticas, ya que a medida que avanza la tecnología conlleva como necesidad actualizar lineamientos, ayudando a combatir los delitos cibernéticos y fortalecer la resiliencia tecnológica, son cuestiones muy importante para el desarrollo económico y social, para mantener normativas de seguridad de tecnología nacional, se necesita evaluar el control de las funciones que tiene una empresa de acuerdo a necesidades que se detecta.

Los ataques buscan un aprovechamiento de información confidencial, se convierten en ataques comunes y van en aumento día a día, como es el ejemplo de Ecuador, en el mes de abril del año 2019 donde existieron 40 millones de ataques por parte de atacantes informáticos a entidades estatales. Por lo que es indispensable asegurar dicha información garantizando la continuidad de las operaciones dentro de las organizaciones públicas, así protegiendo también la privacidad de los clientes y usuarios.

La ausencia de información sobre la protección de los datos personales tanto en América latina como en Ecuador se convierte en una fortaleza ya que permite ser pionero en una propuesta de controles para la protección de datos personales. Dado el riesgo en la cual están expuestos los datos personales, se logra implementar las medidas de control en los países latinoamericanos como son Argentina, Uruguay, Colombia, Perú y México, Ecuador debe de seguir estos estándares ya que es un beneficio para el control de datos en un futuro.

Ecuador, Venezuela y Bolivia son países Latinoamericanos que carecen de una ley que ayude con la protección de datos personales, sin embargo, las normativas que

regulan de forma dispersa e imprecisa en lo que refiere a protección de datos personales se puede tomar en cuenta que no se especifica con claridad lo que se pretende proteger.

De acuerdo al informe de europapress, Brasil el mes de septiembre del año 2021 la página web de la Agencia Nacional de Vigilancia Sanitaria (Anvisa) sufre un ataque de un Servidor web Apache, la información sensible que es saboteada se trata de documentos obligatorios para los turistas extranjeros, debido a la mala configuración de un servidor web permitiendo ataques, accediendo a la información que se almacenaba provocando así que se modifique una bandera Argentina y una referencia indirecta a una cuarentena obligatoria a la que se ven sometidos los viajeros.

En Ecuador dentro del campo empresarial se ha llegado a tomar en cuenta un gran interés en los métodos y procesos que se deben tomar en cuenta para poder tener un buen control proporcionando así un excelente manejo de la información en las empresas ya sea públicas o privadas. Muchas empresas no realizan constantemente evaluaciones acerca del funcionamiento y la constante evolución, tomando en cuenta que actualmente hay una gran prioridad a la competencia de calidad de un servicio o también en lo que respecta a el excelente funcionamiento interno o externo de la empresa. Se debe tomar en cuenta que ya en la actualidad las empresas corren diferentes riesgos en lo que respecta a la administración de la información por lo que se debe llevar en cuenta que el manejo se basa en la tecnología que crece rápidamente que permite así tomar más precauciones para poder evitar pérdidas en las empresas.

Los riesgos que se relacionan con las tecnologías que se maneja se encuentran afines a la gestión y administración de redes, ya que es uno de los medios más importantes por los cuales se causa serios daños a la información de manera intencionada y no intencionada. Uno de los inconvenientes que se resaltó es el de manejo inadecuado de las claves de acceso y a la vez la asignación de roles de manera inadecuada, esto se convierte en un acceso a diversos ataques.

En definitiva, las amenazas dentro de una empresa pueden darse por diferentes causas o situaciones por lo que las organizaciones tienen que cumplir con la obligación de resguardar y al mismo tiempo mantener protegida la información logrando así confidencialidad, autenticidad y la integridad de dicha institución.

De acuerdo con un análisis que se ha realizado a una de las causas que afectan en una empresa para que exista riesgos en el manejo de la información, es la reducida capacitación al personal en las áreas de la institución, generando así información

incompleta y errónea; tomando en cuenta también que la información debe de estar actualizada, completa, segura y sobre todo sea lo más confiable en el Gobierno Descentralizado del Cantón Espejo (GADME).

La empresa debe tener en cuenta que al tener un insuficiente aplicación de Normas de Seguridad Informática puede perjudicar a la institución, por lo que el seguir estándares que permitan la seguridad informática puede llegar a ser útil y sobre todo rentable, ya que sirve como un medio de comunicación en el que se establece reglas, normas y sobre todo un control a los procedimientos para poder normalizar la manera en que la institución prevenga, proteja y pueda manejar los altos riesgos en un manejo de seguridad de la información.

Dentro del Gobierno Descentralizado del Cantón Espejo (GADME) una de las cosas que se ha percatado es que existe un inadecuado control de manejo de la información, lo que conlleva a insatisfacción a los usuarios y esto no favorece a la institución. Tomando en cuenta que el manejo de información es muy importante en la mayoría de las organizaciones, empresas e instituciones para poder ofrecer un servicio de calidad a los usuarios o clientes, procurando brindar servicios públicos domiciliarios, satisfaciendo necesidades básicas, en salud, educación, saneamiento ambiental, agua potable, recreación y deporte.

Si en la empresa existe un poco conocimiento de los riesgos en un manejo de la información, provocaría que la institución debido a la inseguridad de la información y el no seguir políticas que ayuden con esto se verá afectada, sin embargo, si cumpliese con este seguimiento se evitaría perdida de documentación e información electrónica, resguardándola por si existe una circunstancia de error poder recuperar sin ningún inconveniente la información.

1.2 FORMULACIÓN DEL PROBLEMA

El limitado desarrollo de evaluaciones y análisis a la gestión de la información, provoca la existencia de un conjunto ineficiente de controles, ocasionando el incremento de riesgos a la seguridad de procesos del departamento de Tecnologías de la Información y Comunicación en el Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo durante el año 2023.

1.3 JUSTIFICACIÓN

El desarrollo de la presente investigación sobre auditoría informática tiene como finalidad analizar las buenas prácticas que constan de una serie de pasos a seguir, permitirá la toma de decisiones que ayudará con la seguridad de la empresa protegiendo la información, evitando pérdidas y amenazas, gracias a un modelo de

seguridad que admite prevenir inmediatamente los peligros cibernéticos de acuerdo con normativas internacionales.

Es importante destacar que la auditoría informática es principalmente un elemento clave en la gestión de supervisión en lo que refiere a tecnología informática. Un proceso de auditoría Informática ofrece a las empresas ciertas ventajas competitivas frente al mercado, mediante evaluaciones completas en lo que respecta a áreas existentes de una empresa. Dentro de una empresa debe de existir controles, los mismos que podrían ser insuficientes o defectuosos, entonces debe de corregirse para poder incrementar la seguridad.

La auditoría informática ayudará a identificar si las instituciones constan de información actualizada y que se rija a políticas o estándares de seguridad. Es por ello que se debe realizar un análisis de riesgos para poder reducirlos en la medida posible, siguiendo las normativas de control interno 410 tecnologías de la información de la Contraloría General del Estado, que ayuda en el proceso de auditoría a incrementar la efectividad y eficiencia en las operaciones, dentro de la confiabilidad de los informes financieros y el cumplimiento con leyes y regulaciones que se encuentran vigentes.

Con este proceso de auditoría informática se revisa lo que respecta el valor, de los riesgos y los controles en los componentes claves de la tecnología informática, ya sea en las aplicaciones, información, infraestructura y sobre todo el personal técnico, toca tener en cuenta que la empresa consta de estrategias institucionales, sobre todo con funciones y operaciones, no existen ciertas empresas que inviertan en tecnología informática solo por tenerla, posee como fin seguir los objetivos generales de la organización y apoyándose en la gobernanza, la estructura y los procesos empresariales para mantener la tecnología informática centrada en el valor, el riesgo y el control al entorno tecnológico de la empresa.

La inobservancia de lo que muestra la norma de control interno de la contraloría general del estado en el anexo 410 de tecnologías de la información en dicha institución es uno de los inconvenientes en la actualidad ya que no se ha tenido un reajuste de normativas de seguridad durante un determinado tiempo, se busca llevar a cabo una auditoría de seguridad de datos para evaluar el estado de los procesos con el fin de planificar, hacer, controlar y actuar detectando errores permite tomar medidas correctivas. Además, permite conocer los riesgos a los que se somete la información como son los riesgos de interrupción, amenazas y vulnerabilidades en un sistema, permite la confidencialidad, integridad como también afectando la

disponibilidad de la infraestructura tecnológica, que a partir de ello se establece medidas correctivas que permita una mitigación. La empresa con esta investigación obtendrá varios beneficios, porque facilitará la comunicación entre el área de información y directiva de la institución, tales como la realización de entrevistas, la observación y el previo chequeo permitirá obtener la información valiosa para el área directiva, esta información permitirá conocer esta función de esta organización, en los diferentes niveles organizativos. La finalidad del trabajo aportar a la sociedad tomando en cuenta que es viable para ser realizada en dicha institución, debido a que contiene en su estructura interna los reglamentos para la planificación de riesgos informáticos, los cuales pueden ser actualizados mediante un análisis del cumplimiento de las normativas, generando informes de mejora para la organización, apoyando a la calidad de los servicios que se encuentran disponibles para los usuarios en general.

1.4 OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1 Objetivo General

Realizar una auditoría informática a la seguridad de procesos del departamento de Tecnologías de la Información y Comunicación para la identificación de riesgos asociados al manejo de la información con base en la norma ISO 27002 en el Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo.

1.4.2 Objetivos Específicos

- Documentar bibliográficamente bases conceptuales con respecto a la gestión documental con la finalidad de obtener bases concretas sobre el objeto de estudio.
- Conocer acerca de normativas aplicables en la gestión de riesgos informáticos para identificar los requerimientos de la institución.
- Establecer conceptos sobre el tipo de auditoria informática aplicable al Municipio Del Cantón Espejo.
- Proponer acciones de mejora para la seguridad de procesos bajo una metodología que tome en cuenta los riesgos tecnológicos que se enfrenta la institución.

1.4.3 Preguntas de Investigación

- ¿Cuáles son las técnicas e instrumentos de investigación?
- ¿Qué importancia tiene el desarrollo y la organización de tecnologías en los municipios de nuestro país?

- ¿Qué propuestas se planteó de acuerdo con el porcentaje de anteriores encuestas de auditoria informática a los municipios?
- ¿Cuál es tipo de auditoría informática que se aplicará en dicha institución?
- ¿Generar una propuesta de acción de mejora, permitirá a la institución anticiparse ante eventuales problemas?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Una forma de lograr este objetivo es crear políticas de seguridad que definan las reglas para los distintos procesos que se realizan en la organización, en función del ámbito de la misa y de la información interna, como el trabajo, la visión, los objetivos y el entorno.

"La seguridad y los equipos de cómputo y la información que se genera tanto en empresas o establecimientos educativos, se tiene una gran importancia y deben estar debidamente controladas y protegidas". (Muñoz, 2019)

Las alternativas que se puede implementar dentro de las políticas de seguridad informática garantizan la continuidad de una funcionalidad de una empresa, ya que la protección de los datos que se registran dentro de una determinada institución requiere de gran responsabilidad, sobre todo porque pueden ser fácilmente vulnerados debido a una norma que no se actualiza constantemente, puede repercutir como problema y puede generar pérdidas de tiempo y dinero.

"La auditoría informática es el proceso de recopilación, acumulación y evaluación de pruebas para determinar si los sistemas de información protegen los activos de la empresa, mantienen la integridad de los datos, realizan las tareas de la organización con eficacia y utilizan los recursos con eficiencia". (GSITIC, 2019)

"La adecuada funcionalidad de tener un equipamiento de sistemas informáticos debe ser ligado a alcanzar interese importantes de la empresa". (Blog de UTEL, 2019)

Una auditoría informática es un proceso eficaz llevado a cabo por profesionales especialmente formados que se basa en la recopilación, cotejo y evaluación de pruebas para determinar si los sistemas informáticos protegen los activos de una empresa.

La seguridad en equipos informáticos, Gómez (2018) "Mantener todas las operaciones y alcanzar eficazmente los objetivos de las organizaciones, utilizar los

recursos de forma eficiente y cumplir con las leyes según los reglamentos establecidos".

En el caso del entorno empresarial, se trata de un contexto más amplio, donde hay que analizar información general sobre la empresa, como las áreas de especialización, las características, los tipos de servicios ofrecidos, el país de origen, la ubicación geográfica, los destinos de los servicios, la antigüedad de la empresa y el número de empleados (pág. 36).

En su libro Pulgar (2019) aborda la cuestión de la ética en función de la influencia de las experiencias de las personas en diferentes momentos de su vida. Todos estos programas proporcionan un equilibrio entre lo que es aceptable para un empleado y las normas que hay que seguir, lo que no sólo protege los equipos tecnológicos de la empresa, como ordenadores, routers y servidores, sino también los recursos humanos mediante formación y charlas informativas sobre la seguridad de la empresa.

(Vieites, 2019), en su libro de auditoría informática afirma que, La carga útil del virus (parte del programa del virus conocida como "carga útil"). Puede ejecutarse en determinadas circunstancias: en una fecha determinada, tras un cierto número de encendidos del sistema, cuando se ejecuta un programa infectado. Las posibles consecuencias son la aparición de mensajes divertidos o de contenido político o de protesta en la pantalla del ordenador.

Una forma de proteger su sistema de los ataques de virus es utilizar un programa de protección antivirus. Los programas antivirus están diseñados para ejecutarse continuamente, por lo que el usuario no suele ser consciente de que se ha producido al menos un problema.

(Imbaquingo, y otros, 2020) Afirman que: En la actualidad, las organizaciones disponen de una infraestructura informática y están implantando sistemas informáticos y desarrollando procesos para automatizar otros procesos manuales. Los principales problemas de las auditorías informáticas son el elevado coste de su realización, la falta de resultados satisfactorios para los usuarios finales y la posibilidad de obtener resultados negativos relacionados con el hecho de que no siempre son satisfactorios para el usuario final. Por último, pero no menos importante, se subraya la importancia de auditar la seguridad de la información de la propia infraestructura en la nube del auditado.

El objetivo es analizar los errores más comunes que cometen los auditores al realizar auditorías informáticas o de tecnologías de la información, obteniendo información sobre el trabajo realizado que causó problemas en el proceso.

(Kenedy, 2020) Según la investigación que se realiza en esta institución se define que: Los trabajos citados en este documento se refieren no sólo a la auditoría informática, sino también a la auditoría en general, de modo que podemos comprender mejor el estado actual de la técnica en la auditoría informática y comparar diferentes áreas de la auditoría informática.

La revisión con una auditoría es muy importante porque el procesamiento requiere nuevas habilidades, y como no todas las profesiones las tienen, tenemos que crear un ecosistema para nuestros propios servicios, es decir, cómo salir de la caja en la que estamos, a través de la contribución de las diferentes profesiones a la prestación de servicios.

Según el trabajo presentado en la Universidad Nacional de Chimborazo por Rosa Alexandra Gálvez Morocho con el título de "Auditoría Informática de la Cooperativa de Ahorro y Crédito Fernando Daquilema aplicando el marco de trabajo COBIT" concluye lo siguiente:

En el momento de aplicar auditoría informática se aplica un proceso de evaluación y análisis de los procedimientos informáticos llevados a cabo por el departamento de sistemas de la entidad; de acuerdo con el nacimiento de la tecnología de la información, por lo que existe la necesidad de realizar evaluaciones de un sistema informático (Salgado , Osuna, Sevilla, & Morales, 2018)

2.2. MARCO TEÓRICO

2.2.1 Auditoria informática

(Cabello, 2019) La auditoría informática tiene varias finalidades como son evaluar la eficacia y la eficiencia del uso adecuado de los recursos informáticos, el poder evaluar los equipos de cómputo de un sistema o de los procedimientos específico, además ayuda a evaluar los sistemas de información como son los procedimientos, controles, archivos, seguridad y obtención de la información. Se caracteriza por trabajar con sistemas de información ayudando a un control necesario de estos. Es un proceso que permite agrupar y evaluar cierta cantidad de evidencias, las mismas que permitan determinar si los sistemas informatizados salvaguardan los activos, y si una organización puede mantener la integridad de los datos, y poder llevarlos de manera más eficaz.

La auditoría interna es un elemento importante porque permite una auditoría independiente y objetiva con el objetivo de aumentar el valor y mejorar el funcionamiento de una organización mediante un análisis profesional, sistemático, objetivo y disciplinado de las operaciones financieras y administrativas una vez realizadas. La auditoría informática establece acciones de mejora interna que se ejerce por personal de la empresa y la externa que se ejerce por personal independiente de la empresa se toma en cuenta lo expuesto en auditoría informática. Sirve para la revisión y evaluación tanto de control de políticas como de procedimientos, protección de activos, integridad de datos, eficiencia del sistema, seguridad y confidencialidad. Tomando en cuenta las amenazas de ciberataques por falta de medidas de prevención y control obliga a las empresas a utilizar maniobras fraudulentas, sobornos, corrupción y ciberdelincuencia para entrar en nuevos mercados, mientras que las capacidades y recursos técnicos son incapaces de contrarrestar cualquier impacto de riesgo para obtener ventajas políticas y económicas en un contexto nacional. (Fernández, Enrique, Herrera, & Jesús, 2020)

Las organizaciones que utilizan sistemas de información están expuestas a riesgos y, por lo tanto, las organizaciones necesitan detectar ataques complejos que deben ser analizados junto con el análisis del mundo real y los modelos de modelización basados en el riesgo. (Alvarado, Acosta, & Mata de Buonaffina , 2018)

El proceso de planeación de auditoria se basa en un conjunto de técnicas y prácticas que se realiza de manera conjunta en el momento de evaluar y medir como se observa en la Figura 1, donde el proceso de auditoría es posible para las empresas e instituciones.

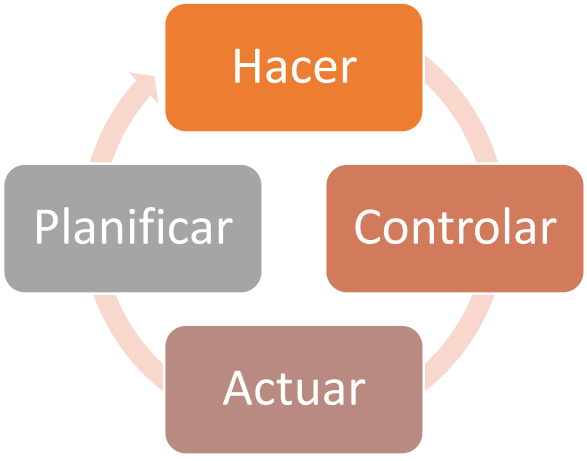


Figura 1. Ciclo Deming.

2.2.2 Procesos de auditoría informática

Según (Aguilar, 2021) afirma que:

Al iniciar con el proceso de planificación de la auditoría informática un auditor de sistemas debe tomar en cuenta los riesgos de una empresa y un control asociado, para continuar con este procedimiento se debe revisar la documentación, con la finalidad de poder identificar controles existentes que se aplica en dicha institución, el aplicar técnicas de diagramas de flujo permitirá documentar aplicaciones automatizada, dando un esquema típico de un determinado programa de planificación en auditoría informática que permite identificar el área donde se realizará esta actividad, el proponer objetivos de auditoría es donde se va a indicar el propósito de realizar dicha evaluación, al plantear alcances de auditoría se tomará en cuenta los sistemas específicos o unidades de organización las cuales se incluyen en la revisión dentro de un lapso de tiempo, por último, la planificación previa en la cual se identifica tanto los recursos como destrezas necesarias para poder desarrollar un trabajo como fuentes de información para demostrar resultados de pruebas revisiones de acuerdo a lugares físicos o instalaciones en el cual se va a auditar. En los procedimientos de auditar se toma en cuenta una serie de procesos los mismos que son efectuados por personas profesionales principalmente de quienes están capacitados para almacenar, adjuntar y sobre todo realizar la evaluación de las evidencias que se obtiene donde la información de la empresa podrá obtener una verificación de los datos que han sido evaluados de acuerdo con la eficiencia con el cumplimiento de leyes y regulaciones. (p. 54)

La auditoría informática trata de la orientación evaluada en sistemas administrativos, ya sea una estructura organizacional, proceso administrativo, operación y ambiente de control para poder determinar pérdidas y diferencias para manejar mejores métodos, formas de control y eficiencia operativa para una mejor utilización de recursos. Tanto en el área administra se realiza un análisis mediante tipos de clasificación, considerando la norma ISO 27002 ya que es más utilizada dentro de organizaciones, es muy independiente del tamaño de empresas o sectores y puede ser implementada, brindando políticas de seguridad que se requiera. La norma ISO 27002 da a conocer recomendaciones y directrices generales para la gestión de seguridad de información, los indicadores de riesgos muestran si la empresa que se va a evaluar se encuentra sujeta o cuenta con alta probabilidad de que pueda ser sometida a un riesgo permitido de acuerdo con la Red Nacional de Investigación y Educación del Ecuador. En la página oficial de ISO donde se hace referencia a dicha información de tomar en cuenta las normas ISO 27002, se destaca el estándar internacional que puede gestionar los riesgos relativos para la seguridad de

información, dicha norma suministra directrices para la gestión de los riesgos. (Ortecho, 2020)

Para la realización de esta auditoría se toma en cuenta el ciclo de Deming donde se emplea lo siguientes procesos, planificar, hacer, consultar, actuar, para la actualización de establecimientos y el mantenimiento y mejoras continuas de acuerdo con Sistema de Gestión de la Seguridad de la Información (SGSI) donde se da a conocer acerca de la organización está utilizando un enfoque sistemático para poder identificar, evaluar y sobre todo poder gestionar los riesgos de seguridad de la información.

La auditoría informática trata de riesgos, dentro de una técnica que permite enfocar los recursos de auditoria hacia los puntos de mayor importancia dentro de las organizaciones, esta técnica es preventiva ante situaciones y eventos no deseados, se centra en tecnologías basadas en riesgos, se toma en cuenta los controles que se llevan a cabo por la administración de la empresa. Al realizar varias investigaciones en las empresas cuentan con un plan de contingencia sanitaria, el coronavirus obligó a las instituciones a abandonar el trabajo de manera radical, Es por ello por lo que se ha tenido que implementar varias metodologías que permitan realizar auditorías anuales implicando procesos informáticos que pueden evidenciar necesidades gracias a un plan de contingencia durante un período de tiempo que ayudaron adoptar medidas por pandemia del COVID-19. (Jorge, 2021)

2.2.3 Técnicas e instrumentos de investigación

Las técnicas que se emplean para una investigación son de mucha importancia ya que ayuda a definir de manera correcta la recolección de datos de acuerdo con el problema de investigación pasando por etapas que servirán para la investigación, para la recolección de datos hay una serie de etapas previas a esta investigación así también como técnicas que ayudan con saberes prácticos o procedimientos para poder obtener resultados. de acuerdo con las técnicas de recolección de información se toma en cuenta a medios prácticos. La recolección de información se refiere a un conjunto de medios que pueden permitir un registro y conservación logrando plasmar lo que se investiga de acuerdo con técnicas utilizadas las mismas que permiten la recolección de información cómo se dará a conocer en la siguiente tabla. Las tecnologías de información y comunicación han cambiado la vida rutinaria de manera vertiginosa, las investigaciones han facilitado el trabajo a través de una comunicación tanto sincrónica como asincrónica dentro de los equipos de investigaciones ayudando a resolver problemas de análisis y recogida de datos.

Tabla 1. Técnicas e instrumentos de investigación.

Datos	Técnicas	Características	Instrumentos
Cuantitativos	Entrevista estructurada	Es considerada una técnica diseñada para la obtención de respuestas verbales a situaciones directas, entre el entrevistador y el encuestado, de tal forma que esta permite aclarar dudas para poder obtener información más completa, facilitando la complementación a la información cuando se aplique otros instrumentos como el cuestionario de observación.	Guía de preguntas
	Encuesta	Una encuesta abarca una serie de preguntas que están dirigidas a una sección demográfica de una población, y tiene como finalidad averiguar estados de opinión, actitudes o comportamientos de las personas ante asuntos específicos.	Cuestionario
	Observación sistemática regulada o controlada	Consiste en el riesgo sistemático, válido, confiable de comportamientos y situaciones observables, a través de un conjunto de categorías y subcategorías.	Fichas

Tabla 2. Técnicas e instrumentos de investigación.

Datos	Técnicas	Características	Instrumentos
Cualitativos	Análisis documental	Implica la revisión de documentos, registros públicos y archivos físicos o electrónicos.	Fichas
	Entrevista no estructurada	Es más íntima, flexible y abierta, va estructurándose conforme avanza el trabajo de campo, se utiliza cuando el problema de estudio no se puede observar o es muy difícil de hacerlo por ética o complejidad. Las preguntas y el orden en que se hacen se adecuan a los participantes.	Guía de preguntas
	Observación sistemática regulada o controlada	Su finalidad es explorar y describir ambientes, comunidades, culturas y los aspectos de la vida social, para lo cual es necesario mantener un papel activo y reflexivo. Estar atento a los detalles, sucesos, eventos e interacciones.	Fichas, libro de campo, cuaderno de notas, mapas.

Biografía e historias de vida	Puede ser individual o colectiva, son revelaciones narrativas acerca de la vida de las personas y se emplean con frecuencia para estudiar patrones culturales en el caso de las ciencias sociales.	Fichas
Documentos, registros, materiales y artefactos.	Estas herramientas nos pueden ayudar a entender el fenómeno central de estudio y conocer los antecedentes de un ambiente, vivencias o situaciones y su funcionamiento cotidiano y anormal. Entre estos elementos podemos mencionar cartas, diarios personales, fotografías, grabaciones de audio y video por cualquier medio, toda clase de expresiones artísticas, documentos escritos de cualquier topo, archivos, huellas, medidas de erosión y desgaste, entre otras.	Fichas

2.2.4 Tecnologías en municipios

2.2.4.1 Equipo de proyectos

En cuanto a los equipos de proyectos tienen la potestad de ejecutar varios proyectos a nivel del territorio digital para ello se toma en cuenta un equipo de trabajo.

Unidad de Dirección: Se conforma por el director de Planificación Institucional o un delegado.

Unidad de Estrategia de Sostenibilidad y Desarrollo Territorial: Se conforma por el personal de conocimiento de planificación y estrategia para el desarrollo territorial e innovación social.

Unidad de Tecnología: Se conforma por un personal que ayuda con el conocimiento informático de sistemas de la información.

Unidad de Administración: Se conforma con conocimientos de administración en la institución para el manejo de procesos de innovación.

Unidad de Comunicación: Se conforma por el personal quien conoce acerca de comunicación social y manejo de comunidades. La gestión interna en los municipios, cada vez muestran cambios significativos los mismos que en los últimos años ya que cada uno de los municipios se encuentran con normativas legales las mismas que dependen de la voluntad de políticas de los líderes.

El fortalecimiento del capital humano se enlaza directamente con la participación de los municipios quienes invierten en obras justas y proyectos dentro de un campo el cual constituye a un instrumento que ayuda a aumentar la productividad y la competitividad tomando en cuenta a la ciudadanía de baja economía a entrar a un

ámbito de desarrollo y ayudando en la comunidad en nutrición, salud, enseñanza y a personas con situaciones vulnerables. Para ayudar a simplificar los métodos administrativos desarrollar ocupaciones poder agilizar gestiones y hacer que la población Tenga una facilidad en obtener recursos es necesario formar equipos de trabajo técnico-político. Se toma en cuenta las instalaciones y recursos que faciliten a la institución llevar a cabo prácticas posibles de manejar con materiales necesarios y adecuados los mismos que constan de oficinas adecuadas, estaciones de trabajo, computadoras de escritorios, accesorios libres a internet, herramientas de informática lo que permitirá un acceso de la información de operaciones. Las instituciones deben de ser eficientes y organizadas ya que lideran un desarrollo cantonal, y deben de disponer de recursos propios tales como personal permanente capacitado quien asume la descentralización en áreas estratégicas, de acuerdo con el interés cantonal, además, contribuye al ordenamiento territorial, seguridad y sobre todo el desarrollo económico, de la misma manera cuidar del bienestar de la población y el ingreso de documentos electrónicos. El área de sistemas tiene como objetivo ocuparse de la red informática que interconecta a la organización también interactúa con aplicaciones programas, así como servicios de uso general, en las organizaciones la parte fundamental es tener definido puestos de trabajo para que funcionen según corresponda como es en el sector de sistema donde se encuentran puestos genéricos que se toman mediante organización y adaptación según las necesidades. (López, y otros, 2019)

Un informático generalista es quien cuenta con destrezas de exploración y un desarrollo de proyectos, experto en desarrollo de proyectos quien se encarga de proyectos en tercer lugar el técnico de sistemas quien es experto en programas, sistemas operativos, el administrador de base de datos quien es un responsable de mantener y gestionar datos. Las instituciones constan de tecnologías las cuales son eficientes y permiten el desarrollo de las actividades que se ajustan a normas que permiten administrar, controlar y poder realizar un seguimiento a servicios de áreas específicas para así poder brindar soluciones informáticas de software y hardware. (Robles, 2022)

Encuesta de madurez de territorios digitales en los Gobiernos Autónomos Descentralizados (GAD) del país durante el año 2013 MYNTEL realiza una encuesta a los 221 GAD donde se obtuvo resultado de 94 municipios los cuales estaban siendo evaluados respecto a infraestructura TIC la gran parte de los evaluados pueden

considerar que es un poco adecuado un despliegue en infraestructura de telecomunicaciones es una situación en la que se tiene como conclusión que durante este período no se obtiene madurez tecnológica debido a factores económicos que puedan ayudar a la tecnología y relaciones con la brecha digital existente. (Cueva, Espinoza, & Jaramillo, 2020)

De acuerdo con una encuesta realizada durante el año 2015 por Intel quién encuesta a aproximadamente 1300 GAD parroquiales cantonales y provinciales en los cuales se obtiene 297 respuestas que han sido válidas, como resultado se obtiene que la utilización de herramientas tecnológicas y como si se debe de tomar en cuenta una agenda Digital en los GAD. (Molina, 2021)

Durante junio de 2017 se realizó una encuesta que se envía a 221 municipios la que es respondida por 101 municipios a nivel nacional teniendo un total de 45,70% del número total considerando que es menor a un total de muestra, pero sin embargo se realiza una muestra aceptable y se permite obtener resultados que permiten conocer acerca de las variables de acuerdo con los sectores provinciales en los cuales se contestaron las encuestas. (Molina, 2021)

2.2.5 Resultados de la encuesta por ejes

2.2.5.1 Componente Transversal de Infraestructura

La infraestructura se puede evidenciar en la Figura 2 de acuerdo a un equipamiento en acceso a internet gratuito cuenta con un 70%, en lo que respecta a zonas para un plan de soterramiento de cables pues cuenta con un 46% así como el plan de ordenamiento en el cableado 41% tomando en cuenta que los GAD tienen que incorporar zonas wifi gratuitas para que puedan mejorar su infraestructura así como también las telecomunicaciones y pueden realizar planes sobre un ordenamiento identificando las zonas que son más prioritarias para dicha implementación. (Sunkel, Trucco, & Espejo, 2019)

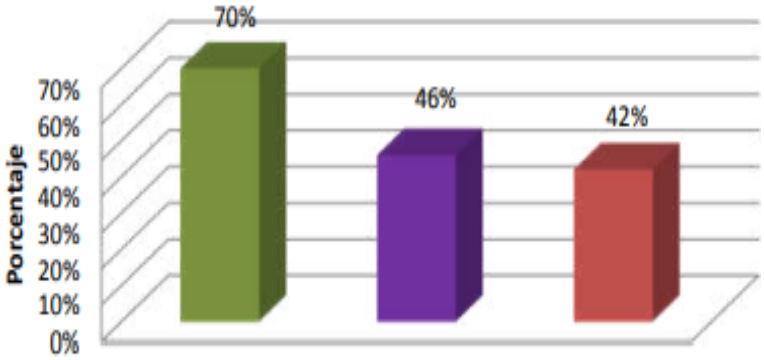


Figura 2. Datos sobre infraestructura
Fuente: MINTEL (2019).

2.2.6 Componente Transversal de Normativa

En componentes transversales de normativas se toma en cuenta un 12% en los GAD que disponen de ordenanzas que tome en cuenta a soterramiento la misma que en la siguiente figura es considerada re con un 25% de planificación de acuerdo a una agencia digital y un 4% que exige una ordenanza la cual estimule desarrollos de tecnología sugiriendo que dentro de los GAD se realiza un plan de soterramiento para poder ordenar donde se incluya planificación de agendas digitales para el desarrollo de tecnologías considerando así las ciudades cada vez más digitales ayudando a la calidad de vida cotidiana. (Parra Zambrano & Pincheira Jiménez , 2019)

Como podemos ver en la Figura 3 donde muestra los porcentajes de acuerdo a una evaluación de componentes transversales de normativas.

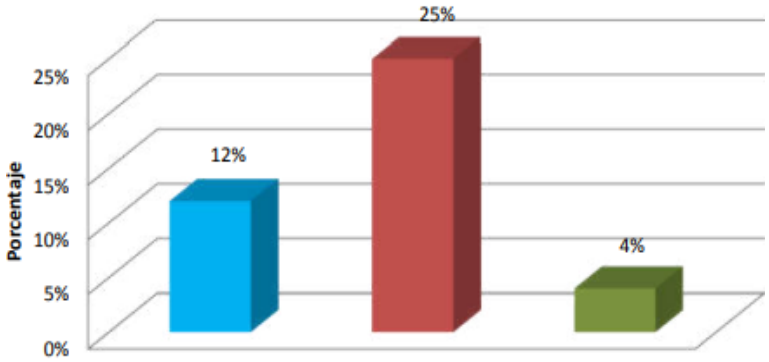


Figura 3. Datos sobre infraestructura
Fuente: MINTEL (2019).

2.2.7 Componentes Transversal de sistemas de información

De acuerdo con componentes transversales en los sistemas de información se puede ver en esta figura que en un 79% usa una firma digital. Sin embargo se sugiere que utilicen herramientas para los beneficios de dicha institución ya que implica un ahorro

de tiempo asimismo de dinero el uso de banca en línea de igual manera simplificando trámites. (Rivoir & Morales, 2019)

Se puede recomendar implementar un sistema de gestión que permita realizar procesos automatizados como es el Quipux ya que este software aumenta la eficiencia, permitiendo que los municipios tengan una mejor administración se sugiere que los municipios puedan utilizar herramientas para una mejor administración ya sea de recursos que pueden ayudar a la implementación de procesos a información de usuarios y el acceso a diferentes datos. La interoperabilidad en los municipios tiene un 41% en el cual se refleja que no se considera necesario dicha facilidad sin embargo favorecería en la eficiencia y eficacia de la gestión. (Baltazar, 2019)

Como podemos ver en la Figura 4 donde muestra los porcentajes de componentes transversales de un sistema de información.

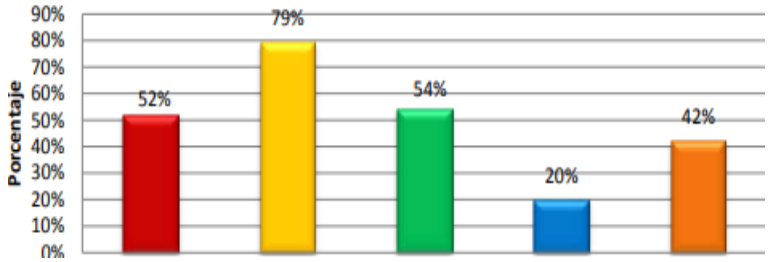


Figura 4. Datos de sistemas.
Fuente: MINTEL (2019).

Se toma en cuenta el 20% en los municipios que disponen de proyecto de datos y se recomienda también que los proyectos que se genere tengan una temática y uso adecuado para que ayude a las personas en ámbitos muy importantes como es emprendimiento como también transparencia y generando más participación de la ciudadanía en instituciones públicas como son los municipios. (Mina, 2019)

2.2.8 Eje E-Gobierno.

Las tecnologías de información y comunicación se encuentran en constante mejora y pueden ir mejorando de acuerdo a un gobierno en línea en los municipios y es que es una parte fundamental para poder establecer una apertura de municipios y poder implementar sistemas que puedan ayudar a progreso y gestión se toma en cuenta un 100% en los municipios que constan de página web las mismas que les permite la participación ciudadana, por ende un 77% puede realizar el uso de estas herramientas las cuales son de gran ayuda ya que permite simplificar trámites y hacerlos de manera rápida. (Ayala, 2022)

Como podemos ver en la Figura 5 donde muestra los porcentajes de un eje E-Gobierno.

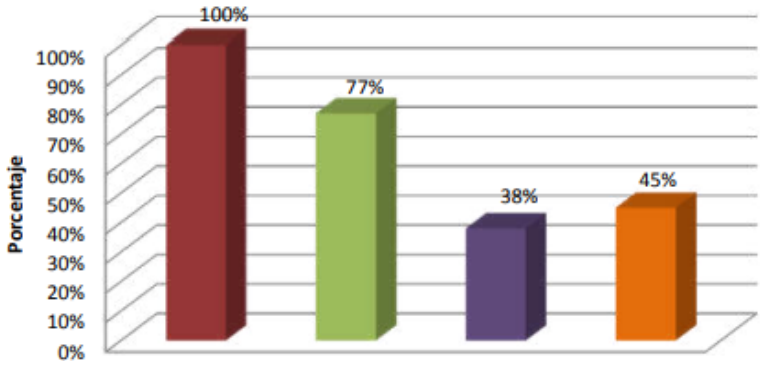


Figura 5. Datos de eje.
Fuente: MINTEL (2019).

2.2.9 Eje de alistamiento digital

En esta ilustración se toma el 33% que tienen una iniciativa de formación de acuerdo con los recursos humanos, el 38% han capacitado a la población sobre tecnologías, el 60% cuentan con un Infocentro, ayudando a la capacidad de la ciudadanía en temas de tecnologías, el 18% dispone de software para la capacitación en temas básicos para especializar en el área de talento humano y que la ciudadanía conozca acerca de conceptos básicos sobre las TIC. (Albán, 2018)

La Figura 6 donde muestra los porcentajes del eje de alistamiento digital.

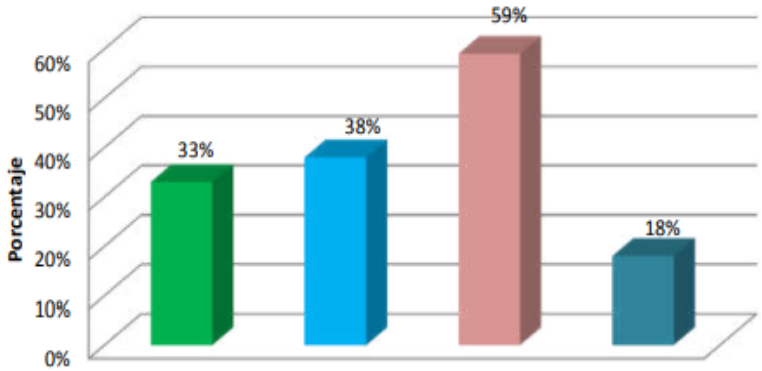


Figura 6. Aislamiento digital.
Fuente: MINTEL (2019).

2.2.10 Ejes esenciales

La Figura 7 donde muestra los porcentajes de ejes esenciales donde se obtiene resultados de acuerdo con la encuesta. Tomando en cuenta estos porcentajes se recomienda que los GAD a nivel nacional pueden hacer el uso de herramientas que

permitan agilizar gestiones y proyecto (Ministerio de telecomunicaciones y de la sociedad de la información, 2018)

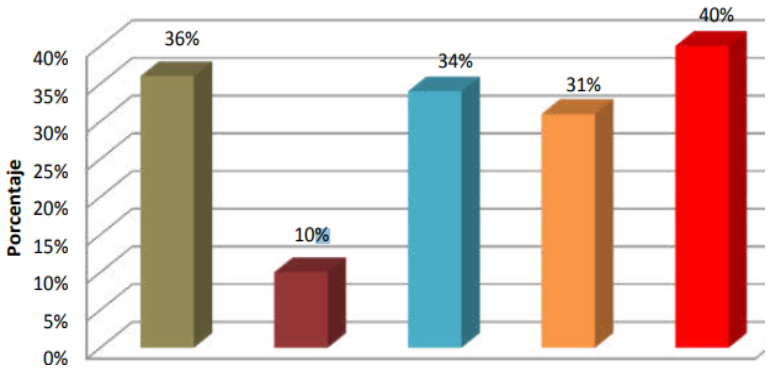


Figura 7. Ejes esenciales.
Fuente: MINTEL (2019).

2.2.11 Ejes productivos

La Figura 8 donde muestra los porcentajes de ejes productivos. El 10% de los GAD administran un plan que promueve alianzas y utilice transferencias tecnológicas y un 23% de los GAD se les sugiere el uso de herramientas que impulsen un comercio electrónico. (Ministerio de telecomunicaciones y de la sociedad de la información, 2018)

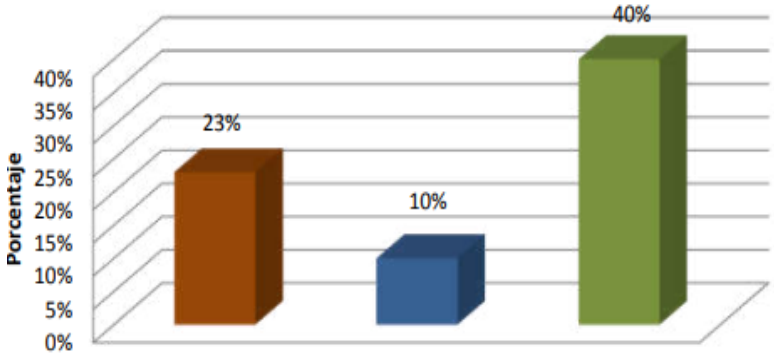


Figura 8. Datos sobre eje productivo.
Fuente: MINTEL (2019).

2.2.12 Dirección de Gobierno de Tecnologías de la Información

El gobierno de TI que es Tecnologías de la Información y comunicación la misma que hereda las metas y estrategias para que los departamentos de una institución puedan proporcionar con eficiencia el uso de las tecnologías y donde se pueda obtener una estructura más comprensible. La dirección de gobierno utiliza un estándar internacional el cual trata de buenas prácticas la función principal es hacer cumplir normas tomando en cuenta seis principios y tres procesos. Es muy importante tomar en cuenta que el Gobierno de TI y la gestión, esta se encarga de evaluar de

acuerdo con los seis principios para establecer condiciones mediante el grupo de directivas que permite decidir y establecer un monitoreo de desempeño, cumplimiento para poder iniciar un progreso de acuerdo con los objetivos, en el campo de administración y gestión donde se planifica y construye directrices. (Cano, Cano, & Pineda, 2018)

2.2.13 Normativa de control interno 410 tecnologías de la información de la Contraloría General del Estado

La ley orgánica de la Contraloría General del Estado, es un organismo que ayuda con la regulación y buen funcionamiento del sistema de control, aprobación, revisión y actualización en las Normas de Control Interno, de acuerdo a estos parámetros de regulación las instituciones del Estado, dictarán las normas o políticas que permitan cumplir con las gestiones propuestas.

En las áreas de tecnología las normativas de control interno de la contraloría general del estado y las entidades que integran el régimen autónomo descentralizado. El objetivo principal de este tipo de auditoría es determinar objetivamente si algo no se está haciendo correctamente. El auditor interno debe ser un profesional cualificado que tenga una visión general de lo que ocurre en la empresa y que sea capaz de detectar si algo no se está haciendo correctamente en la empresa. Si se realiza un trabajo correctivo o preventivo de calidad, una auditoría interna de su SGSI mejorará su seguridad.

2.2.14 ISO/IEC 27002

El objetivo principal es hacer cumplir normas y principios donde los directores de las instituciones en base a los resultados puedan tomar las decisiones correspondientes con la finalidad de dirigir, monitorear y evaluar el uso de la tecnología en las empresas, es aplicable para diferentes organizaciones sin importar el tamaño, teniendo como propósito promover un uso eficaz, eficiente y aceptable de las tecnologías de la información en todas las organizaciones, garantizar que las partes interesadas puedan confiar en la gestión de las tecnologías de la información en la organización y proporcionar orientación a los directivos sobre el uso adecuado de las mismas.

2.2.15 Principios de las normas ISO 27002

El primer principio se basa en la responsabilidad claramente definida para los servicios de tecnologías de información, la planificación informática para apoyar mejor las operaciones.

Capacidades operacionales: Utilizado cuando la organización requiere una clasificación de controles desde una perspectiva práctica:

- Protección de información
- Seguridad en sistemas y redes
- Seguridad en aplicaciones
- Gestión de acceso e identidades
- Gestión de amenazas y vulnerabilidades
- Gestión de eventos de seguridad de la información
- Aseguramiento de la seguridad

Dominios de Seguridad: Atributos usados en el caso que la organización quiera clasificar sus controles desde las perspectivas del campo de aplicación de la seguridad

- Gobernanza y ecosistema
- Protección
- Defensa
- Resiliencia

5.23 Seguridad en el uso de servicios en la nube

8.11 Enmascaramiento de datos

8.12 Prevención de fuga de datos

8.13 Filtrados web

8.28 Codificación segura

2.2.16 Mantenimiento

La tecnología los municipios y sus procesos dependen de la información y de la comunicación el mismo que se relaciona con un conjunto de recursos y herramientas proporcionando mantenimiento en los equipos y programas informáticos, tanto como para aplicaciones, redes y medios, dentro del departamento de los municipios el poder mantener en buen funcionamiento y la optimización de las plataformas tecnológicas que se encuentran en la institución, proveyendo un asesoramiento de manera continua y permanente a el usuario, el poder alcanzar la optimización de las plataformas y satisfacer los requerimientos del sistema informático y dar soluciones a

los problemas de hardware y software en un determinado tiempo lo más reducido posible con la finalidad de maximizar recursos.

El departamento de soporte se encarga de solventar problemas en los sistemas informáticos en dicha organización, el objetivo es utilizar los sistemas de información y las herramientas automatizadas para hacer un uso eficiente y eficaz de los recursos. La norma ISO 27002 trata de incorpora la gestión de riesgos a través de su enfoque o pensamientos basados en el riesgo. Con esto, la empresa tiene en cuenta los riesgos de la organización en su conjunto, lo que es de bastante ayuda a la hora de alcanzar los objetivos que debemos lograr. Es una norma internacional la misma que ayuda a un enfoque de procesos de desarrollo ayuda a la implementación y mejorar la eficiencia de un sistema de gestión de calidad, para así poder aumentar la satisfacción del cliente mediante el cumplimiento de los requisitos del cliente, el enfoque a procesos implica la definición y gestión sistemática de procesos e interacción de acuerdo con la calidad y la dirección estratégica de la organización.

La aplicación de un enfoque o los procesos en un sistema de gestión de calidad se descarga de una comprensión y de coherencia en el cumplimiento de los requisitos como también la consideración de los procesos en términos de valor agregado, el desempeño de un proceso de manera eficaz y también el mejoramiento de los procesos con base a la evaluación de los datos de la información.

2.2.17 Desarrollo

En las instituciones municipales el desarrollo se trata de una instancia que permite la participación democrática y política el encargado de la administración es el alcalde el objetivo principal es de promover el desarrollo socioeconómico sostenible en esta institución mediante la coordinación de acciones y estrategias que permitan promover el uso adecuado de los recursos humanos, materiales y económicos del municipio.

2.2.18 Infraestructura tecnológica

Es un departamento que ayuda a la organización a poder identificar ciertas fallas en sistemas, así como también tomando en cuenta las oportunidades de mejora en los procesos internos permitiendo evaluar la eficiencia y eficacia en los controles internos, mejorando y manteniéndolos vigentes, analizar la aparición de riesgos e implementando procedimientos para minimizar o reducir problemas.

2.2.19 Seguridad informática

La seguridad informática también se llama a la protección de información, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas, con la finalidad de que las personas formen un equipo tecnológico.

2.2.20 Confidencialidad

Se define como uno de los principios que garantizan que toda la información de la organización solo puede ser accedida solo por personal autorizado.

2.2.21 Integridad

Hace referencia a las cualidades de la información que sea correcta y no se haya modificado manteniendo así los datos, los que no deben de haberse alterado por parte de terceros.

2.2.22 Disponibilidad

Se define como uno de los procesos que deben de tener información que no se puede acceder, se trata de la capacidad de un servicio y de autenticación.

2.2.23 Auditoría

Iniciar el control y la evaluación de los documentos, operaciones y registros de los organismos del estado municipal para controlar los procedimientos administrativos, realizados de acuerdo con la normativa vigente.

III. METODOLOGÍA

3.1 ENFOQUE METODOLÓGICO

3.1.1 Enfoque

El enfoque mixto busca responder a un problema de investigación según (Ortega, 2010), el enfoque mixto permite ampliar la perspectiva de estudio dando un criterio más completo el mismo que permite realizar una exploración y evaluación en distintos niveles de fortalezas y debilidades, logrando obtener mayor magnitud y claridad. Al momento de incorporar enfoques optimiza su confiabilidad en los datos de interpretaciones de utilidad y brindando veracidad en la muestra y así en el uso de instrumentos.

En el presente trabajo se toma en cuenta la prioridad de los elementos utilizados en varios enfoques que pueden facilitar la obtención de requerimientos logrando un análisis de resultados en cada proceso y etapa, este enfoque permite reducir una incertidumbre consolidando argumentos que provienen de evaluación de datos, se logra deducir que el enfoque cualitativo representa un porcentaje, basado en la recolección de información en base a entrevistas semiestructuradas, observación y cuantitativo que en su minoría es un complemento de suma importancia, una vez sacado información y dado la propuesta de mitigación a través de un análisis de escalas y proporcionar la información de los problemas de seguridad de la información en el departamento de sistemas.

3.1.2 Tipos de investigación

3.1.2.1 Investigación de campo

Dentro de esta investigación se realiza un estudio de medidas y procesos, con la finalidad de realizar una investigación que permita la recolección de datos y como se toma en cuenta los procesos de búsqueda dando origen a las variables. Donde se utilizan instrumentos para ejecutar un análisis de resultados mediante encuestas, entrevistas y una determinada observación.

3.1.2.2 Investigación Explicativa

La investigación explicativa es importante porque da a conocer las causas, factores y estrategias del problema. Por lo cual como lo define el autor Bernal (2010) "Tiene como fundamento la prueba de hipótesis y busca que las conclusiones lleven a la formulación además estudia el porqué de las cosas, los hechos, los fenómenos o las situaciones, analizando causas y efectos de la relación entre variables" (p. 115).

De este modo, este tipo de investigación es primordial en el estudio de un problema ya que radica en el estudio profundo de las causas centrales de un suceso con la finalidad de poder analizarlo y relacionar variables que puedan dar solución a dicho problema.

La presente investigación se enfoca en el diagnóstico de la empresa determinando la inobservancia de lo que muestra la norma de control interno de la contraloría general del estado en el anexo 410 de tecnologías de la información aumenta los riesgos de seguridad en la información a los procesos del departamento de Tecnologías de la Información y Comunicación.

3.1.2.3 Investigación documental

El proceso de investigación documental se dispone, esencialmente de revisión de información a través de instrumentos como libros, revistas científicas y entre otros estudios. Por ende, según el autor Bernal (2010) define a la investigación documental como "un análisis de información escrita sobre un tema para establecer relaciones, diferencias, etapas, posturas o estados del conocimiento respecto al tema objeto de estudio donde las cuales se caracterizan por abordar problemas de carácter teórico y empírico" (pp. 111-112).

De esta forma, al analizar la investigación documental representa a la relación de documentos escritos o fílmicos con la finalidad de generar conocimiento previo al estudio y dar solución a la problemática del estudio. Por lo cual, las teorías fundamentadas planteadas en la investigación serán de aportes para la culminación de forma exitosa y dando resultados favorables.

La recopilación de información de manera documental ayuda a la obtención de información dispuesta a ser utilizada para proporcionar resultados que sean favorables para establecer una posible solución a un problema, además, el poseer habilidades y sobre todo un nivel considerable de experiencia que permita realizar una investigación.

Este tipo de modalidad de investigación se obtiene a través de una búsqueda, la misma que aporta de la mejor manera a encontrar documentos apropiados para la recolección de datos, de acuerdo con un proceso definido y sobre todo a información que fundamente teorías de acuerdo con el tema.

Con referencia a la utilización de las principales fuentes de información en este tipo de investigación son documentos escritos como libros, informes, etc., además toma en cuenta los antecedentes, que se emplearon en la investigación documental con la cual se logrará obtener la información de las últimas investigaciones realizadas en el área y partir desde ese punto para establecer mejoras.

3.1.2.4. Investigación Descriptiva

La investigación descriptiva es una forma adecuada para analizar los resultados del estudio de modo que se usan gráficos representativos para generar análisis adecuados. Es así como Bernal (2010) conceptualiza como "estudios que muestran, narran, reseñan o identifican hechos, situaciones, rasgos, características de un objeto de estudio o se diseñan productos modelos, prototipos que se soportan en técnicas como la encuesta, la entrevista, la observación y la revisión documental" (p. 113). Por lo cual se define de forma adecuada a los datos, ya que realizan un resumen detallado de los resultados que se han obtenido en el estudio con el fin de generar una explicación estructurada de los datos obtenidos en la investigación.

En el presente trabajo se tomará en cuenta la investigación descriptiva de tal forma que se logre emplear a lo largo de todo el documento caracterizando de forma correcta las variables en donde se logre describir los aspectos esenciales que mediante el análisis de datos permitan describir los hallazgos para mostrarlos en los resultados enfocándose en las variables.

3.2 IDEA PARA DEFENDER

La auditoría informática favorecerá los controles de seguridad disminuyendo los riesgos asociados al manejo de la seguridad en los procesos del departamento de Tecnologías de la Información y Comunicación en el Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo.

3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

3.3.1 Definición de variable independiente

Tabla 3. Variable independiente

Variable Independiente	Definición conceptual de la variable	Dimensión	Indicadores	Técnica	Instrumento	Informante
Auditoría informática	La auditoría informática se la conoce como un proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos lleva a cabo eficazmente los fines de la organización y utiliza	Seguridad de la información. Eficiencia en las actividades. Buena infraestructura de la institución. Normativas actuales Recursos tecnológicos Mejoramiento constante Llevar a cabo buenas prácticas	Nivel de cumplimiento en: Productividad Calidad del servicio Usabilidad Instalaciones Orientación al usuario Eficacia Cumplimiento Satisfactorio Completitud en respuesta a solicitudes. Rapidez Incremento de la seguridad	Análisis Inspección Confirmación Investigación Observación	Entrevista Encuesta según las normativas de control	Analista de sistemas informáticos Asistente de apoyo 3

3.3.2 Definición de variable dependiente

Tabla 4. Variable dependiente

Variable Dependiente	Definición conceptual de la variable	Dimensión	Indicadores	Técnica	Instrumento	Informante
Seguridad de procesos al departamento de TIC	Se trata de aquella área relacionada con la informática y con la protección de la infraestructura del ordenador y todo relacionado con él y en especial, la información que se almacena en él. Así como la que circula entre las redes de ordenadores. Para garantizar y promover la seguridad tic hay una serie de estándares, protocolos, métodos, reglas, utilidades y leyes que han sido diseñadas para eliminar o reducir en la medida de la posible los riesgos que puedan afectar tanto a la infraestructura como a la información contenida.	Seguridad de la información. Eficiencia en las actividades. Buena infraestructura de la institución. Normativas actuales Recursos tecnológicos Mejoramiento constante Llevar a cabo buenas prácticas	Nivel de cumplimiento en: Productividad. Calidad del servicio. Usabilidad. Instalaciones. Orientación al usuario Eficacia. Cumplimiento satisfactorio. Completitud en respuesta a solicitudes. Rapidez Incremento de la seguridad	Porcentaje de efectividad del control de acceso. Porcentaje de efectividad de controles de seguridad de la información. Disponibilidad de la infraestructura de TI. Disponibilidad del servicio de internet. Disponibilidad de equipos de TI. Porcentaje de eficacia de administración de usuarios. Porcentaje de eficacia acceso a instalaciones Porcentaje de eficacia del plan de mantenimiento de equipos Porcentaje de fallas de TI atendidas Promedio de nivel de riesgo de SI.	Entrevista Encuesta según las normativas de control	Analista de sistemas informáticos Asistente de apoyo 3

3.4 MÉTODOS UTILIZADOS

3.4.1 Método analítico

El uso de este método es muy importante ya que permite incluir investigaciones literarias, opiniones púbicas, pruebas científicas y metaanálisis, por lo que suele incluir la compilación de artículos, datos y hechos importantes que son pertinentes a un proyecto. Como lo afirma Bernal (2010) el método analítico "cosiste en descomponer un objeto de estudio, separando cada una de las partes de todo, para estudiarlas en forma individual" (p. 60).

Los procedimientos analíticos son una parte importante para los procesos de auditoría y consiste en evaluación de información acerca de cómo se realizan los procedimientos de la institución.

3.4.2 Método deductivo

Se realizó la investigación fundamentada en este tipo de método debido a que permite establecer conclusiones en base a un análisis general de la situación de la empresa, para poder brindar un aporte de carácter específico sobre las posibles propuestas que serán de ayuda en el desarrollo de los procesos que tenga la empresa. Con base al criterio de Bernal (2010) afirma de forma específica como un tipo de "razonamiento que consiste en tomar conclusiones generales para obtener explicaciones particulares" (p.59).

De forma consecuente, las explicaciones dotadas por el modelo consisten en destacar las falencias de los procesos, con la oportunidad de solucionar estos problemas y facilitar su nivel productivo dentro de la empresa.

En base a lo antes planteado se puede decir que el análisis estadístico establece de forma congruente la forma de relacionar las variables que plantee el problema, con la finalidad de obtener resultados comprobados sobre la eficiencia de procesos. Esto implica realizar de forma significativa los puntos focales para análisis y comprobar la valoración que tiene cada variable, para determinar el nivel de dependencia o independencia según lo planteado en el estudio.

3.4.3 Técnicas e instrumentos

3.4.3.1 Entrevista

Para el desarrollo de la investigación se realizará una recolección de datos gracias a una entrevista que se centre en la interpretación de los mismos, se obtiene varias fuentes de información se trata de un intercambio de conocimientos e interpretarlos dependiendo de la complejidad así mismo fortaleciendo los resultados, tomando en cuenta que se tenga habilidad de conocer acerca de temas relacionados para poder aclarar incertidumbres y sobre todo entrenando las capacidades de comunicación, permitiendo obtener información directa con la persona quien es entrevistado facilitando la comunicación y obteniendo información de acuerdo con el objetivo que se quiere lograr.

El poder observar e interpretar minuciosamente los procesos que se sigue en dicha institución y en los diferentes departamentos se puede validar resultados acerca de características y los diferentes comportamientos de acciones que son de mayor necesidad para cumplir con el objeto de estudio.

3.4.3.2 Encuesta

La recolección de datos mediante encuestas es una técnica ampliamente utilizada en investigación de mercado, estudios de opinión y análisis social. Consiste en la recopilación de información de un grupo de individuos mediante la presentación de preguntas estructuradas.

Se entregaron cuestionarios impresos a los participantes, quienes debían completar y devolver los formularios. Independientemente del método utilizado, es importante diseñar la encuesta de manera clara y precisa, utilizando preguntas que sean fáciles de entender y responder. También es recomendable realizar pruebas piloto previas a la implementación para identificar posibles errores o ambigüedades en las preguntas.

Una vez recolectados los datos, se deben tabular y analizar para obtener resultados significativos. Esto puede incluir la elaboración de gráficos, tablas o la aplicación de técnicas estadísticas. La recolección de datos mediante encuestas es una herramienta efectiva para obtener información de un grupo de individuos. Sin embargo, requiere de una cuidadosa planificación y diseño para asegurar la validez y confiabilidad de los resultados obtenidos.

3.5 ANÁLISIS ESTADÍSTICO

3.5.1 Población y muestra

Dentro del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo se ha seleccionado con un número alrededor de 42 personas del departamento de fiscalización, departamento de asesoría jurídica, departamento de secretaría general, departamento de atención ciudadana, departamento de participación ciudadana y control social, departamento de dirección de gestión financiera, departamento de contabilidad, departamento de rentas, departamento de tesorería, departamento de bodega, departamento de comisaría municipal, departamento de administración general, departamento de policía municipal, departamento de dirección de gestión administrativa y talento humano, departamento de compras públicas, departamento de seguridad ciudadana, departamento de comunicación, departamento de institucional y pública, departamento de dirección de planificación estratégica, departamento de participación ciudadana y control social, departamento de sistemas.

Dentro de esta población como una totalidad y con el fin de realizar estudios he seleccionado una muestra por conveniencia de 42 personas abarcando el personal administrativo ya que son quienes se encuentran en constante manejo de equipos informáticos es por lo que el aplicar la encuesta favorece a la investigación.

Por otra parte, se excluyó al personal de dirección de gestión ambiental y desarrollo económico local, dirección de gestión de obras públicas y vialidad ya que los usuarios no manejan equipos informáticos, es decir, desconocen los procesos, capacitaciones brindadas por el área de sistemas, acceso a la información, entre otros acerca de la seguridad de procesos, como se observa en la tabla 5.

Tabla 5. Población y muestra

Muestra por conveniencia	Muestra(número)	Técnica
Departamento de fiscalización	2	Encuesta
Departamento de asesoría jurídica	2	Encuesta
Departamento de secretaría general	1	Encuesta
Departamento de atención ciudadana	2	Encuesta
Departamento de participación ciudadana y control social	3	Encuesta
Departamento de dirección de gestión financiera	2	Encuesta
Departamento de contabilidad	1	Encuesta
Departamento de rentas	3	Encuesta
Departamento de tesorería	2	Encuesta
Departamento de bodega	2	Encuesta
Departamento de comisaría municipal	2	Encuesta
Departamento de administración general	2	Encuesta
Departamento de policía municipal	2	Encuesta
Departamento de dirección de gestión administrativa y talento humano	1	Encuesta
Departamento de compras públicas	2	Encuesta
Departamento de seguridad ciudadana	2	Encuesta
Departamento de comunicación	3	Encuesta
Departamento de institucional y pública	2	Encuesta
Departamento de dirección de planificación estratégic	2	Encuesta
Departamento de participación ciudadana y control so	2	Encuesta
Departamento de sistemas	2	Entrevista
	42	

La tabla da un resultado de población y muestra escogida para el análisis de la investigación. La encuesta fue realizada a la muestra de 42 personas, debido a que están en contacto con los equipos informáticos que mantienen la empresa. El personal se encuentra distribuido entre, jefes de área, personal.

IV. RESULTADOS Y DISCUSION

4.1 RESULTADOS

4.1.1. Planificar la auditoría informática

Objetivo de auditoría

Analizar los controles y procesos del departamento de sistemas del G.A.D Municipal, con el fin de evaluar el cumplimiento de normativas e identificar riesgos e impactos que se pueden provocas en la institución.

Alcance

El alcance de la investigación se enfoca en inspeccionar el grado de madures de las normas ISO/IEC 27002 y la normativa 410 de tecnologías de la información de la contraloría general del estado, estándares de seguridad de la información, para así realizar una auditoría informática y según los resultados, ejecutar un plan de contingencia para la mejora continua de seguridad a los procesos del departamento de TIC.

Justificación

El análisis de normativas de control se lo realizará en el departamento de sistemas ya que está sujeto a vulnerabilidades y amenazas, poniendo en riesgo la pérdida de disponibilidad, confidencialidad e integridad, de los datos, detectando falencias que se pueden minimizar o riesgos que se puede evadir.

Datos informativos

Gobierno Autónomo Descentralizado Municipal del Cantón Espejo

Logotipo

Figura 9. GADME
Fuente: GADME (2019).

Ubicación

Calle Esmeraldas y Salinas frente al Parque principal, El Ángel, Carchi, Ecuador.

Análisis de la situación actual del GAD Municipal de Espejo

El GAD Municipal de Espejo es una institución que ayuda a generar desarrollo social, económico, productivo, vial, en un ambiente sano, está dedicado a prestaciones de servicios que permite brindar seguridad y eficiencia, procurando el bienestar de la colectividad dentro de áreas urbanas y rurales, fomentando la resolución de problemas, coordinando con otras entidades para mejorar el desarrollo continuo del cantón.

La estructura organizacional del gobierno autónomo descentralizado municipal del cantón Espejo se rige a una visión y misión establecida en la constitución de la república y el código orgánico de la organización territorial, autonomía y descentralización la cual se enfoca en productos, servicios y procesos con el propósito de asegurar su ordenamiento orgánico o interno.

En el departamento de sistemas el área que sí es manual forma parte de dicha institución municipal comprendo varias funciones que determinan un laboral muy importante, la cual es dependiente de la dirección de gestión administrativa y puede garantizar procesos que infieren gran impacto en la seguridad de la información siendo activos de mayor prioridad para la organización. Una institución que es eficiente y organizada para el cantón debe de disponer de recursos propios, personal permanente sobre todo capacitado, que asume la descentralización en áreas de interés, lo que contribuye así al ordenamiento la territorial, a la seguridad, al desarrollo económico y bienestar de la población del cantón Espejo.

El inventario de activos se encuentra estructurado de la siguiente manera, existen 99 computadores, de los cuales 89 se encuentran en funcionamiento, como también 35 impresoras en funcionamiento.

Inventario de activos del departamento de sistemas del GADME

Tabla 6. Inventario de activos informáticos

Nombre De PC	Ubicación	MAINBOARD	MEMORIA RAM				
		MANUFACTURER	TIPO	TAMAÑO	SLOT	CAPACIDAD MÁXIMA	CAPACIDSAD MÁXIMA GB
Analista Sistemas	unidad de sistemas	ASUSeK COMPUTERN INC	DDR4	16 GB	4	67108864	64
Tesorera (Rosalina Enríquez)	Libre	HP	DDR3	4GB	2	16777216	16
Sistemas Álvaro	unidad de sistemas	Gigabyte technology Co.Ltd.	DDR4	8GB	4	67108864	64
Comunicación Martin	unidad de comunicación	ASUSTeK COMPUTER INC.	DDR4	64GB	4	134217728	128
Miguel	unidad de comunicación	Gigabyte technology Co.Ltd.	DDR4	8GB	4	67108864	64
Laura	unidad de comunicación	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Secretaria Germania	secretaria general	Intel Corporation	DDR2	2GB	2	4194304	4
Auris Tatiana	secretaria general	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Jessica Vaca	Jurídico	Intel Corporation	DDR3	4GB	2	33554432	32
Arturo Leon	Jurídico	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Kelly Andamarca	Alcaldía	Intel Corporation	DDR3	4GB	2	16777216	16
Paula García	dirección financiera	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Mercedes Cifuentes	Contabilidad	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Jessenia Chamorro	Contabilidad	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Nataly Carrera	directora financiera	ASUSTeK COMPUTER INC.	DDR4	8GB	4	67108864	64
Rubí García	compra publica	Forxconn	DDR2	3GB	2	2097152	2
Carlos Enríquez	gestión ambiental	MICRO-STAR INTERNATIONAL CO.LTD	DDR3	2GB	4	4194304	4
Pablo Yazan	gestión ambiental	HEWLETT-PACKARD	DDR3	8GB	2	16777216	16

Paola Rosas	gestión ambiental	Intel Corporation	DDR2	2560GB	2	8388608	8
Joselito Meneses	gestión ambiental	Forxconn	DDR3	2GB	2	8388608	8
Emerson Bravo	gestión ambiental	Gigabyte technology Co.Ltd.	DDR4	8GB	3	67108864	64
Marco Benalcázar	gestión ambiental	Intel Corporation	DDR2	4GB	2	8388608	8
Yolanda Vallejo	obras publicas	Forxconn	DDR3	2GB	2	ERROR	0
Miguel Mafla	obras publicas	Pegatron corporation	DDR2	4GB	4	ERROR ACCESO DENEGADO	0
Marco Guerrero	obras publicas	ASUSTeK COMPUTER INC.	DDR3	12GB	4	16777216	16
Humberto Paspuezan	obras publicas	Gigabyte technology Co.Ltd.	DDR4	8GB	3	67108864	64
Janeth Chafuelan	compras publicas	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
María Elena Carlosama	planificación estratégica	Forxconn	DDR3	6GB	2	4194304	4
Israel Guerrero	planificación estratégica	Gigabyte technology Co.Ltd.	DDR4	8GB	3	67108864	64
Paola Camacas	planificación estratégica	HEWLETT-PACKARD	DDR3	4GB	2	16777216	16
Margoth Pozo	Fiscalización	ASUSTeK COMPUTER INC.	DDR3	8GB	4	16777216	16
Franklin Cadena	jefatura de planificación	Gigabyte technology Co.Ltd.	DDR4	8GB	3	67108864	64
Franklin Pulles	no tiene computador	NO TIENE COMPUTADOR	NO	NO	NO TIENE COMPUTADOR	NO TIENE COMPUTADOR	NO TIENE COMPUTADOR
Paul Chandi	no tiene computador	NO TIENE COMPUTADOR	NO	NO	NO TIENE COMPUTADOR	NO TIENE COMPUTADOR	NO TIENE COMPUTADOR
Zandra España	Recepción	ASRock	DDR4	4GB	2	33554432	32
Gissel Chamorro	servicio medico	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32

El CPU No Enciende	servicio medico	NO	NO	NO	NO	NO	NO
Edison Garcia	Rentas	ASUSTeK COMPUTER INC.	DDR4	4GB	2	67108864	64
Cristina Caisedo	Rentas	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Edison Garcia	Rentas	Intel Corporation	DDR2	2GB	2	4194304	4
Tiffany Soto	rentas, recaudación	ASUSTeK COMPUTER INC.	DDR4	4GB	4	67108864	64
Maria Augusta Herrea	Tesorería	ASUSTeK COMPUTER INC.	DDR4	8GB	4	67108864	64
Veti Meneses	Tesorería	Forxconn	DDR2	4GB	2	2097152	2
Zoila Montalvo	avalúos y catastros	DELL INC.	DDR3	8GB	4	33554432	32
Diana Portilla	avalúos y catastros	ASUSTeK COMPUTER INC.	DDR4	16GB	4	67108864	64
Henrry Narvaes	avalúos y catastros	DELL INC.	DDD 3	8GB	4	33554432	32
Jhonny Torres	bodega manejo y bienes	ASUSTeK COMPUTER INC.	DDR3	8GB	4	16777216	16
Guillermina Montenegro	bodega manejo y bienes	Gigabyte technology Co.Ltd.	DDR4	4GB	4	67108864	64
Guilman Cazares	talento humano	ASUSTeK COMPUTER INC.	DDR4	8GB	4	67108864	64
Jorge Lomas	talento humano	ASUSTeK COMPUTER INC.	DDR3	8MB	4	16777216	16
Tito Sanches	registro de la propiedad	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Nataly Cumba	registro de la propiedad	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32

Wiliam De La Cadena	registro de la propiedad	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Servidor Al Registro	registro de la propiedad	BIOSTAR Group	DDR3	2GB	4	4194304	4
Susana Meneses	registro de la propiedad	ASUSTeK COMPUTER INC.	DDR4	8GB	2	33554432	32
Gabriel Iñyiguez	atención prioritaria y deportes	Forxconn	DDR3	2GB	2	8388608	8
Pamela Meneses	atención prioritaria y deportes	BIOSTAR Group	DDR3	2GB	4	4194304	4
Binicio Guama	atención prioritaria y deportes	BIOSTAR Group	SDRAM	2GB	4	ACCESO DENEGADO	0

Tabla 7. Desarrollo de sistemas

Categoría	Nombre del Software	Descripción	Lenguaje	Desarrollo Categoría	Nombre del Software	Descripción	Lenguaje	Desarrolladores
Gestión de archivo	Sistema de archivo	Sistema que permite llevar a la institución loa archivos documentados.					Javascript	Roberto Almendariz Rueda
Gestión de archivo	Archivo Virtual	Se trata de un software web que permite almacenar organizadamente la información de los archivos, tanto como documentos escaneados.					PHP	Hernán Veliz
Gestión de correspondencia	Guía de archivo	Ayuda a registrar el envío de documentos de la institución					Java	Franklin Arias
Gestión de documentos	Contenedor de archivos LOTAIP	Contenedor de archivos para el GADME					PHP	Lenin Fernando Calle

Gestión de documentos	Sistema de gestión de documentos Quipux	Sistema de gestión que ayuda a el registro, control, circulación y sobre todo la organización de los documentos digitales o físicos que se recibe y se envían dentro de la institución.	PHP	David Gamboa
Gestión de documentos	Sistema documental	Gestión de documentación interna	C++	Klever Pozo
Gestión de inventarios	Inventario IP	Software de inventarios con IP y recursos físicos		Klever Pozo
Gestión de inventarios	Sistema de bodega	Sistema que permite el control de bodega	Java	Klever Pozo
Gestión de inventarios	Sistema de administración de los bienes	Se lo desarrolla con la finalidad de gestionar la administración de suministros de la institución		Klever Pozo
Gestión de inventarios	Sistema de suministros	Sistema que permite llevar los inventarios de suministros de las oficinas de la institución	Java	Klever Pozo
Gestión de inventarios	Sistema que permite un inventario de software público	Sistema de inventario de software que permite al sector público.	Oddo	Jhonnson Sani
Gestión de inventarios	Sistema de bienes	Software de manejo de bienes y genera acta de entrega y reporte con bitácoras con los movimientos de bienes	PHP	Klever Pozo
Gestión de inventarios	Sistema de insumos	Sistema para controles de inventario de gastos, permite realizar el registro de ingresos y egresos, tanto como los requerimientos de los funcionarios para la solicitud de los diferentes insumos varios.	Java	Klever Pozo
Gestión de inventarios	SIGAFI	Aplicativo para el registro de mantenimiento de los equipos	PHP	Franklin Arias
Gestión de inventarios	Sistemas de inventarios de bienes y asistencia humanitaria	Software para el control de inventario de bienes de la institución, bodega y custodia de la asistencia humanitaria	Phyton	Vanessa Robles

Gestión de proyectos	Sistema de información para los Gobiernos Autónomos Descentralizados SIGAD	Herramienta informática que se diseña para la captura de información que se requiere para el cálculo y cumplimiento de metas, tanto para la asignación de los recursos de los gobiernos autónomos descentralizados.	Java	Claudia Quezada
Gestión de Talento humano	Aplicación de marcaciones	Interfaz web para marcar el ingreso y salida del personal, con el objetivo de regular los permisos o atrasos	PHP	Mario Humberto Recalde Bravo
Gestión de Talento humano	Aplicación de talento humano	Aplicativo para gestionar las solicitudes de vacaciones y acciones personales.	VB.NET	Paola León
Gestión de Talento humano	Aplicación de pagos mensuales	Sistema de gestión para gestionar certificados y visualización de roles y pagos mensuales.	PHP	Sandra Elizabeth Meza Cevallos
Gestión de Talento humano	KARDEX personal	Registro de datos de manera personal y los movimientos personales.	C++	Washington Bravo
Gestión financiera	Sistema de integrado de recaudación del SRI	Aplicación que permite la realización de recaudación correspondiente a servicios de DIGERCIC por medios de las agencias a nivel nacional	Java	Manuel Plascencia

Organización del GADME

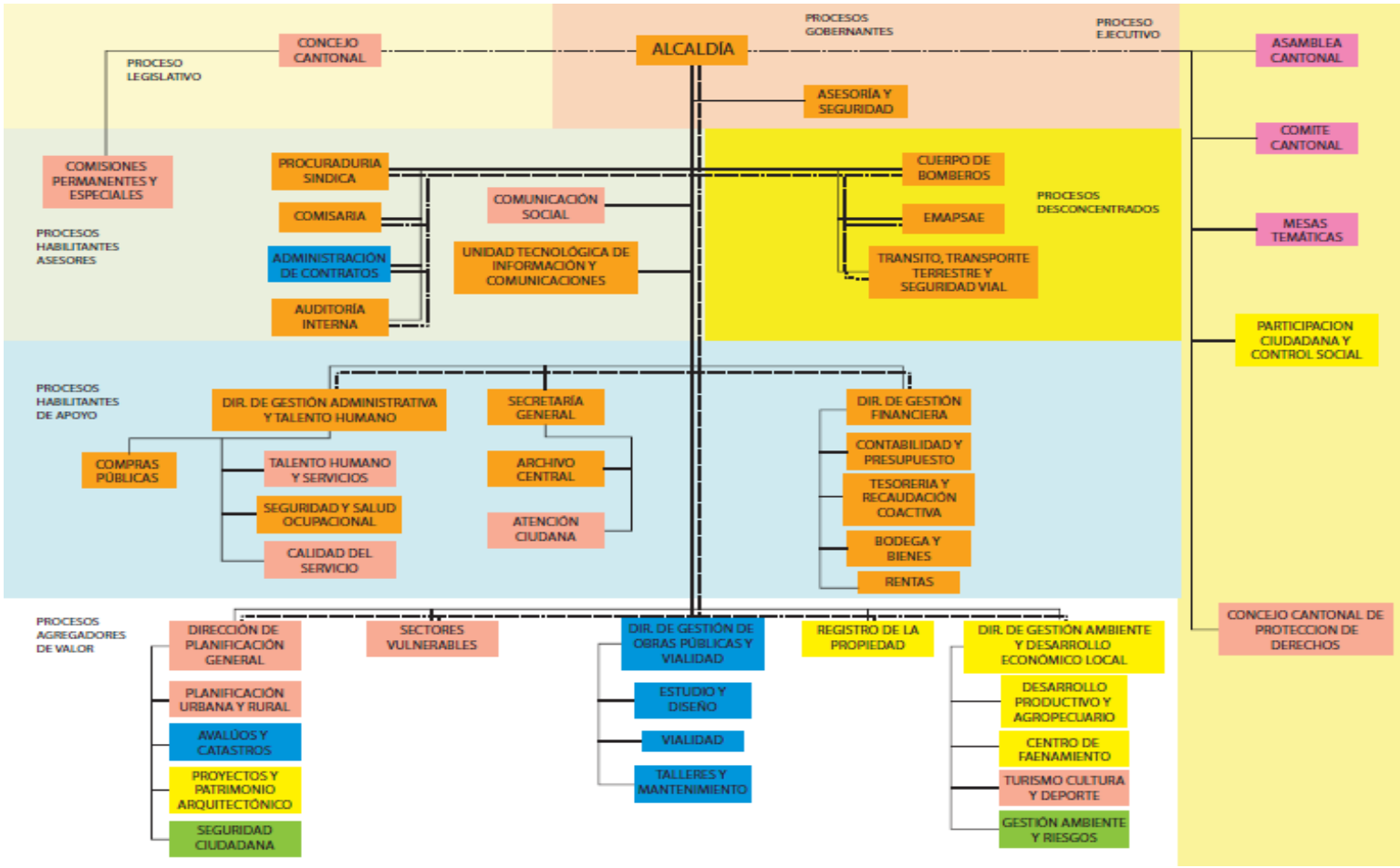


Figura 10. Situación actual del GADME
Fuente: GADME (2019).

4.1.1.2 Hacer la auditoría

Se realizó la auditoría mediante la coordinación tanto con el director de gestión administrativa y talento humano, el analista de sistemas informáticos, se verificó la disponibilidad del tiempo para poder realizar las visitas. Además, se tomó en cuenta el alcance de los objetivos y justificación de la auditoría, realizando el cronograma de actividades, sobre todo dando a conocer acerca de los instrumentos que se va a aplicar dentro de este departamento y las oficinas en general.

Equipo auditor

Auditor Leidy Murillo

Asesor Ing. Marco Yandún, MSc.

Identificación de documentos aplicables

La auditoría de seguridad de procesos a el departamento de sistemas en el Gobierno Autónomo Descentralizado Del Cantón Espejo fue lleva a cabo aplicando la normativa ISO 27002:2013. Con un total de 114 controles, donde 33 no se aplicaron a la revisión por motivo de que los procesos que yo he tomado en cuenta son infraestructura, seguridad, desarrollo, mantenimiento, y no he tomado en cuenta la seguridad física, administración de actividades que realiza el departamento de talento humano, los mismo que son enlistados a continuación:

- A.11.1.1 Perímetro de seguridad física
- A.11.1.2 Controles físicos de entrada
- A11.1.3 Seguridad de oficinas, despachos y recursos
- A.11.1.4 Protección contra las amenazas externas y ambientales
- A.11.1.5 El trabajo en áreas seguras
- A.11.1.6 Áreas de carga y descarga
- A.11.2.1 Emplazamiento y protección de equipos
- A.11.2.2 Instalaciones de suministro
- A.11.2.3 Seguridad del cableado
- A.11.2.5 Retirada de material propiedad de la empresa
- A.11.2.6 Seguridad de los equipos fuera de las instalaciones
- A.11.2.7 Reutilización o eliminación segura de equipos
- A.11.2.8 Equipos de usuario desatendido
- A.11.2.9 Políticas de puesto de trabajo despejado y pantalla limpia
- A.12.1.3 Gestión de capacidades
- A.13.2.3 Mensajería electrónica

- A.14.1.1 Análisis de requisitos y especificaciones de seguridad de la información
- A.14.1.2 Asegurar los servicios de aplicaciones en redes públicas
- A.14.1.3 Protección de las transacciones de servicios de aplicaciones
- A.14.2.4 Restricciones a los cambios de paquetes de software
- A.14.2.7 Externalización del desarrollo de software
- A.15.1.1 Políticas de seguridad de la información en las relaciones con los proveedores
- A.15.1.2 Requisitos de seguridad en contratos con terceros
- A.15.1.3 Cadena de suministro de tecnología de la información y de las comunicaciones
- A.15.2.1 Control y revisión de la provisión de servicios del proveedor
- A.15.2.2 Gestión de cambio en la provisión del servicio del proveedor
- A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información
- A.18.1.1 Identificación de la legislación aplicable y de los requisitos contractuales
- A.18.1.2 Derecho de propiedad intelectual (DPI)
- A.18.1.3 Protección de los registros de la organización
- A.18.2.1 Revisión independiente de la seguridad de la información
- A.18.2.2 Cumplimiento de las políticas y normas de seguridad
- A.18.2.3 Comprobación del cumplimiento

Los controles que se emplean para la evaluación de la institución son os siguientes:

- A.5.1.1 Políticas para la seguridad de la información
- A.5.1.2 Revisión de las políticas para la seguridad de la información
- A.6.1.1 Roles y responsabilidades en seguridad de la información
- A.6.1.2 Segregación de tareas
- A.6.1.3 Contacto con las autoridades
- A.6.1.4 Contacto con grupos de interés especial
- A.6.1.5 Seguridad de la información en la gestión de proyectos
- A.6.2.1 Políticas de dispositivos móviles
- A.6.2.2 Teletrabajo
- A.7.1.1 Investigación de antecedentes
- A.7.1.2 Términos y condiciones del empleo
- A.7.2.1 Responsabilidades de gestión
- A.7.2.2 Concienciación, educación y capacitación en seguridad de la información

- A.7.2.3 Proceso disciplinario
- A.7.3.1 Responsabilidades ante la finalización o cambio
- A.8.1.1 Inventario de activos
- A.8.1.2 Propiedad de los activos
- A.8.1.3 Uso aceptable de los activos
- A.8.1.4 Devolución de activos
- A.8.2.1 Clasificación de la información
- A.8.2.2 Etiquetado de la información
- A.8.2.3 Manipulado de la información
- A.8.3.1 Gestión de soportes extraíbles
- A.8.3.2 Eliminación de soportes
- A.8.3.3 Soportes físicos en tránsito
- A.9.1.1 Política de control de acceso
- A.9.1.2 Acceso a las redes y a los servicios de red
- A.9.2.1 Registro y baja de usuario
- A.9.2.2 Provisión de acceso de usuario
- A.9.2.3 Gestión de privilegios de acceso
- A.9.2.4 Gestión de la información secreta de autenticación de los usuarios
- A.9.2.5 Revisión de los derechos de acceso de usuario
- A.9.2.6 Retirada o reasignación de los derechos de acceso
- A.9.3.1 Uso de la información secreta de autenticación
- A.9.4.1 Restricción del acceso a la información
- A.9.4.2 Procedimientos seguros de inicio de sesión.
- A.9.4.3 Sistema de gestión de contraseñas
- A.9.4.4 Uso de utilidades con privilegios del sistema
- A.9.4.5 Control de acceso al código fuente de los programas
- A.10.1.1 Política de uso de los controles criptográficos
- A.10.1.2 Gestión de claves
- A.11.2.4 Mantenimiento de los equipos
- A.12.1.1 Documentación de procedimientos de las operaciones
- A.12.1.2 Gestión de cambios
- A.12.1.4 Separación de los recursos de desarrollo, prueba y operación
- A.12.2.1 Controles contra el código malicioso
- A.12.3.1 Copias de seguridad de la información
- A.12.4.1 Registro de eventos

- A.12.4.2 Protección de la información del registro
- A.12.4.3 Registros de administración y operación
- A.12.4.4 Sincronización del reloj
- A.12.5.1 Instalación del software en explotación
- A.12.6.1 Gestión de las vulnerabilidades técnicas
- A.12.6.2 Restricción en la instalación de software
- A.12.7.1 Controles de auditoría de sistemas de información
- A.13.1.1 Controles de red
- A.13.1.2 Seguridad de los servicios de red
- A.13.1.3 Segregación en redes
- A.13.2.1 Políticas y procedimientos de intercambio de información
- A.13.2.2 Acuerdos de intercambio de información
- A.13.2.4 Acuerdos de confidencialidad o no revelación
- A.14.2.1 Política de desarrollo seguro
- A.14.2.2 Procedimiento de control de cambios en sistemas
- A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo
- A.14.2.5 Principios de ingeniería de sistemas seguros
- A.14.2.6 Entorno de desarrollo seguro
- A.14.2.8 Pruebas funcionales de seguridad de sistemas
- A.14.2.9 Pruebas de aceptación de sistemas
- A.14.3.1 Protección de los datos de prueba
- A.16.1.1 Responsabilidades y procedimientos
- A.16.1.2 Notificación de los eventos de seguridad de la información
- A.16.1.3 Notificación de puntos débiles de la seguridad
- A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información
- A.16.1.5 Respuesta a incidentes de seguridad de la información
- A.16.1.6 Aprendizaje de los incidentes de seguridad de la información
- A.16.1.7 Recopilación de evidencias
- A.17.1.1 Planificación de la continuidad de la seguridad de la información
- A.17.1.2 Implementar la continuidad de la seguridad de la información
- A.17.2.1 Disponibilidad de los recursos de tratamiento de la información
- A.18.1.4 Protección y privacidad de la información de carácter personal
- A.18.1.5 Regulación de los controles criptográficos

Estado de situación previo a la auditoría

Revisión de auditorías previas

No se encontró documentación de haber realizado una auditoría de seguridad de procesos a el departamento de sistemas de esta institución. Una vez aplicada la encuesta a la muestra escogida por conveniencia para la presente investigación, se muestra los siguientes resultados.

Pregunta 1: **¿Durante qué tiempo usted solicita al área de sistemas que le facilite mantenimiento preventivo y correctivo en los equipos de cómputo?**

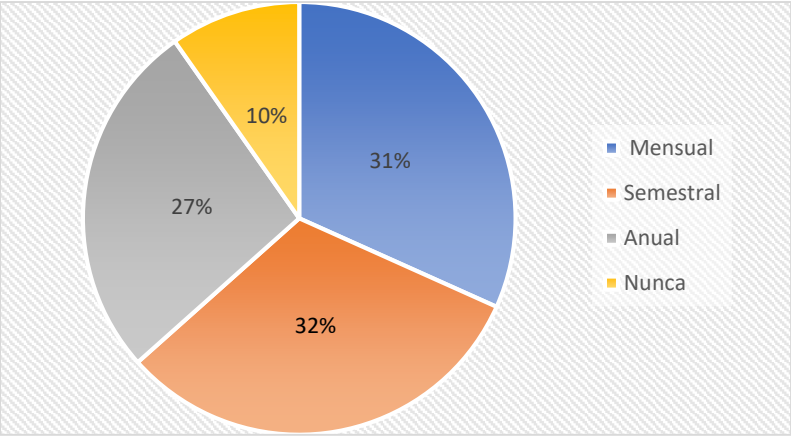


Figura 11. Pregunta 1

Análisis e interpretación. El 90% de los administrativos solicita al departamento de sistemas que le facilite mantenimiento preventivo y correctivo en los equipos de cómputo por lo que se determina que existe una sobrecarga de trabajo para los funcionarios del área de sistemas ya que son pocos técnicos en el área de sistemas y tienen actividades de desarrollo, infraestructura y seguridades, no obstante, a pesar de los limitados recursos tratan de cubrir con la mayor parte de necesidades.

Pregunta 2: **¿Qué servicios brinda el departamento de sistemas?**

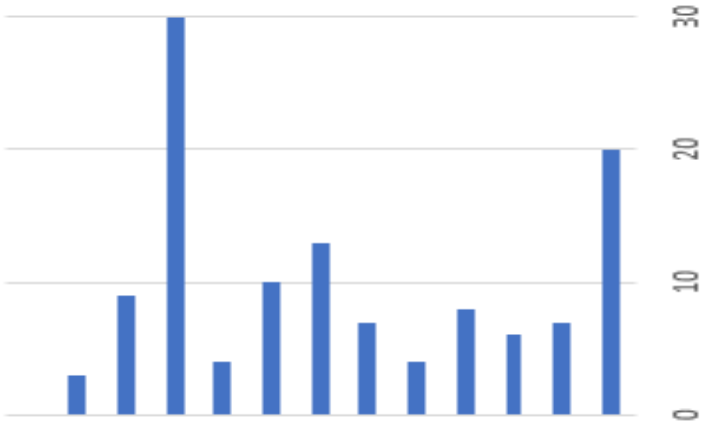


Figura 12. Pregunta 2

Análisis e interpretación. Según el gráfico podemos afirmar que la mayoría de los empleados desconocen acerca de los servicios que brinda el departamento de sistemas, el personal administrativo conoce más sobre el mantenimiento y reparación de equipos de cómputo, administración y mantenimiento de los sistemas existentes en la institución, excepto en los temas de administración de redes, revisión periódica de la información, evaluación, adquisición de software y paquetería, control de compras de todo lo que respecta a equipos informáticos, consumibles y accesorios computacionales son temas que no se conocen la implementación y administración de los servicios de Internet e Intranet, correos electrónicos, en lo que respecta a contratación de servicio y asesorías externas, elaboración de manuales y documentación, el desarrollo de nuevos sistemas, estudios de factibilidad, compra e instalaciones de equipo.

Pregunta 3: **¿En el último mes cuantas veces usted solicitó soporte técnico para solucionar problemas en su computador?**

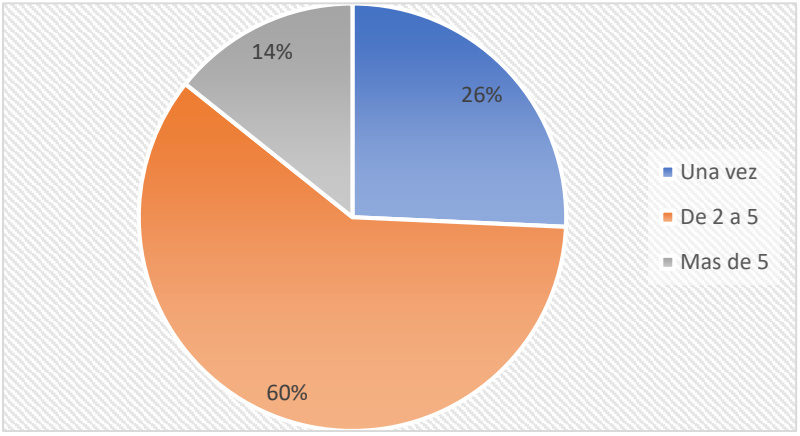


Figura 13. Pregunta 3

Análisis e interpretación. Según los datos que se obtuvieron en base a esta encuesta la mayoría de encuestados solicitan soporte técnico dentro de un mes, afirmando que el departamento ayuda a solucionar problemas cuando se requiere.

Pregunta 4**: ¿Cuáles son los principales problemas que ha tenido con su computador?**

Figura 14. Pregunta 4

Análisis e interpretación. Los resultados nos han dado a conocer que el mayor porcentaje de problemas en los equipos ha sido el funcionamiento lento del computador, lo mismo que puede provocar varios inconvenientes como el desempeño reducido, dentro de la parte de seguridad puede ser más propensa a los ataques de malware puesto que los virus y otros programas de carácter malicioso se pueden ejecutar de manera más rápida que el sistema operativo, es por ello que hay el riesgo de infectar la computadora antes de que el sistema operativo tenga la oportunidad de detenerlos, la PC se reinicia o apaga sola, ya no enciende el CPU, los paros de sistemas inesperados, el teclado no responde, no enciende, mal rendimiento de la batería, son otros inconvenientes que afectan a el rendimiento de las tareas, reduciendo la productividad, la probabilidad de que exista este tipo de problemas es muy alta ya que los equipos están expuestos a actividades constantemente.

Pregunta 5: **¿El departamento de sistemas en que lapso soluciona los problemas de su computador o fallas que se presenten en sistemas informáticos?**

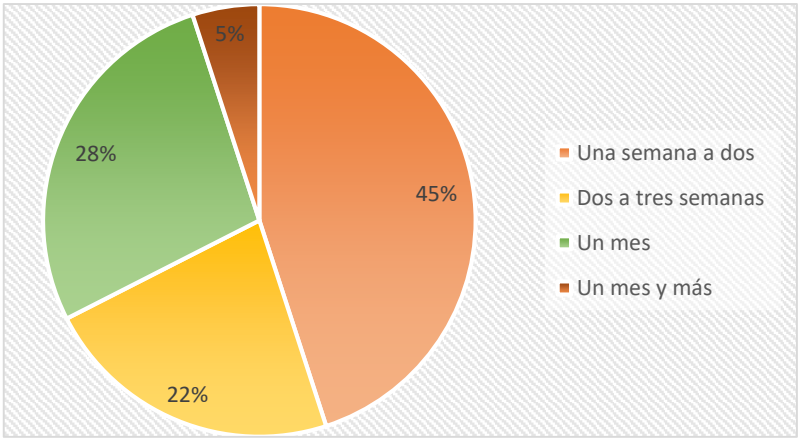


Figura 15. Pregunta 5

Análisis e interpretación. Según el resultado que se ha tenido en esta encuesta es que el departamento de sistemas soluciona problemas dentro de un mes, con un 95% de administrativos que lo confirman, podemos decir que su trabajo es eficiente, afirmando también que existe una prioridad de problemas, es por lo que algunos de los inconvenientes que existen tardan más tiempo en ser atendidos.

Pregunta 6: **En una escala del 1 al 5 califique la asesoría que brinda el personal de tecnología del municipio acerca de seguridad.**

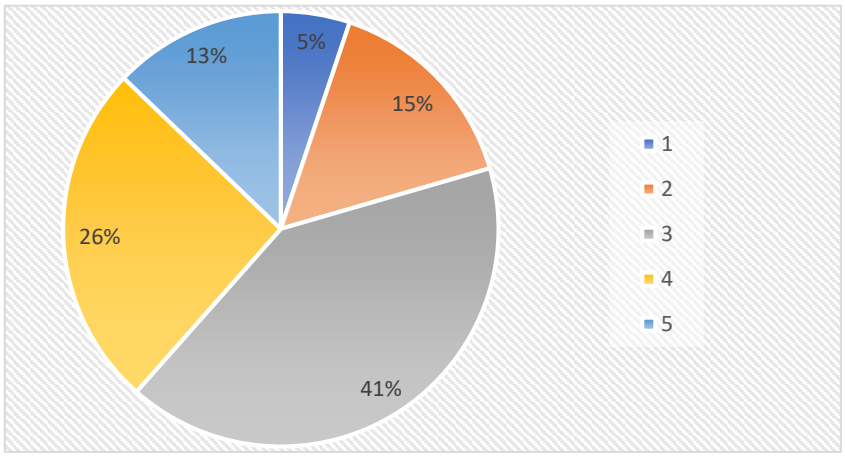


Figura 16. Pregunta 6

Análisis e interpretación. Como se puede apreciar un 61% del personal administrativo afirma un nivel bajo en asesoría de seguridad de la información puede demostrarse que si los administrativos que manejan información delicada no conocen cómo manejarla puede llevar a un acceso no autorizado a una de estas redes informáticas o a los equipos que en ella se encuentran ocasionando

en la gran mayoría de los casos graves problema, como es el robo de información sea esta sensible y confidencia, con una probabilidad muy alta ya que la pérdida de información confidencial daños y repercusiones que se relacionan con la confidencialidad, integridad y disponibilidad pueden ocasionar el cierre de una empresa, un 39% del personal tienen en cuenta medidas de seguridad.

Cuestionario de Auditoría correspondiente al desarrollo de proyectos

Pregunta 7: **¿Los sistemas son desarrollados de manera?**

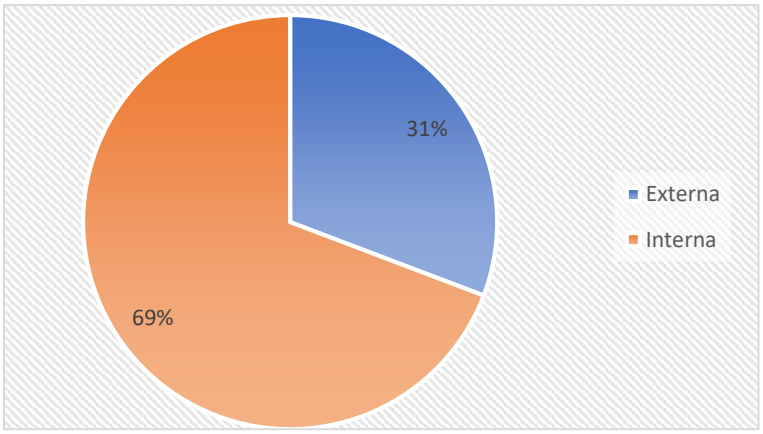


Figura 17. Pregunta 7

Análisis e interpretación. Según este análisis la mayoría de los sistemas informáticos se desarrollan de manera interna, dando a conocer que los sistemas que manejan han sido desarrollados por el departamento de sistemas, afirmando que realizan diseño, programación, implementación y pruebas de sistemas informáticos en los departamentos, un 31% afirma que existe un desarrollo externo trayendo contras como puede ser costes ocultos, falta de control del proyecto, aún más en la seguridad y cuestiones de confidencialidad de los datos.

Pregunta 8: **¿Considera que el área de sistemas cubre las necesidades para el manejo de redes, sistemas operativos, aplicaciones?**

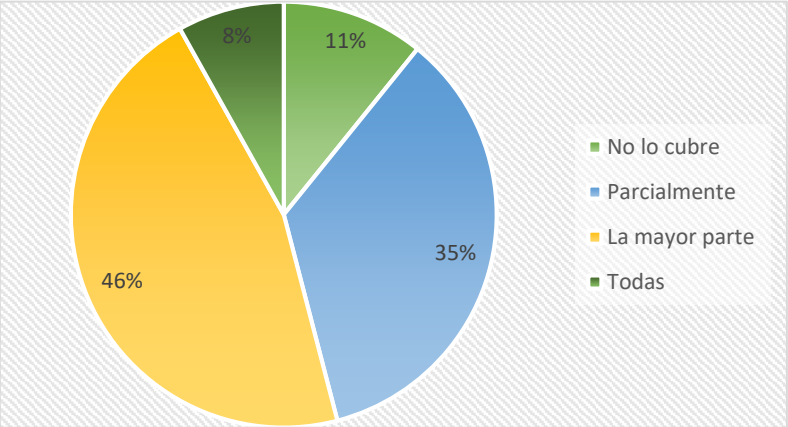


Figura 18. Pregunta 8

Análisis e interpretación. En los resultados obtenidos de esta pregunta se toma en cuenta que el departamento de sistema cumple con un 89% es decir que atiende la mayoría de las necesidades en lo que respecta a redes, sistemas operativos y aplicaciones, un 11% afirman que no lo cubre dando paso a consecuencias negativas como la conexión de internet deficiente, una mala distribución de la web, al igual que el no mantener los sistemas o aplicaciones en funcionamiento llevaría a riesgos altos de pérdida de información y manipulación inadecuada.

Pregunta 9: **¿Existen políticas para el manejo de redes, sistemas operativos, aplicaciones?**

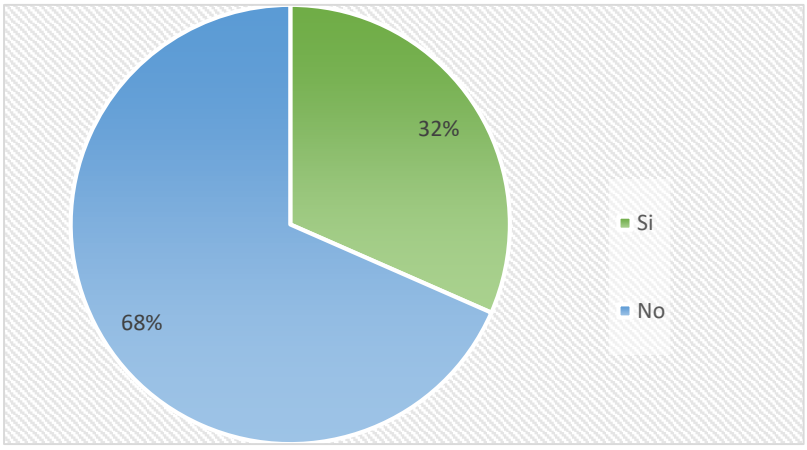


Figura 19. Pregunta 9

Análisis e interpretación. Se ha realizado dicha pregunta para conocer acerca de si se emplea políticas para el manejo de redes, sistemas operativos y aplicaciones, donde un 68% han afirmado que no existe ningún tipo de normas a seguir, conociendo que el impacto es muy alto ya que no se toma en cuenta la no revelación de información confidencial, y el resto afirma que sí, pero en su mayoría desconocen cuáles son.

Pregunta 10: **¿Dentro del departamento existe la disponibilidad de desarrollo de sistemas, aplicaciones que se realicen en un lapso establecido?**

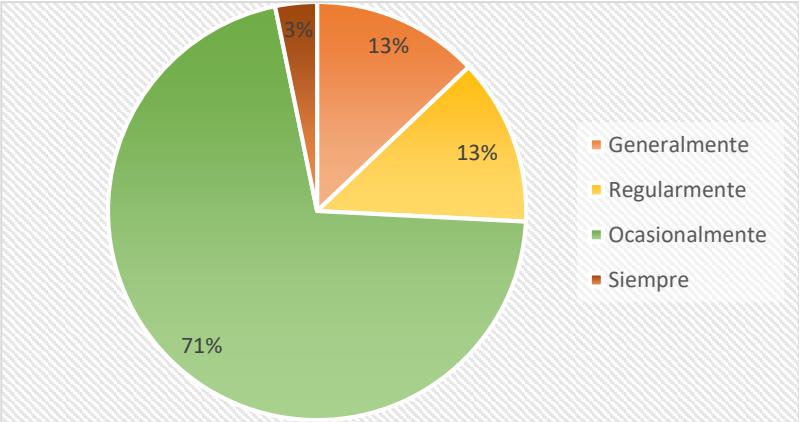


Figura 20. Pregunta 10

Análisis e interpretación. Un 100% de los encuestados han afirmado que existe la disponibilidad de desarrollo de sistemas y aplicaciones, el departamento de sistemas debe tomar en cuenta directrices o guías para controlar el proceso de diseño, desarrollo, implementación y actualización de los sistemas o aplicaciones, se debe de utilizar técnicas de programación seguras tanto para nuevo desarrollos, como la reutilización de código ya que si no existe este tipo de normas se tendrá una probabilidad de riesgo significativa para la integridad y disponibilidad de los sistemas.

Cuestionario de Auditoría correspondiente a seguridad de la información

Pregunta 11: **¿Usted ha recibido capacitaciones sobre políticas de seguridad?**

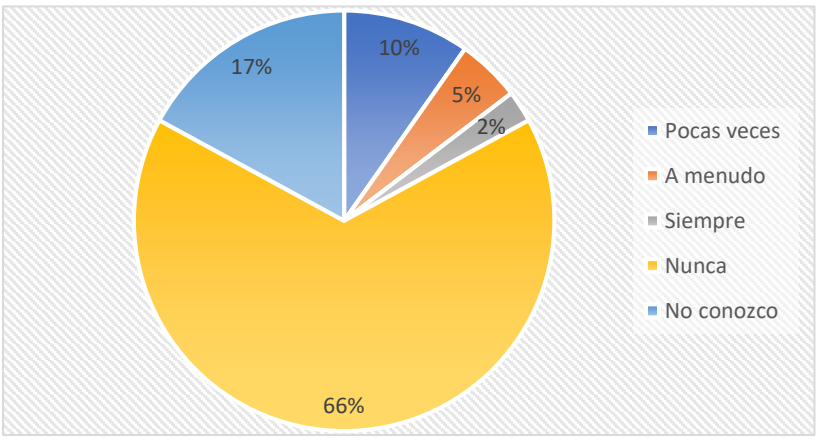


Figura 21. Pregunta 11

Análisis e interpretación. En cuanto a los resultados de esta pregunta, 83% de los encuestados afirman de manera mayoritaria que nunca se ha realizado capacitaciones sobre políticas de seguridad de información, por lo que se

desconoce cómo resguardar los datos y mantener la información segura, lo que trae impactos en la seguridad, activo asociados a la información y a los recursos de tratamiento de la información, el personal que ha venido trabajando desde periodos anteriores pueden confirmar que se capacitó, pero actualmente ya no se emplean las mismas formas de salvaguardar datos existe un probabilidad de violación de seguridad ya que son actividades que se exponen diariamente y se incumple con procesos disciplinarios.

Pregunta 12: **¿Conoce si los sistemas del municipio cuentan con políticas de seguridad que se encarguen de supervisar la manera en la que se manipula la información?**

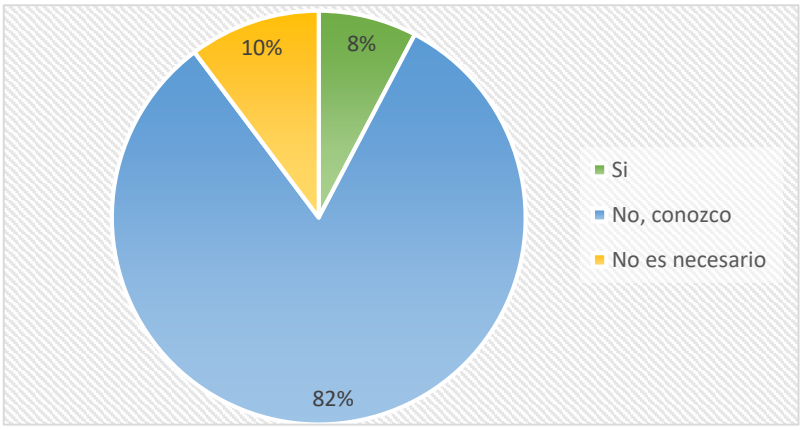


Figura 22. Pregunta 12

Análisis e interpretación. El personal no conoce si existe este tipo de políticas de seguridad que se encarga de supervisar la manera en que se manipulen los datos al momento de manejar un sistema, ya que conlleva a manipulaciones indebidas y accesos de personas que no están autorizadas, ciertas personas al afirman que no es necesario aplicar estas políticas pueden afirmar que no conocen los riesgos de monitoreo de seguridad, un porcentaje muy pequeño conoce acerca de estas políticas pero necesitan capacitaciones constantes para mejorar estos procedimientos, existe una probabilidad muy alta ya que puede haber riesgos de integridad.

Pregunta 13: **¿Se ha establecido procedimientos para la gestión de los medios de almacenamiento removibles de acuerdo con el valor de la información?**

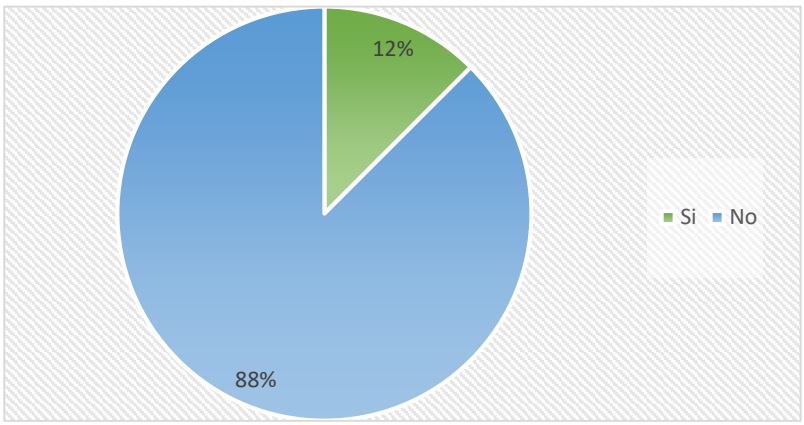


Figura 23. Pregunta 13

Análisis e interpretación. De acuerdo con los resultados se considera que se desconoce los procedimientos para gestión de medios de almacenamiento removible, ya que conlleva a un mal uso y corrupción de la información contenida, existe riesgos de revelación que puede causar incomodidad o poner en riesgo la supervivencia de la organización.

Pregunta 14: **¿Cada qué tiempo realiza el respaldo de la información?**

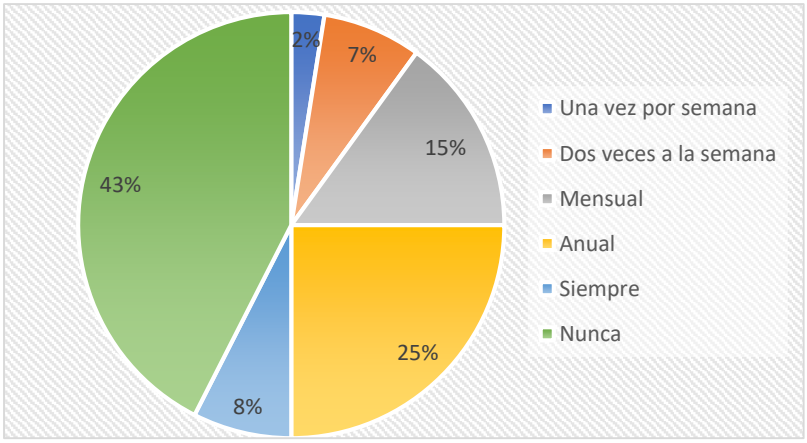


Figura 24. Pregunta 14

Análisis e interpretación. Según los datos de los encuestados se afirma que un total 32% mantienen procedimientos para realizar copias de respaldo y sobre todo asegurar que la información y software esenciales pueden ser nuevamente recuperados después de un desastre o fallos de soportes, existe un porcentaje muy alto de quienes nunca realizan respaldos de información los riesgos pueden ser tempranos y futuros ya que se los datos son atendidos diariamente.

Pregunta 15: **¿En qué dispositivos usted respalda la información?**

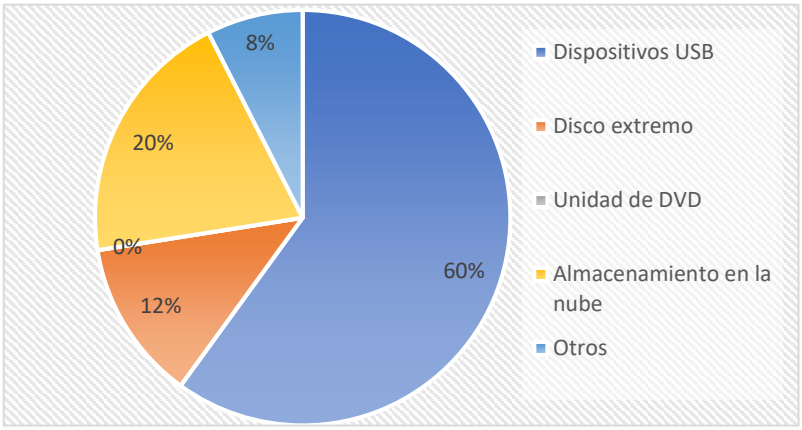


Figura 25. Pregunta 15

Análisis e interpretación. Un total de 80% realizan respaldos en dispositivos externos afirmando que la información puede ser expuesta a distintas amenazas como es virus y sustracción de archivos, un 20% realiza el almacenamiento en la nube, donde se puede tener un impacto de sobrecarga en los servidores o fallas de internet y no permitan el acceso a los datos requeridos, el riesgo es considerable ya que la pérdida de información podría derivar responsabilidades legales a quienes administran estos datos.

Pregunta 16: **¿El cambio de contraseña es?**

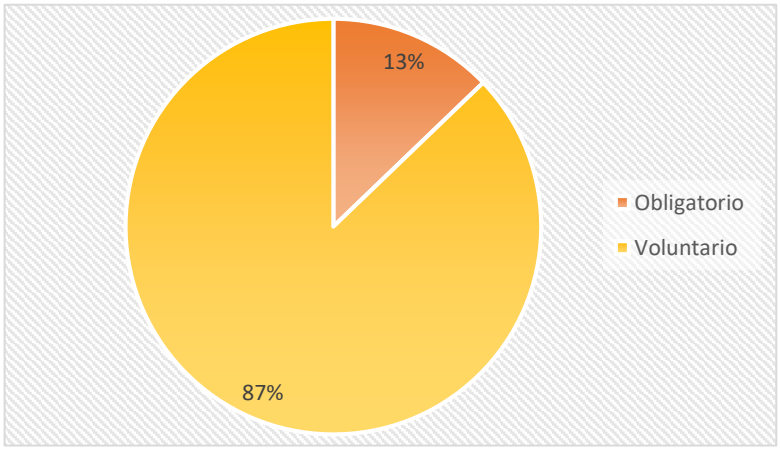


Figura 26. Pregunta 16

Análisis e interpretación. Según los resultados que se obtuvieron es que la mayoría de las personas realizan de manera voluntaria el cambio de contraseña en sus equipos y quienes no renuevan durante un tiempo se les informa actualizar su contraseña para mayor seguridad.

Pregunta 17: **¿Cada qué tiempo usted renueva las claves de seguridad en los equipos del municipio?**

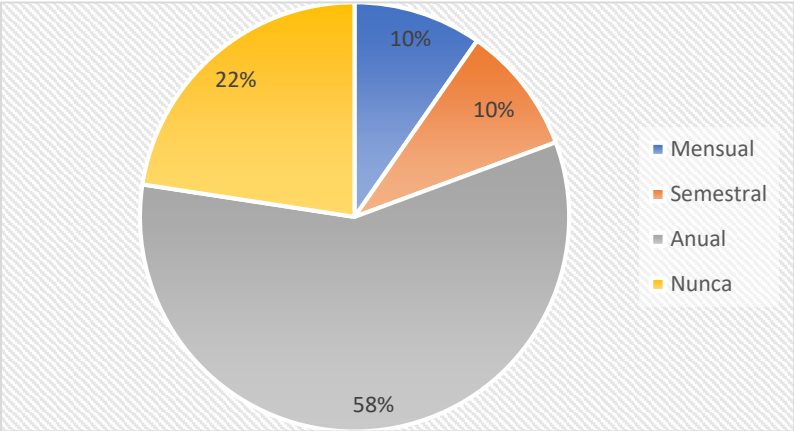


Figura 27. Pregunta 17

Análisis e interpretación. El cambio de contraseña para el 78% de administrativos está dentro de un año, evitando el ingreso de delincuentes, el 22% de personas no realizan cambios de contraseñas, esto provocará que una tercera persona que ha logrado descifrar pueda ingresar sin ningún inconveniente a cuentas o sistemas donde existe datos importantes, la probabilidad es alta.

Pregunta 18: **¿Existe alguna exigencia o control para el acceso a sitos webs permitidos, para el cumplimiento de sus funciones?**

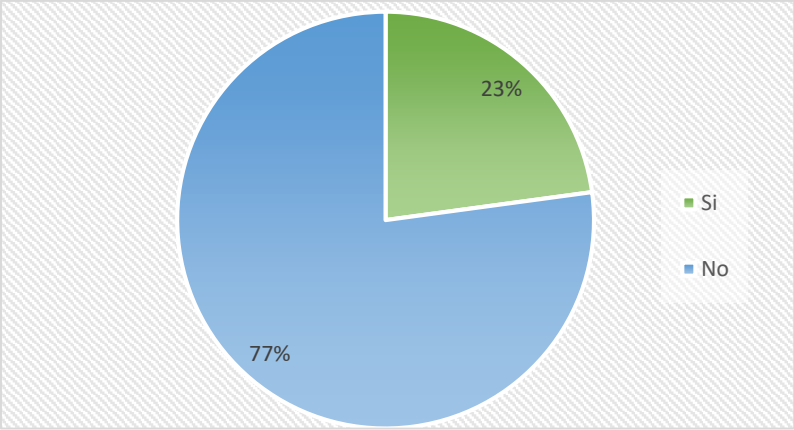


Figura 28. Pregunta 18

Análisis e interpretación. Según el resultado no existe ningún tipo de control que limite a el usuario a no acceder a sitios webs esto provoca que distracción y sobre todo al momento de ingresar a estos sitios existe problemas de ciberdelincuencia ya que son ellos que crean estos sitios web con la intención de simular ser legítimos y robar los

datos personales, contraseñas comprometiendo la seguridad de datos de la empresa y personal, en un mínimo porcentaje del personal le restringen este acceso, es por ello que la probabilidad de tener fallos en los equipos y vulnerabilidad de la información es considerable.

Pregunta 19: **¿Qué medidas de seguridad se encuentran disponibles para evitar que otros usuarios accedan a su computador?**

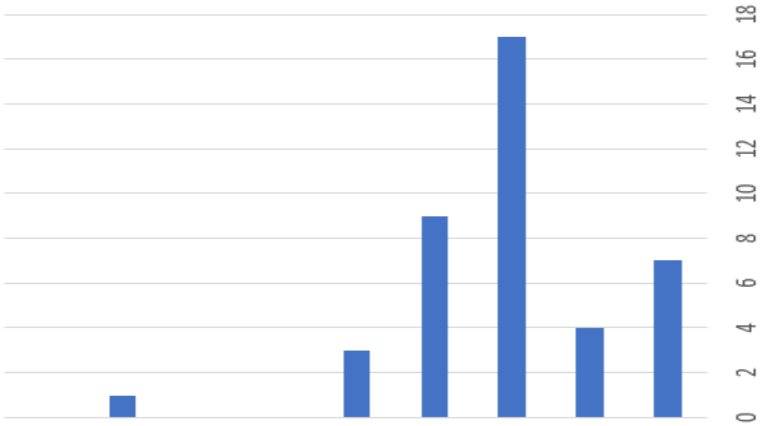


Figura 29. Pregunta 19

Análisis e interpretación. Según las estadísticas que se obtienen es que el uso de contraseñas seguras es un método de seguridad adecuado y más común ya que la mayoría de administrativo lo conocen, existe una gran falta de formación y conciencia sobre seguridad informática puede ocasionar grandes amenazas en activo de la institución.

Pregunta 20: **¿Cómo se da cuenta que otro usuario ha utilizado su equipo?**

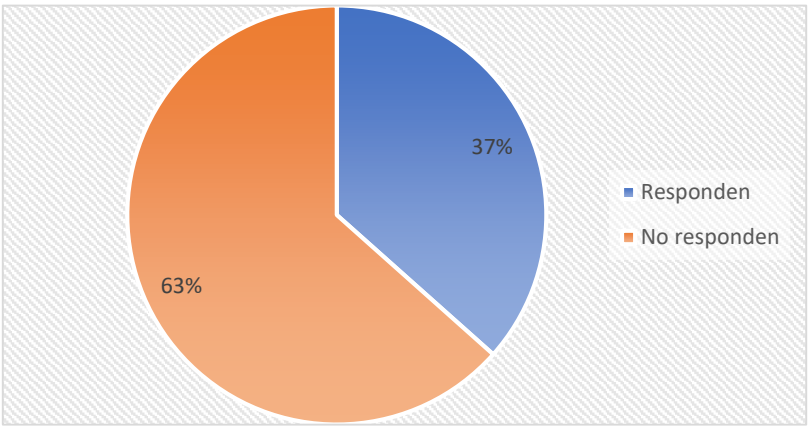


Figura 30. Pregunta 20

Análisis e interpretación. En cuanto a los resultados de esta pregunta la mayoría de los encuestados no responden a esta pregunta y se puede afirmar que no se dan cuenta o no saben cómo, un del personal da a conocer cómo se dan cuenta que

sus equipos han sido manipulados por terceras personas por ejemplo la inexistencia de datos, la información es otra, cuando dejan encendida la máquina, por la copia de seguridad, al momento de revisar el historial, al momento de ingresar dice la contraseña es incorrecta, pérdida de información, o el computador se encuentra bloqueado.

Pregunta 21: **¿Qué medidas de seguridad aplica?**

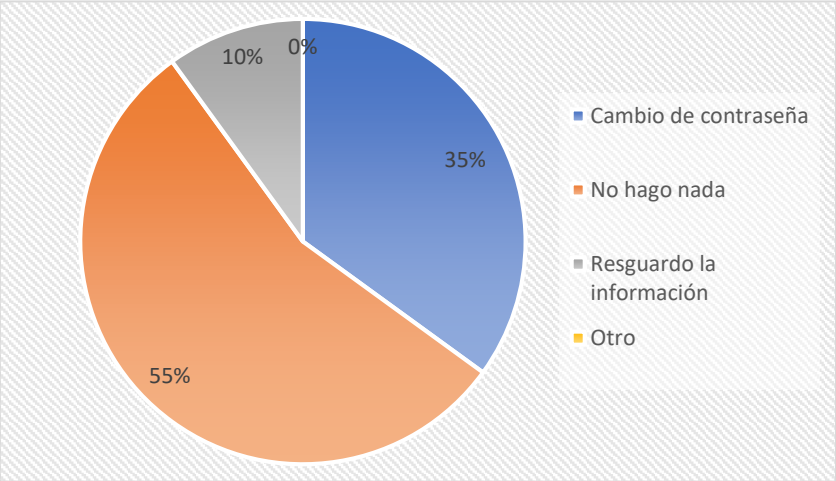


Figura 31. Pregunta 21

Análisis e interpretación. En base a la respuesta de esta pregunta se puede confirmar que mayormente las personas no hacen nada ya que no toman en cuenta cuando el equipo ha sido manipulado por otro usuario o simplemente dejan pasar por alto, un 45% cambian su contraseña y resguardan los datos de la mejor manera para evitar pérdidas de información esto provoca sensibilidad en los equipos y gestión inadecuada de la información la probabilidad es considerable ya que no se toma en cuenta políticas que ayuden con la protección de datos que la organización recopila y utiliza diariamente.

Pregunta 22: **¿Cuándo fue la última capacitación que recibió acerca del uso de dispositivos y sistemas informáticos?**

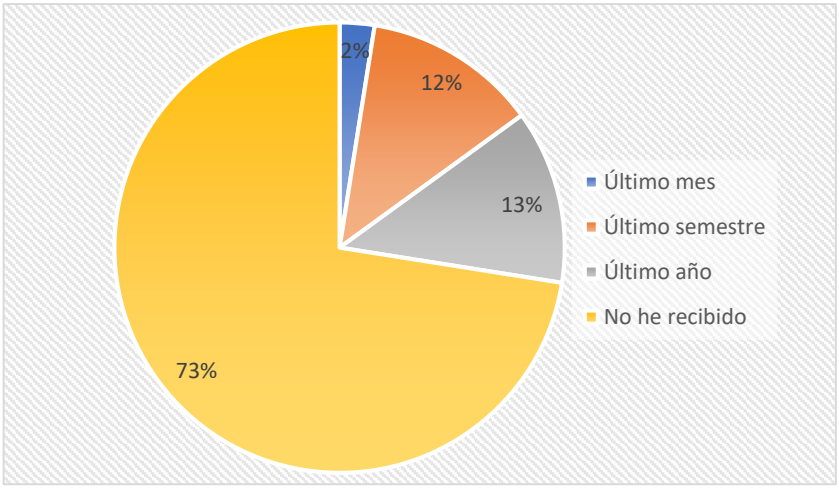


Figura 32. Pregunta 22

Análisis e interpretación. Al obtener los siguientes resultados podemos afirmar que no ha recibido capacitaciones sobre el uso de dispositivos y sistemas informáticos, el impacto mayormente afecta en la seguridad, ya que se puede tener el control de los equipos sin el consentimiento de la persona que lo maneja, generando una probabilidad muy alta de fugas de información, robo de credenciales.

Pregunta 23: **¿Qué temáticas de capacitación ha recibido últimamente?**

Figura 33. Pregunta 23

Análisis e interpretación. Los resultados muestran que no se ha recibido capacitaciones de la parte del departamento de sistemas de ninguna temática de manejo de seguridad de los datos, algunos temas como es el almacenamiento de información, han sido instruidos de manera rápida pero no en todos los

departamentos, al igual que wi-fi público, ofimática y seguridad informática, base de datos y seguridad en la nube, el no estar capacitado el personal de esta institución, los impactos dentro de la empresa sería en el perder el acceso total o parcial de la información, o al momento de dañarse los dispositivos, podría afectar a las finanzas de la institución, la probabilidad es muy alta ya que al no tenerse en cuenta estos riesgos, no solo afectan a datos personales, sino también a el ambiente laboral, generando así inconvenientes en la seguridad de la información de la institución.

Pregunta 24: **¿En caso de que el municipio restrinja el acceso a ciertos sitios web indique que categorías pertenece?**

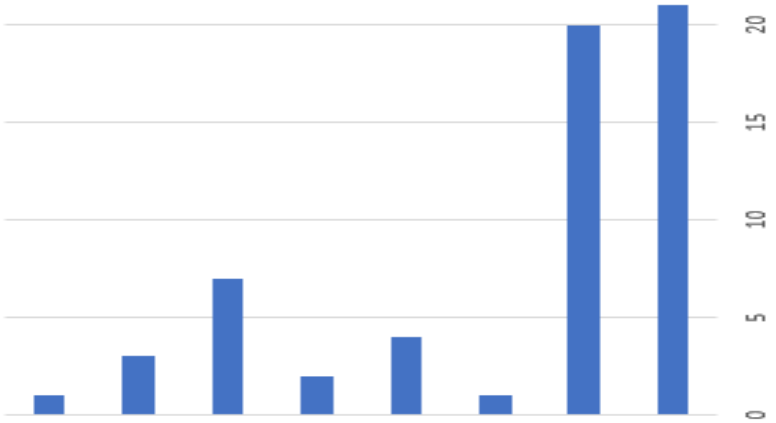


Figura 34. Pregunta 24

Análisis e interpretación. Las páginas que en su mayoría se restringen se han seleccionado como es redes sociales y páginas para adultos, sin embargo, hay escalas de restricción en lo que respecta a YouTube, algunos de los administrativos afirman que no se les restringe ningún tipo de páginas los impactos son negativos ya que puede existir una baja productividad y eficiencia en los administrativos además de tener un riesgo significativo de infección por virus de estos sitios otro inconveniente es el no tener internet perjudicando a la infraestructura de la empresa debido a cableado dañado, o por haber muchos dispositivos conectados, teniendo probabilidades altas.

Pregunta 25: **¿Existen políticas para el manejo de internet?**

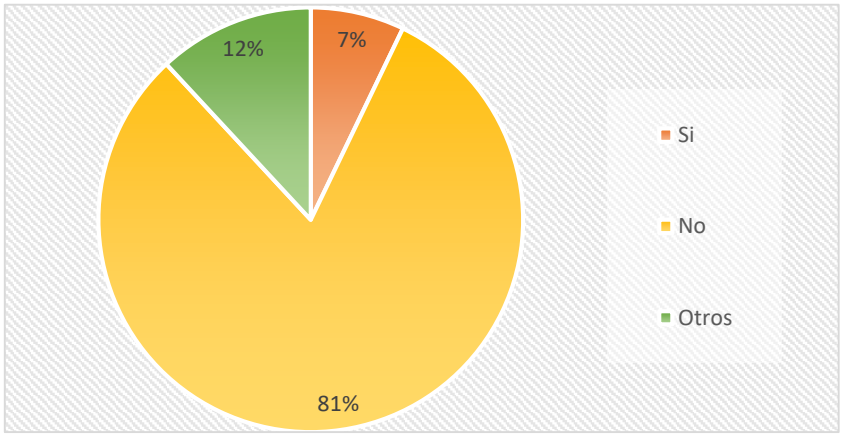


Figura 35. Pregunta 25

Análisis e interpretación. Al no existir ningún tipo de políticas para el manejo de internet en los departamentos existe un gran riesgo de ataques DDoS o sufrir ataques de malware, esto provoca gastos para recuperar y restaurar daños, o en peor de casos llevar a pérdida total de los datos y recursos.

Cuestionario de Auditoría correspondiente a infraestructura

Pregunta 26: **¿El lugar donde se ubica, cuenta con los equipos necesarios para realizar las actividades de manera más adecuada?**

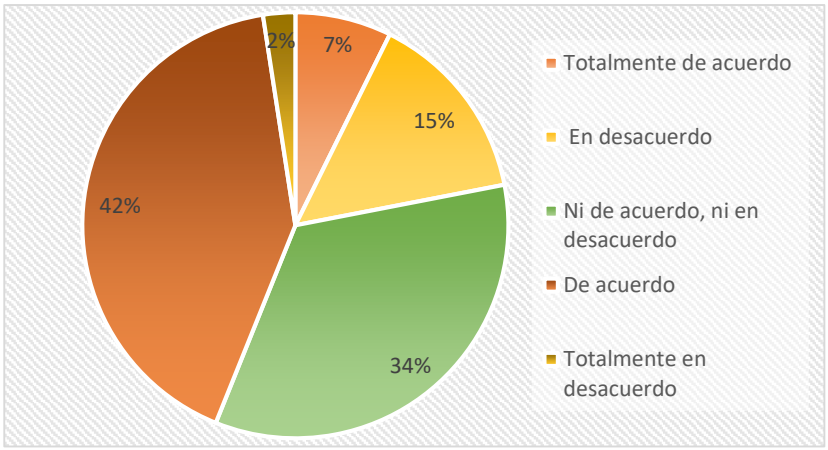


Figura 36. Pregunta 26

Análisis e interpretación. Parte de los administrativos dan a conocer que existe una incomodidad con respecto a la infraestructura causando pérdidas financieras, corrupción en la seguridad de la información teniendo un riesgo elevado en los recursos operacionales requeridos por la empresa.

Pregunta 27: **¿Está de acuerdo con la eficiencia de la señal de WIFI que usted tiene acceso?**

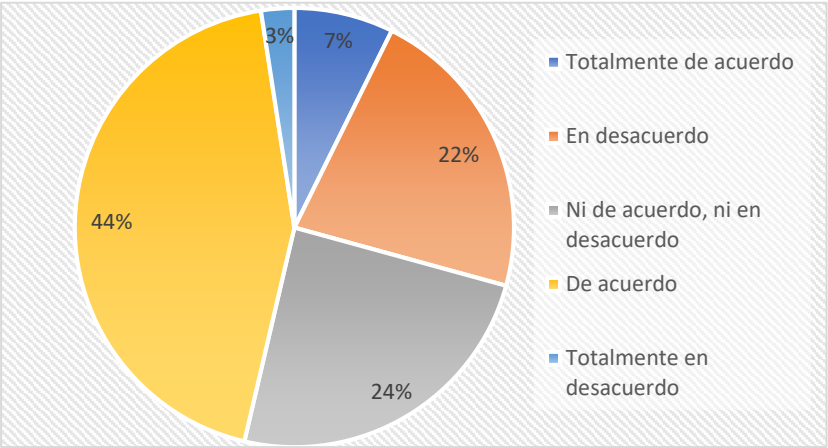


Figura 37. Pregunta 27

Análisis e interpretación. La mitad de los encuestados no están de acuerdo con la eficiencia de la señal de wi-fi teniendo un impacto medio ya que los datos pueden ser corrompidos en el proceso de trasladar datos a la web.

Pregunta 28: **¿Cómo recibe su internet a su puesto de trabajo?**

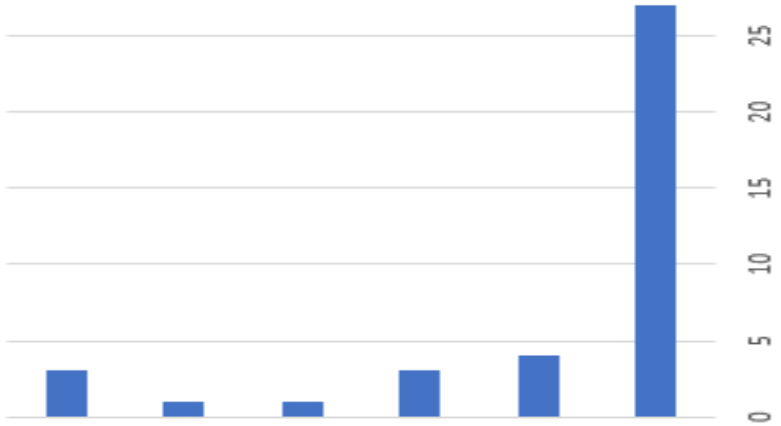


Figura 38. Pregunta 28

Análisis e interpretación. La mayoría de los encuestados afirman que el internet que reciben en sus puestos de trabajo es con cableado estructurado, lo cual provoca que la velocidad de transferencia sea estable asegurando la transferencia de datos dentro de la institución, aunque no existe como tal un control de puertos de acceso en este tipo de conexión.

Pregunta 29: **¿Qué pasa cuando se le daña el internet?**

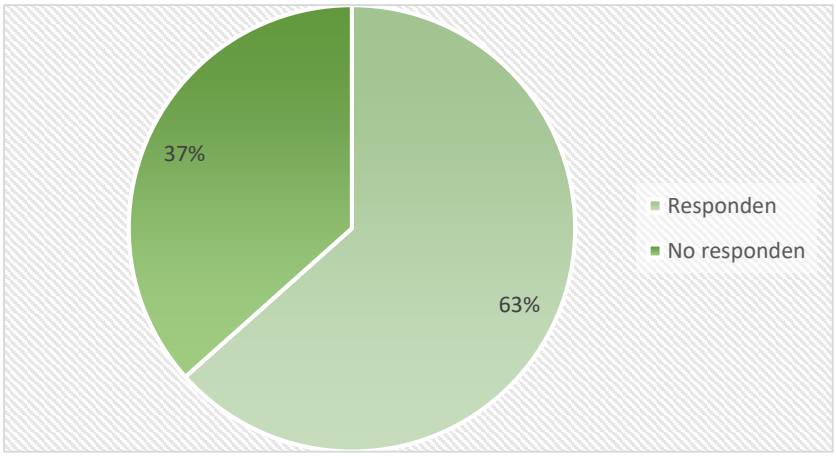


Figura 39. Pregunta 29

Análisis e interpretación. Según la pregunta que se realizó y tenían que responderla de manera textual un 63% del personal respondieron que informan a el departamento de sistemas que solucione este inconveniente, ya que no se puede trabajar y detiene los servicios administrativos, tomando en cuenta que un 37% no responde ya que desconoce lo que puede suceder o esperan a que se dé solución a este problema.

Pregunta 30: **Se ha realizado capacitaciones sobre infraestructura tecnológica sobre:**

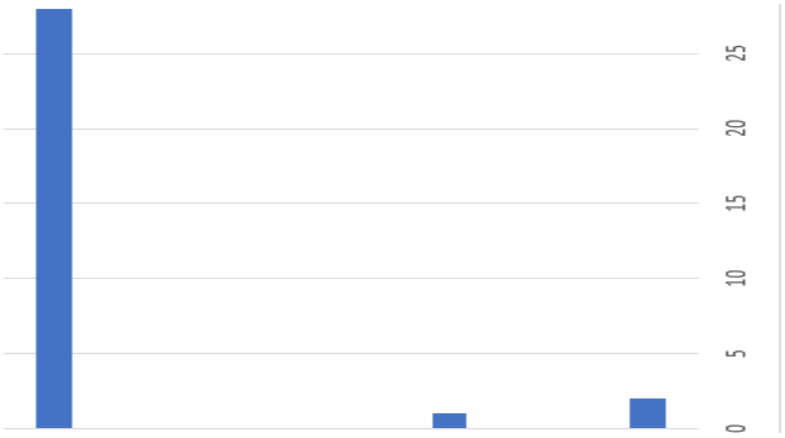


Figura 40. Pregunta 30

Análisis e interpretación. Se ha obtenido resultados que demuestran que se ha realizado capacitaciones sobre instalaciones y administración de hardware en anteriores periodos, pero no actualmente en el nuevo ingreso de administrativos, en la parte de otros, han afirmado que no se ha realizado capacitaciones y que desconocen acerca de los temas planteados, actualmente la institución no cuenta

con personal capacitado en el área de TIC o algún conocimiento básico que permita entender o solucionar problemas.

4.1.1.4 Hacer la guía de auditoría

Se realizó una entrevista que fue aplicada a el analista de sistemas informáticos. (Ver Anexo 2)

4.1.1.5 Consultar la información

De los documentos solicitados a el área de sistemas se resume de la siguiente manera:

1. Se solicitó a el jefe de sistemas que si se tienen los documentos.

El Ing. Clever Pozo señaló que de los documentos que están propuestos en el siguiente documento se encuentran:

Publicado:

- ✓ Políticas para la seguridad de la información
- ✓ Responsabilidades de gestión
- ✓ Inventario de activos
- ✓ Propiedad de los activos
- ✓ Uso aceptable de los activos
- ✓ Provisión de acceso de usuario
- ✓ Uso de la información secreta de autentificación

Socializado:

- ✓ Documentación de procedimiento de las operaciones

En desarrollo:

- ✓ Matriz sobre incidentes de seguridad de la información

Verificado:

- ✓ Políticas para la seguridad de la información
- ✓ Contacto con grupo de interés especial
- ✓ Políticas de dispositivos móviles
- ✓ Responsabilidades ante la finalización o cambio
- ✓ Políticas de control de acceso

No disponible

- ✓ Métodos de gestión de proyectos
- ✓ Proceso disciplinario
- ✓ Copias de seguridad de la información
- ✓ Registro de administración y operación

- ✓ Políticas de desarrollo seguro
- ✓ Procedimientos de control de cambios en el sistema
- ✓ Notificación de puntos débiles de la seguridad
- ✓ Implementar la continuidad de la seguridad de la información

No aplica

- ✓ Uso de la información secreta de autentificación
- ✓ Restricción en la instalación de software
- ✓ Políticas y procedimientos de intercambio de información
- ✓ Acuerdo de intercambio de información
- ✓ Acuerdos de confidencialidad o no revelación

Análisis: No se cumple con políticas o procedimientos para iniciar con el desarrollo de un proyecto, no cuentan con procesos disciplinarios que se debe tomar cuando existe algún fallo en la información, no se realiza copias de respaldo en un tiempo determinado y no se revisa al momento de sacar la información, no se tiene procedimientos de desarrollo de sistemas o aplicaciones y no consta con manuales de usuario, al igual que el control de cambio de software, si existe inconvenientes no se realiza notificaciones de manera urgente y no existe ningún plan de contingencia, estando expuesto el departamento de sistemas y la organización en general a riesgos de pérdidas económicas y de control en la organización, no existe acuerdos de intercambio de información y de confidencialidad o no revelación.

2. Se preguntó a el jefe de departamento si se lleva a cabo el desarrollo de proyectos informáticos como sistemas o aplicaciones por medio de teletrabajo.

El Ing. Clever Pozo informó que no existe este tipo de desarrollo ya que los sistemas que se requiere en la empresa son básicos y se desarrollan por pasantes que ingresan al área.

Análisis: Se puede verificar que no se emplea el teletrabajo, sin embargo se recomienda el desarrollo de sistemas o realizar actividades por medio del teletrabajo ya que brinda varias ventajas como es la optimización de los motores de búsqueda, el diseño y el desarrollo que se puede ajustar a las necesidades de la institución así como también la fácil administración de contenido, tener mayor control ya que supone mayor seguridad ante un ataque y vulnerabilidad en cuanto al acceso ayudando también al rendimiento.

3. Se preguntó si al momento de ingresar a el área de desarrollo ellos revisan el currículo o antecedentes de quien ingresa a su departamento.

Manifestó que no existe ningún tipo de control de su parte que esas funciones se realizan directamente del departamento de gestión administrativa y talento humano.

Análisis: Se toma en cuenta que el departamento de sistemas no verifica este tipo de procesos y si se realiza dentro de la institución, pero en el área de talento humano

4. Al preguntarle acerca de si las personas que intervienen en el desarrollo firman un acuerdo de no revelación de la información sensible.

Supo afirmar que no existe este tipo de documentación ya que es una empresa que desarrolla ocasionalmente y si realizan esta actividad es de sistemas pequeños.

Análisis: Si el departamento no cuenta con documentación que asegure que la información no será revelada traerá riegos en la confidencialidad, protección de datos, en la ética, uso adecuado de los equipos y recursos de la organización, así como incumpliendo prácticas profesionales.

5. En referencia a cuál es el mecanismo que motiva a el departamento a mantener los datos seguros.

Afirmó que no existe ninguna motivación para salvaguardar los datos de la institución lo que ellos tratan es de cumplir con las responsabilidades de acuerdo con normas de control interno SGCI.

Análisis: Dentro de la organización no se cuenta con normativas que eviten revelar información existe un riesgo de descuido en los datos o como también el mal uso de los activos dentro de la organización.

6. Se peguntó si realizan capacitaciones al personal sobre seguridad de la información.

Se afirmó que nunca se realizó ninguna capacitación de este tipo que cada uno de los administrativos salvaguarda los datos de la manera en que ellos vean correcto.

Análisis: Se debería realizar capacitaciones que permiten cumplir una normativa de seguridad ayudando a los administradores a manejar la información de mejor manera es muy importante capacitar al personal de una empresa ya que pueden ayudar a evitar que cualquier atacante pueda llegar hasta la información, el realizar esta capacitación permite ahorrar dinero e incrementar la productividad, ayuda a reducir errores que cometen los empleados y refuerza la confianza a los empleados.

7. En base a la anterior pregunta era necesario conocer acerca de cuándo fue la última capacitación y si se realiza a toda la empresa o a cierto grupo de administrativos.

Afirmo que nunca se realizó esta capacitación de ningún tema respecto a seguridad.

Análisis: No se realizan capacitaciones en este departamento provocando un riesgo laboral en responsabilidad y desarrollo de su trabajo, mala imagen, ya que no se cumplen con normas de seguridad, presión en los administrativos debido a que existirá un cargo en el trabajo, por otro lado, el personal deberá realizar actividades en menos tiempo, lo que obliga a minimizar la calidad en el trabajo, dando paso a la burocracia ya que se empleara mucho tiempo y esfuerzo en la elaboración de documentos.

8. Se preguntó que si existe un proceso disciplinario si existe perdida de datos en el departamento.

No existe un proceso disciplinario en el departamento, sin embargo, si existe perdida de datos ellos tratan lo más rápido posible recuperarlos.

Análisis: En el departamento de sistemas y la organización en general no existe un proceso disciplinario a pesar de que en la norma 410 de la contraloría general del estado afirma tomar accione si existe pérdida de información, se recomienda tomar en cuenta esta política ya que puede evitar impactos mayores como es la pérdida de datos, el no implementar estas políticas lleva a una violación de procedimientos de seguridad, la probabilidad de riesgo es alta ya que lo datos pueden ser revelados en cualquier momento y si existe un inconveniente se requerirá de acciones inmediatas.

9. Se pregunta si la persona quien estaba encargada de desarrollo finalizo su contratación y expuso información privada cual es el procedimiento que toma el departamento de sistemas

Afirmó que se procede a el cambio de contraseña de los sistemas que se manejaba en el departamento y con ello quitándole el acceso a información privada de esta institución.

Análisis: Se puede afirmar que existe procedimientos que impiden el acceso, sin embargo las instituciones deben de tener en cuenta procesos seguros para el ingreso a sistemas de información de la institución y procedimientos que ayuden con controles criptográficos garantizando la integridad, disponibilidad y confidencialidad de datos, debe de existir procedimientos de gestión donde se tome en cuenta el almacenamiento seguro de llaves, actualización o cambio de contraseñas tanto como revocación y recuperación de llaves.

10. Se consultó si existen hojas de resguardo de quipos informáticos.

Afirmo que no existe ningún tipo de documentación de propiedad o historial de los activos informáticos del departamento.

Análisis: Normalmente se debe implementar procesos para asegurar la asignación de activos, el conocer acerca de esta norma ayudará a asegurar los activos del departamento de sistemas, y la persona que se encuentre encargado de estos activos realice una revisión periódica de restricción de acceso asegurando la eliminación y destrucción de este.

11. De acuerdo con la pregunta realizada sobre si se tiene implementado reglas de uso aceptable de la información.

Se dio a conocer que se tiene implementado normas en lo que respecta a el desarrollo manual de uso de equipos.

Análisis: La respuesta del encargado se afirma que existe normativas, pero en la revisión no existe documentación, sin embargo, es necesario tenerlo ya que sirve para gestión y clasificación de datos, se considera como una no conformidad dentro de esta institución.

12. Se ha preguntado acerca de que si se tiene un proceso de desvinculación la cual incluya equipos informáticos o información relevante que sean custodiados por el departamento.

Afirmó que con respecto a la información le impide todo tipo de permisos y el retiro de activos lo realiza del departamento de guardalmacén.

Análisis: Existe un procedimiento para quitar activos, pero no existe documentación, es por ello que se lo toma como una no conformidad, se debe de tomar en cuenta la devolución de activos ya que los empleados que se retiren de sus cargos deben devolver lo activos del departamento, donde los empleados de una institución deben de haber firmado un compromiso para el respaldo de información la cual debe de ser protegida incluyendo controles de acceso, autentificación tanto como la encriptación.

13. Se solicitó que se seleccione en qué grado se encuentra la siguiente información ya sea pública, privada, confidencial y restringida.

Análisis: La información no se encuentra clasificada de la mejor manera ya que cierta información que es privada los usuarios pueden acceder sin ningún inconveniente.

14. Se preguntó acerca de cómo se encuentra estructurada la base de datos de los usuarios de la institución.

Afirmó que la clasificación de esta base de datos es confidencial y la estructura del sistema de gestión que ellos manejan se conforma por género, departamento, cédula, nombres y apellidos.

Análisis: El procedimiento de etiquetado de información es un requisito clave ya que la información que se encuentra etiquetada al momento de sufrir vulnerabilidad será más fácil identificar la información robada ya sea por miembros internos o externos.

15. Se preguntó quiénes son responsables de este sistema y etiquetado de información.

Afirmo que plenamente el departamento de sistemas en este caso el analista de sistemas y el asistente de dicha área.

Análisis: Se debería implementar un conjunto de normativas que se debe tomar en cuenta para la manipulación de la información, se debe redactar el manejo, tratamiento, almacenamiento y comunicación de cómo es la restricción de acceso, protección de copias y el almacenamiento de los datos.

16. Según la norma 27002 se tiene en cuenta directrices para la gestión de soportes extraíbles, las mimas que deberían ser señaladas si se cumplen o no.

Se pudo evidenciar que no se emplean técnicas de criptografía que protejan los datos en soportes extraíbles, además no se emplea la directriz de transferencia de datos a soportes antes de que sean ilegibles, ayudando a mitigar los riesgos de degradación durante el tiempo en que los datos aun no son necesarios.

Análisis: Se debería implementar procedimientos que ayuden con técnicas de criptografía de datos en soportes extraíbles como también en la realización de copias múltiples para reducir el riesgo de daños o perdida simultanea de estos.

17. Se preguntó si existe procedimientos para la eliminación de soportes informáticos.

El Ing. Clever Pozo afirmó que no existe ningún tipo de procedimientos de eliminación de dispositivos de almacenamiento.

Análisis: Para la eliminación de soportes debería establecerse ciertos procedimientos ayuden a minimizar riesgos de filtración de información ya sea personal o confidencial la probabilidad es alta por lo que esto elementos se encuentran almacenando información continuamente.

18. Según la pregunta que se realizó si enviaban información en soportes extraíbles fuera de la institución.

Quien manifestó que, si envían información, pero no existe ningún tipo de seguridad de esta información.

Análisis: Es importante tomar en cuenta la seguridad de soportes extraíbles ya que permite proteger el acceso no autorizado usos indebidos o deterior, existen riesgos de mal uso y corrupción durante el transporte, sobre todo si se lleva información, confidencial y no está cifrada es allí donde se debe tomar medidas de protección física adicional.

19. De acuerdo con esta pregunta se preguntó si el departamento cuenta con procedimientos de autorización que determine quién puede acceder a redes y a que servicios.

Se afirmó que no existe ningún tipo de procedimientos o documentación que trate de protección de redes, sin embargo, al momento de que un usuario ingrese a el departamento de sistemas existe contraseña solo para la red de esa área.

Análisis: Se recomienda emplear políticas para el acceso a redes y contar con una monitorización de estos servicios el impacto de redes no autorizados o inseguras afectar a la organización en la conexión de red a las aplicaciones más sensibles la probabilidad es alta ya que afecta a usuarios que se encuentran manejando información en áreas públicas o externas que se encuentran fuera de control de seguridad de la información.

20. De acuerdo con la pregunta sobre si existe procedimientos donde se da de baja a los usuarios.

Afirmó que no existe ningún tipo de procedimientos que permitan la baja de usuarios.

Análisis: Debería implantarse procedimientos que permitan el registro de retirada de usuarios logrando una asignación de derechos de acceso o asegurando que no se identifique, sobre todo que el usuario que ya se retiró de la base no pueda acceder a la información y se evitara una revelación de datos.

21. Se preguntó si existe una matriz de usuarios donde permita verificar que accesos y que privilegios tiene un usuario.

La respuesta a esta pregunta fue que si se tiene este informe ya que permite construir pautas que ayudan a limitar el acceso a datos de confidencialidad.

Análisis: No existe evidencia que respalde este tipo de información es muy importante conocer acerca de gestión y configuración de cada uno de los usuarios del sistema ya que depende de este registro, la ejecución de tareas y la seguridad de los datos evitando ser vulnerados y expuestos por lo tanto se le denomina una no conformidad.

22. Se preguntó acerca del mecanismo para restablecer una contraseña.

Lo que se responde es que se debe solicitar a el departamento de sistemas para ellos poder realizar este proceso.

Análisis: Se conoce que el departamento no cuenta con procesos de restablecimiento de contraseña, existe este tipo de inconvenientes en la institución, se trata de un riesgo de la información sea compartida, perdida de información y problemas relacionados con el acceso, las amenaza pueden ser por parte del personal administrativo de la misma organización con accesos legitimados se conoce como una no conformidad.

23. Se preguntó si se ha implementado un sistema quien puede acceder de manera privilegiada.

Quien afirmó que el departamento de TIC´S es el único que tiene acceso.

Análisis: Se toma en cuenta que varios sistemas están en su cargo, sin embargo, si existe fallos en varios sistemas a la vez puede haber ineficiencia de gestión de los datos, la productividad de los trabajadores será desperdiciada, al momento de presentar problemas con un flujo de datos, no se podrá satisfacer a los usuarios con las actividades que lo requieran.

24. De acuerdo con la pregunta de qué tiempo renueva las claves de seguridad en los equipos.

Afirmo que desconoce en qué tiempo es adecuado cambiar contraseña y personalmente el cambio de contraseña lo realiza cada año.

Análisis: Se debería cumplir con ciertas políticas que sigan prácticas en el uso de la información secreta de autenticación, normas que permitan, advertir a los usuarios sobre tiempo de cambio de contraseña que puede ser evitando riesgo de revelación de información recomendable secreta de autentificación.

25. Según la pregunta de si al momento de desarrollar se toma en cuenta el menú de acceso que permita el acceso a los usuarios.

Afirmó que si se toma en cuenta ya que es la mejor manera de visibilizar quien tiene acceso a las plataformas.

Análisis: Se debe tomar en cuenta no guardar las contraseñas dentro de nuestro equipo o nuestro correo electrónico ya que existen muchos usuarios que no cifran las listas de contraseñas quedando desprotegidas, el riesgo es considerable ya que si un

atacante ingresa a un computador podría obtener de manera muy fácil las contraseñas y poder descifrarlas y robar información.

26. Se preguntó si en el momento de desarrollar un sistema o aplicación se toma en cuenta procedimientos seguros de inicio de sesión de los usuarios.

En la cual se afirma que si ya que depende de un acceso por identificación de nombre y contraseña.

Análisis: No existe procesos que aseguren que se cumple con esta normativa como es identificación, autentificación y la autorización de acceso a los sistemas es por ello que se toma en cuenta como una no conformidad dentro de la organización.

27. Se preguntó que el cambio de contraseña se lo realiza de manera obligatoria o voluntaria.

Se afirma que es de manera obligatoria pero no se realiza frecuentemente este cambio.

Análisis: Se debería implementar una política donde se imponga contraseñas seguras y robustas permitiendo a los usuarios escogerlos y cambiarlas se debería tomar en cuenta los cambios regulares de contraseña bajo petición.

28. Se pidió información sobre si existe documentación sobre el ingreso a programas.

Quien afirmó que no existe ningún tipo de procedimiento ya que los sistemas que ellos manejan los realizan sin ningún tipo de manual.

Análisis: La implementación de directrices para el uso de programas que ayuden a la segregación, autorización y limitación de usuario es importante ya que permitirá reducir impactos como acceso de personas y evitar un colapso en el servidor.

29. Según la pregunta de si todo tipo de código se encuentra estrictamente controlado.

Se afirmó que no existe ningún tipo de control que permita la seguridad de los códigos fuente.

Análisis: Es recomendable restringir el acceso al código fuente de los programas que se realizan en el municipio el personal de informática debería tomar en cuenta la actualización.

30. En base a la pregunta de si quien desarrolla emplea algún método criptográfico durante la etapa de desarrollo.

Manifestó que al momento de desarrollo no existe un control criptográfico.

Análisis: Se debería implementar políticas que ayuden a proteger la información tomando en cuenta el uso de controles criptográficos para base de datos protegiendo su confidencial, integridad, no repudio y la autenticación, si no se emplea controles de este tipo la institución estará expuesta a software maliciosos como (malware), el uso de técnicas ayuda a cumplir regulaciones y restricciones nacionales.

31. En referencia a si existe claves para resguardar sistemas y aplicaciones.

El jefe de esta área manifestó que no existe ningún tipo de claves.

Análisis: Sería recomendable implementar políticas para el uso, protección y tiempo de duración de claves de cifrado ya que protegerá contra la modificación, la perdida y la contribución de datos, para reducir la posibilidad de mal uso a las claves se debería tomar en cuenta técnicas basadas en fechas de activación y desactivación de las claves, de formas que solo se puedan usar durante un tiempo definido.

32. Es importante conocer si al momento de desarrollar un sistema quine únicamente tiene acceso.

El departamento de sistemas supo manifestar que solo ellos pueden acceder a dicho monitoreo de código fuente.

Análisis: Para mantener el código fuente protegido se debe conocer sobre algunas maneras de resguardar esta información como es el utilizar el principio de privilegio mínimo ya que es un repositorio que nos ayuda a controlar estrictamente para que solamente las personas que están autorizadas puedan acceder a este según sea necesario, otro de las formas es limitar el acceso del administrador la cual se basa en no dar a todos los desarrolladores el acceso como administrador a la configuración de este código, el realizar revisiones de código, limitar las credenciales de combinación, evitar la proliferación de los repositorio de código.

33. Se quiere conocer si al momento de desarrollar existe una base de datos independiente a la que se maneja actualmente.

Afirmaron que sí, ya que le ayuda a la modificación de su aplicativo.

Análisis: Al momento de realizar estas actividades de probar un sistema con una base de datos de prueba debe tomarse en cuenta que el mantenimiento puede ser más costoso debido a que la base de datos crece a un gran tamaño durante el tiempo que se encuentre un sistema en desarrollo ya que podría existir riesgos de perdida de información de toso ese tiempo que se mantuvo en progreso.

34. Se les pregunto si se encuentra implementado controles preventivos y recuperación que sirvan como protección de código malicioso.

Se afirmó que no existe ningún tipo de control que permita la protección de código malicioso.

Análisis: Es necesario tomar en consideración controles de detección y recuperación que sirvan como protección para código malicioso y procedimientos para los usuarios sobre concienciación en la seguridad.

35. Se indicó señalar si se realiza copias de seguridad.

Se señaló que se realizan respaldos de la base de datos cada semana, que este respaldo se realiza fuera del servidor y que esta información permanece cifrada, se evita proteger la información con contraseñas que estén en documentación física y sobre todo mental, pero sin embargo una vez realizado el respaldo no se comprueba si la información se encuentra almacenada completamente.

Análisis: Se debería implementar políticas que normalicen el realizar copias de seguridad en un determinado tiempo las copias de seguridad en un determinado tiempo las copias de seguridad deben tener un nivel adecuado que permita proteger sus datos.

36. Se preguntó acerca de si se realiza un registro, protección y revisión periódica de actividades de usuario durante el proceso de desarrollo.

Afirmó que si se realiza este proceso de revisión periódica de estas actividades durante el proceso de desarrollo.

Análisis: Se debería implementar controles de detección, prevención y sobre todo la recuperación que sirva como una protección contra el código malicioso, la protección que brinda la organización deberá estar basada en un software de detección de código malicioso donde se considere las directrices como es la implantación de políticas que protejan de riesgos asociados.

37. Se preguntó de cuanto es la capacidad de almacenamiento de los ficheros de registro.

Se afirmó que es suficiente y se encuentra al redero de 200G.

Análisis: Se deberá tomar en cuenta la administración de los datos considerando los datos valiosos de la organización, cumpliendo con las regulaciones de control de datos, además la administración de calidad donde los usuarios tengan sus datos

suficientemente fiables, tomando en cuenta la seguridad de los datos, distribución y coherencia de los datos.

38. De acuerdo con la pregunta de si se encuentran sincronizados los relojes.

Se confirmó que es necesario tenerlo ya que les ayuda a llevar su horario.

Análisis: Es importante documentar como uno de los requisitos dentro del área de sistemas como en la organización en general ya que es importante garantizar la precisión de registros, debe considerarse también que el usar relojes sincronizados ayuda a los servidores a realizar sus actividades de manera continua y sin presentar ningún tipo de inconveniente.

39. Se preguntó si existe una plataforma de auditoria la cual permita informar el funcionamiento adecuado de los sistemas.

Se supo manifestar que no existe ninguna plataforma que permita informar a los administrativos guiarse al momento de no conocer el funcionamiento de los programas.

Análisis: Es recomendable implementar una planificación de auditoria para los sistemas de información evitara riesgos a los sistemas de información ayudara a verificar si como en la cláusula 410-15 capacitación informática de la contraloría general del estado.

40. Se preguntó que si se establece controles especiales para salvaguardar la confidencialidad e integridad de datos.

Se confirmó que no existe ningún tipo de controles que permite salvaguardar los datos.

Análisis: Es necesario implementar po9liticas sobre controles para garantizar la seguridad de la información en los datos estos controles deberán establecerse para salvaguardar los datos la confidencialidad y la integridad con una probabilidad de vulnerabilidad en los datos ya que se encuentran de manera pública.

41. Se preguntó que si se modifica los sistemas operativos y aplicativos.

Se afirmó que si existe este tipo de modificaciones ya que permitirán garantizar afectos adversos.

Análisis: El modificar código debe de llevar un proceso el cual no se encuentra documentado es importante tomar en cuenta que el robo de código fuente cada vez es más frecuente es por ello que la información debe de tener seguridad ya que un atacante pude acceder a este mediante creación de exploits que se denomina como un código esqueleto de un software dando la posibilidad de examinar todo el

código encontrando puntos más vulnerables, la extorción es otro inconveniente que sufre el código fuente ya que puede ser creado por otra persona haciendo que sea más fácil leer la información.

42. Se preguntó cuál es el proceso de desarrollo de aplicativos y sistemas.

Afirmó que no se desarrolla programas complejos, que alumnos pasantes desarrollan programas básicos, pero no existe ningún tipo de procedimientos.

Análisis: Considerar procedimientos para el desarrollo de sistemas y aplicativo favorecerá y equilibrará necesidades de seguridad de información con respecto al diseño y sobre todo a su accesibilidad proyectará al momento de autentificación de usuarios, el control de sección segura y se deberá tomar en cuenta procedimientos para validación y depuración de datos y eliminación de códigos depurados.

43. Se quiere conocer qué tipo de reglas de desarrollo seguro se tiene presente.

Esta pregunta no fue respondida.

Análisis: Se asume que no se tiene estandarizado los tipos de reglas de desarrollo seguro, debería establecerse políticas, procedimientos y controles que ayuden a proteger los datos, tomando en cuenta requisitos de seguridad de la información.

Para un desarrollo de software seguro se debe tomar en cuenta los siguientes lineamientos:

- Se debe utilizar técnicas de programación que ayuden con la seguridad de información de igual manera si se reutiliza códigos.
- Se deberá conocer acerca de los criterios de seguridad y calidad que se debe considerar, durante las fases del desarrollo de los sistemas.
- Al momento de iniciar con el desarrollo de un software debe de firmar contratos donde se comprometa a asegurar los datos y mantenga la confidencialidad e integridad de los mismos.

44. De acuerdo con la pregunta de si se realiza pruebas de aceptación del sistema.

Afirmó que si existe pruebas de este tipo ya que se verifica su funcionamiento para el empleo en los departamentos que lo requieran.

Análisis: No existe un documento que lo respalde, donde describa los procesos para evaluar que un sistema se encuentre funcional para emplearlo en la organización, se debería establecer y aplicar reglas donde se considere seguridad durante la fase de diseño y las capacidades de reparar algún tipo de vulnerabilidad si este provoca algún tipo de falla.

45. Se preguntó si existe seguridad en la fuga de información a quien se le informaría.

Se afirmó que no existe ningún plan que ayude con la fuga de información.

Análisis: Aplicar procedimientos de responsabilidad favorece a el área y a la institución en general evitando riesgos de quebrantamiento de seguridad se debería establecer normas que aseguren actividades de gestión de incidentes.

46. Se requiere conocer si existe un proceso de notificación en base a fuga de información.

Pero manifestó que como no existe un plan que ayude con la verificación de información pues no existe procedimientos para notificar sobre estos inconvenientes en esta institución.

Análisis: La organización debería evaluar los riesgos que existe al momento de iniciar un desarrollo de un sistema tomando en cuenta la sensibilidad de los datos la manera en que se procesan, almacenan y transmiten por el sistema. Tomar en consideración las copias de almacenamiento y el control de datos.

47. Se preguntó si se evalúan los riesgos de las notificaciones de los incidentes que ocurren dentro de la organización.

Se afirmó que no existe este proceso que ayuda a notificar incidentes que ocurren dentro de la institución, pero sin embargo se toma las medidas necesarias para tomarlas en cuenta.

Análisis: No se tiene procesos que ayuden a notificar fallos de seguridad de la información que existen dentro de este departamento, ya que puede darse por un acceso no autorizado, uso de recursos de manera inapropiada es importante implementar estrategias que permitan tomar decisiones oportunas para evitar mayores incidentes y ayude a disminuir daños a demás recursos de la institución.

48. Si se ha sufrido fallas en la seguridad de la información se requiere saber cuáles fueron sus aprendizajes.

Lo que se manifiesta es que ayudado para tener en cuenta el almacenamiento y resguardo de credenciales de acceso.

Análisis: Debería existir documentación que afirme que procedimientos se debe seguir y mantener un registro adecuado de los fallos que ocurrieron, detallando en que momento sucedió, como se gestionó el incidente.

49. Se preguntó cuáles son los procesos de recopilación de evidencias.

Se manifiesta que el proceso de recopilación de evidencias sigue el proceso de verificar la información con seguridad del GADME y la verificación del personal que ocupa.

Análisis: La organización debería averiguar cuáles son las necesidades de seguridad de la información, para reducir el tiempo y esfuerzo de los impactos, esto implica los requisitos de continuidad.

50. En base a la pregunta de si se tiene una planificación de continuidad de la organización.

Se manifestó que si existe una falla como por ejemplo en la información el proceso que se toma en cuenta son el servidor de pruebas para el levantamiento de servicios caídos con base de datos que se respaldaron.

Análisis: El departamento de sistemas afirma que si existe un plan de contingencia por si existe algún tipo de fallas, pero sin embargo no existe documentación que respalde dicha información, es por ello que se lo toma como una no conformidad ya que deberías estar establecido, documentado, implementado y se mantengan normalizados con el personal administrativo.

4.1.2 Auditoría informática

En la reunión que se tuvo con el departamento de talento humano y gestión administrativa se dio a conocer las acciones a realizarse en el proceso de auditoría además he realizado la entrega del cronograma de actividades en el cual se detalla los departamentos donde se aplicará la auditoria y las personas involucradas dentro de este proceso pidiendo su autorización para iniciar con esta actividad.

Apertura de la auditoria

La reunión de apertura se llevó a cabo en las instalaciones del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo, en primer lugar, se llevó a cabo una reunión con el departamento de sistemas a quienes se les informó cómo sería el proceso de entrevista dentro de la hora establecida de 11:30 AM en donde se contó con la presencia de quienes conforman el área de sistema.

Di a conocer que estaré encargada de realizar la auditoria, a donde se quiere llegar y el alcance de la auditoria, se empleó la ISO 27002 con preguntas basadas en los controles que fueron seleccionados para esta revisión con la cual se ejecutaría esta actividad. Dando a conocer el cronograma y la documentación de apoyo.

Finalizando la reunión se solventó dudas de parte del personal administrativo.

4.1.2.1 Obtención de evidencias

Realizo una clasificación de documentación tomando en cuenta la categoría en la que se encuentra.

Tabla 8. Clasificación de información en documentos.

Confidencialidad	Integridad	Disponibilidad	Criticidad
Información Restringida	A – Alta	1 – Alta	ALTA
Información Privada	M – Media	2 – Media	MEDIA
Información Pública	B – Baja	3 – Baja	BAJA
Información no publicada	No clasificada	4 – No clasificada	

Se realizó una respectiva clasificación de la información en documentos.

Tabla 9. Clasificación de información de documentos

Documento	Confidencialidad	Integridad	Disponibilidad	Criticidad
Plan estratégico, metas y objetivos institucionales.	Información pública	Baja	3	Baja
Planes operativos anuales	Información pública	Media	2	Media
Proyectos institucionales, normativa interna y su documentación.	Información pública	Media	2	Media
Plan de inversión anual	Información pública	Media	2	Media
Documentación de soporte al Sistema de Información General	Información privada	Bajo	3	Bajo
Informe sobre escalas salariales	Información pública	Media	2	Media
Norma técnica para la aplicación de remuneración	Información pública	Baja	3	Baja
Criterios informes jurídicos y absoluciones de consultas jurídicas cuyo objeto es el análisis de temas de diversa índole legal como temas comerciales, financieros, tributarios, laborales.	Información pública	Alta	1	Alta
Base de datos de los usuarios de la institución.	Información confidencial	Alta	1	Alta
Descripción de los procesos, políticas y procedimientos del área	Información privada	Alta	1	Alta
Planes y proyectos de inversión	Información pública	Media	2	Media
Plan operativo	Información pública	Media	2	Media
Infraestructura de red y de equipos	Información pública	Alta	1	Alta
Configuración de la red y equipos	Información restringida	Alta	1	Alta
Manuales técnicos de las plataformas tecnológicas	Información privada	Alta	1	Alta

Índices, reportes, registros, estadísticas, propios del área	Información privada	Alta	1	Alta
Programas fuentes de los sistemas adquiridos desarrollados	Información restringida	Alta	1	Alta
Código fuente de procedimientos, paquetes y scripts de base de datos e interfaces de sistemas	Información restringida	Alta	1	Alta
Scripts de seguridad a nivel de aplicativos y bases de datos para encriptación de la información	Información restringida	Alta	1	Alta
Manuales técnicos/ Usuario/ Instalación y configuración tanto de HW como de SW, incluye sistemas de información.	Información privada	Alta	1	Alta
Documentación de procesos críticos relacionados con los servicios de comunicación en la institución	Información privada	Media	2	Media
Diagrama de diseño de infraestructura y tecnología de red, Data Center y en general de la arquitectura tecnológica de la institución	Información confidencial	Alta	1	Alta
Inventarios de HW y SW incluye aplicaciones	Información privada	Media	2	Media
Inventario de Usuarios, nombres de cuentas, contraseñas para las plataformas tecnológicas y sistemas de información.	Información pública	Alta	1	Alta
Proyecto y presupuestos de inversión para TI	Información pública	Alta	1	Alta
Planes de tratamiento de riesgo	Información privada	Alta	1	Alta
Información de procesos contractuales para la provisión de soluciones tecnológicas	Información pública	Media	2	Media

Registro de las observaciones

Los hallazgos que se encontraron en la auditoria se revisaron para determinar las conformidades de la empresa y no conformidades.

Tabla 10. Registro de auditoría.

Objetivo de control	No Conformidad	Hallazgos de la auditoría
A.5 Políticas de seguridad de la información.	A.5.1.1 Políticas para la seguridad de la información	Dentro del gobierno autónomo descentralizado municipal del cantón espejo, no se encuentran documentos procedimientos o normativas a seguir para resguardar los datos.
A.6 Organización de la seguridad de la información	A.6.1.1 Roles y responsabilidades en seguridad de la información	Dentro de e área de sistemas no se encuentra definido roles de seguridad de la información.
	A.6.1.2 Segregación de tareas	El departamento de sistemas no cubre con los objetivos establecidos por la institución, por falta de personal que desempeñe las actividades.
A.7 Seguridad relativa a los recursos humanos.	A.7.1.1 Investigación de antecedentes	Existe contratos a personas sin una experiencia en el área y tiene desventajas como es la alta inversión de tiempo, esfuerzo innecesario y en diferentes ocasiones dinero.
	A.7.1.2 Términos y condiciones del empleo	No se capacita sobre seguridad de la información y no se conoce las normas ISO 27002.
	A.7.2.2 Concienciación, educación y capacitación en seguridad de la información	El no estar capacitado el personal genera pérdidas de productividad o costo en la rotación de los trabajadores.
	A.7.2.3 Proceso disciplinario	No disponen de un procedimiento disciplinario basado en una investigación preliminar, una investigación disciplinaria, la finalización de una investigación y un periodo de desarrollo y prueba.
A.8 Gestión de activos	A.8.1.2 Propiedad de los activos	No se cuenta con documentos de control de inventarios por lo que puede ocasionar problemas de operatividad e identificación de problemas de producción.
	A.8.3.2 Eliminación de soportes	No se establece procedimientos para la eliminación de soportes.
A.9 Control de acceso.	A.9.1.2 Acceso a las redes y a los servicios de red	No existe documentación donde afirme quien puede acceder a redes o servicios de redes y son expuestos a la manipulación del personal.

	A.9.2.1 Registro y baja de usuario	El no contar con un procesos de baja de usuarios puede ocasionar problemas de desmotivación y reducción de productividad afectando a la seguridad de los datos ya que el personal estará rotando y necesitaran un proceso de adaptación de como resguardar los datos y se mantendrá en modificación y puede haber problemas de alteración de datos.
	A.9.4.4 Uso de utilidades con privilegios del sistema	No existe ningún tipo de supervisión por parte del área de sistemas y pueden acceder personas no autorizadas y vulnerar datos.
A.10 Criptografía	A.10.1.1 Política de uso de los controles criptográficos	No se cuenta con políticas internas para el uso de la criptografía en los datos, al momento de iniciar con el desarrollo de un sistema para la empresa.
	A.10.1.2 Gestión de claves	La aplicaciones y sistemas si cuentan con contraseñas pero no son resguardadas de la mejor manera.
A.12 Seguridad de las operaciones.	A.12.2.1 Controles contra el código malicioso	No se cuenta con controles preventivos que permitan controlar códigos maliciosos.
	A.12.7.1 Controles de auditoría de sistemas de información	No cuentan con controles de acceso a los datos más estrictos.
A.13 Seguridad de las comunicaciones	A.13.1.1 Controles de red	No se establece controles para la administración de redes y no existe ningún tipo de normas para la confidencialidad e integridad de la información.
A.14 Adquisición, desarrollo y mantenimiento de los sistemas de información.	A. 14.2.5 Principios de ingeniería de sistemas seguros	Durante el desarrollo de sistemas no se tiene procedimientos de seguridad ya que se afirma que desarrollan de manera ocasional y no son programas extensos.
A.16 Gestión de incidentes de seguridad de la información.	A.16.1.1 Responsabilidades y procedimientos	El personal de esta área de sistemas, no cumple con la segregación de funciones ya que son dos personas que están dentro de este departamento.
	A.16.1.2 Notificación de los eventos de seguridad de la información	No existe procesos de notificación si existe un posible fallo de seguridad y riesgos en la base de datos, o error en hardware.
	A.16.1.4 Evaluación y decisión sobre los eventos de seguridad de información	Si existe riesgos y no son informados adecuadamente existe probabilidades de que una amenaza explote la vulnerabilidad.

De acuerdo a la verificación de cada uno de los controles y riesgos de seguridad informática a los procesos dentro del área de sistemas, representándolos en la siguiente matriz.

Tabla 11. Clasificación de muestra.

		GRAVEDAD (IMPACTO)				
		MUY BAJO 1	**BAJO 2**	**MEDIO 3**	**ALTO 4**	**MUY ALTO 5**
PROBABILIDAD	**MUY ALTA 5**	5	10	15	20	25
	ALTA 4	4	8	12	16	20
	MEDIA 3	3	6	9	12	15
	BAJA 2	2	4	6	8	12
	MUY BAJA 1	1	2	3	4	5

En base a la clasificación que se muestra en la tabla 11 se procede a realizar la matriz de riesgos en donde se da a conocer las conformidades encontradas dentro de este proceso de auditoría.

Tabla 12. Validación de controles con la ISO 27002:2013.

Objetivo de control	Riesgo	Probabilidad	Gravedad Impacto	Valor de riesgo	Nivel de riesgo
A.5.1 Directrices de gestión de la seguridad de la información.	A.5.1.2 Revisión de las políticas para la seguridad de la información.	3	5	15	Muy grave
A.6.1 Organización de la seguridad de la información.	A.6.1.1. Roles y responsabilidades en seguridad de la información.	3	5	15	Muy grave
	A.6.1.2. Segregación de tareas.	5	5	25	Muy grave

	A.6.1.3. Contacto con las autoridades	4	5	20	Muy grave
	A.6.1.4. Contacto con grupos de interés especial	4	4	16	Muy grave
	A.6.1.5. Seguridad de la información en la gestión de proyectos.	5	4	20	Muy grave
	A.6.2.2. Teletrabajo	1	3	3	Apreciable
A.7. Seguridad relativa a los recursos humanos	A.7.1.1. Investigación de antecedentes.	3	5	15	Muy grave
	A.7.1.2. Términos y condiciones del empleo.	4	5	20	Muy grave
	A.7.2.2. Capacitación , educación y capacitación en seguridad de la información	5	5	25	Muy grave
	A.7.2.3. Proceso disciplinario	4	4	16	Muy grave
A.8. Gestión de activos	A.8.1.1. Inventarios de activos	4	4	16	Muy grave
	A.8.1.4. Uso aceptable de los activos	5	3	15	Muy grave
	A.8.2.1. Clasificación de la información	4	4	16	Muy grave
	A.8.2.2. Etiquetado de la información	5	4	20	Muy grave
	A.8.3.1. Gestión de soportes extraíbles.	4	5	20	Muy grave
	A.8.3.2. Eliminación de soportes.	4	4	16	Muy grave
A.9. Control de acceso	A.9.1.1. Políticas de control de acceso.	4	5	20	Muy grave
	A.9.1.2. Acceso de las redes y a los servidores de red.	3	5	15	Muy grave
	A.9.2.1. Registro y baja de usuario.	5	4	20	Muy grave
	A.9.2.2. Provisión de acceso de usuario.	4	4	16	Muy grave
	A.9.2.3. Gestión de privilegios de acceso.	5	3	15	Muy grave
	A.9.4.1. Restricción del acceso a la información.	4	5	20	Muy grave
	A.9.4.3. Gestión de contraseña	4	4	20	Muy grave
	A.9.4.4. Utilidades con privilegios	4	4	16	Muy grave
A.10. Criptografía	A.10.1.1. Política de uso de controles criptográficos	4	5	20	Muy grave
	A.10.1.2. Gestión de claves	5	5	25	Muy grave

A.11. Seguridad física y del entorno	A.11.2.4 Mantenimiento de los equipos	4	4	16	Muy grave
A.12. Seguridad de las operaciones	A.12.1.1. Documentación de procedimientos de la operación.	5	4	20	Muy grave
	A.12.1.2. Gestión de cambios	4	4	16	Muy grave
	A.12.3.1. Copias de seguridad de la información.	5	5	25	Muy grave
	A.12.4.1. Registro de eventos.	4	5	20	Muy grave
	A.12.4.3. Registro de administración y operación.	4	5	20	Muy grave
	A.12.5.1. Instalación del software en explotación	4	3	12	Importante
	A.12.6.1. Gestión de las vulnerabilidades técnicas	4	5	20	Muy grave
	A.12.6.2. Restricción en la instalación de software	3	4	12	Importante
	A.12.7.1. Controles de auditoria de sistemas de información	5	4	20	Muy grave
A.13. Seguridad de las comunicaciones	A.13.1.1. Control de red	4	4	16	Muy grave
	A.13.1.2. Seguridad de los servicios de red	5	5	25	Muy grave
	A.13.1.3. Segregación en redes	5	3	15	Muy grave
	A.13.2.1. Políticas y procedimientos de intercambio de información	5	4	20	Muy grave
	A.13.2.2. Acuerdos de intercambio de información	4	3	12	Importante
	A.13.2.4. Acuerdos de confidencialidad o no revelación	4	3	12	Importante
A.14. Adquisición, desarrollo y mantenimiento de los sistemas de información	A.14.2.1. Políticas de desarrollo seguro	4	4	16	Muy grave
	A.14.2.2. Procedimiento de control de los cambios en sistemas	4	5	20	Muy grave
	A.14.2.3. Revisión de aplicaciones tras cambios de sistemas operativos	4	5	20	Muy grave
	A.14.2.6. Entorno de desarrollo seguro	5	4	20	Muy grave

	A.14.2.9. Pruebas de aceptación de sistemas	4	5	20	Muy grave
	A.14.3.1. Protección de los datos de prueba	5	4	20	Muy grave
A.16. Gestión de incidentes de seguridad de la información	A.16.1.1. Responsabilidades y procedimientos	4	5	20	Muy grave
	A.16.1.2. Notificación de los eventos de seguridad de la información.	5	4	20	Muy grave
	A.16.1.3. Notificación de puntos débiles de la seguridad	5	4	20	Muy grave
	A.16.1.4. Evaluación y decisión sobre los eventos de seguridad de la información	3	4	12	Importante
	A.16.1.5. Respuesta a incidentes de seguridad de la información	3	5	15	Muy grave
A.17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio.	A.17.1.2. Implementar la continuidad de la seguridad de la información	5	4	20	Muy grave
	A.17.2.1. Disponibilidad de los recursos de tratamiento de la información	4	3	12	Importante
A.18. Cumplimiento	A.18.1.4. Protección y privacidad de la información de carácter personal	4	4	16	Muy grave
	A.18.1.5. Regulación de los controles criptográficos	4	5	20	Muy grave

4.1.2.3 Finalización de la auditoría

Una vez que se finalizó el proceso de verificación de los controles y objetivos de las normativas se puede obtener el informe final de la auditoria y el plan que ayude a la mitigación de estos riesgos.

Informe final de auditoría 29 de mayo de 2023.

Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo.

Institución auditada

Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo

El proceso de auditoría de seguridad informática se llevó a cabo bajo la normativa ISO 27002:2013, en donde se evalúa los controles de seguridad en el departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo, que tuvo inicio en marzo de 2023 y finalizó en mayo de 2023.

La auditoría se seguridad de ña información fue desarrollada por Leidy Murillo, egresada de la carrera de ingeniería en ciencias de computación de la universidad politécnica estatal del Carchi, bajo el asesoramiento del Ing. Marco Yandún Msc, docente de la misma carrera.

El proyecto de investigación se realizó con el apoyo de quienes conforman el departamento de sistemas, Ing, Klever Pozo, Analista de sistemas informáticos y el Tnlgo. Álvaro Zambrano.

Para realizar la presente auditoria se solicitó la siguiente información a el departamento involucrado.

- Sistema de gestión de la seguridad informática
- Inventario informático
- Matriz de riesgos para la seguridad informática
- Matriz de riesgos para la seguridad informática
- Plan de mejora de la seguridad informática
- Proceso de asignación de seguridad informática
- Procedimientos de creación de soportes extraíbles
- Procedimientos de creación de contraseñas
- Procedimientos de creación de copias de seguridad
- Procedimientos de gestión de soportes extraíbles
- Procedimientos de control de acceso a Internet

- Programa de mantenimiento de equipos informáticos
- Informes de mantenimiento de equipos informáticos
- Planes de mantenimiento de equipos informáticos
- Acuerdos de confidencialidad firmados por el personal.
- Registros de formación en seguridad informática para usuarios internos.

Capacidad del proceso de auditoría.

El proceso para la evaluación que se aplicó en este proceso de auditoria se basó en 114 controles de la norma ISO 27002:2013, donde 81 fueron aplicados al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo y 33 no fueron aplicados.

De un total de 81 controles que se aplicó en el departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo al finalizar el proceso de auditoria se obtiene los siguientes resultados, 18 conformidades y 63 no conformidades, a continuación, se detalla.

Conformidades.

A.5.1.1. Políticas de seguridad de la información. Dentro del departamento de sistemas se mantiene un conjunto de políticas para la seguridad de la información, la misma que es aprobada por la dirección, es publicada y comunicada al personal administrativo que maneja dispositivos que se utilizan diariamente.

A.6.2.1. Políticas de dispositivos móviles. El departamento de sistemas tiene políticas de seguridad que permite asegurar el buen manejo de dispositivos móviles.

A.7.2.1. Responsabilidad de gestión. Cumple con nomas que se estipulan en el departamento y se basan en normativas de contraloría general de estado.

A.7.3.1. Responsabilidades ante la finalización o cambio. Se tiene procedimientos a seguir al momento de que el personal de desarrollo del departamento haya cumplido su función en la organización.

A.8.1.2. Propiedad de los activos. Se mantiene designado los equipos al personal que trabaja dentro de este departamento.

A.8.1.3. Uso aceptable de los activos. Los equipos y la seguridad de ellos dependen de quienes están a cargo de ellos y son los únicos responsables de su uso.

A.8.2.3. Manipulado de la información. La información se resguarda por cada uno de los responsables que manipulan estos datos.

A.9.2.5. Revisión de los derechos de acceso de usuario. El departamento revisa quien puede acceder a las diferentes plataformas.

A.9.2.6. Retirada o reasignación de los derechos de acceso. El departamento de sistemas se encarga de dar acceso a los diferentes sistemas, bases de datos de las cuales se encargan.

A.9.3.1. Uso de la información secreta de autentificación. La información se respalda mediante contraseñas seguras que se actualizan de manera obligatoria.

A.9.4.2. Procedimientos seguros. Consta con seguridad en la base de datos esta es duplicada para al momento de experimentar con un sistema no se pierda información.

A.12.1.4. Separación de los recursos de desarrollo, prueba y operación. En el momento de desarrollo el departamento de sistemas utiliza métodos que permiten un desarrollo seguro de los sistemas.

A.12.2.1. Controles contra el código malicioso. El departamento se encarga de resguardar los datos y sacar respaldos de los datos ingresados para evitar pérdida por ingreso de virus a los equipos.

A.12.4.4. Sincronización del reloj. En todas las oficinas se encuentra sincronizados los relojes mediante el segundo intercalar.

A.14.2.5. Principios de ingeniería de sistemas seguros. En el desarrollo de sistemas se mantiene un desarrollo seguro a momento de implementar un sistema de información.

A.16.1.6. Aprendizaje de los incidentes de seguridad de la información. El departamento ha sufrido pérdidas de información, y según el conocimiento adquirido y la resolución de los incidentes de seguridad de la información el departamento de informática ha implementado procedimientos de resguardo de datos como también el evitar acceso a personas quienes no son encargadas de manipular los datos de usuarios.

A.16.1.7. Recopilación de evidencias. Dentro del departamento se define procedimientos que permiten identificar la recogida, adquisición y preservación de la información la cual se debe evidenciar.

A.17.1.1. Planificación de la continuidad de la seguridad de la información. Dentro del departamento de sistemas se analiza las necesidades de seguridad de

información y de continuidad para la gestión de la seguridad de la información adversa.

No conformidades

A.5.1.2. Revisión de las políticas para la seguridad de la información. El departamento de sistemas no cuenta con documentación que detalle cuales son los procesos a seguir y que identifique a información segura

A.6.1.1. Roles y responsabilidades en seguridad de la información. El departamento de sistemas y en sí la organización no cuenta con definición de roles y responsabilidades para mantener una seguridad en la información.

A.6.1.2. Segregación de tareas. No se realiza la separación de responsabilidades, es decir, el personal del departamento de recaudación puede realizar actividades del área de sistemas.

A.6.1.3. Contacto con las autoridades. No se cuenta con procedimientos donde se especifique a quien debe de contactar en el caso de que existan sospechas de haber infringido leyes de seguridad.

A.6.1.4. Contacto con grupos de interés especial. El área de sistemas no mantiene ninguna relación con equipos de soporte técnico apropiados que tengan intereses y sean especializados en seguridad.

A.6.1.5. Seguridad de la información en la gestión de proyectos. El departamento de sistemas cuando inicia un proyecto no consta de métodos de gestión sobre todo en desarrollo de aplicaciones o sistemas y no se cuenta con seguridad de la información.

A.6.2.2. Teletrabajo. El departamento de sistemas recibe capacitaciones de manera online y realiza actividades que requieren de autodisciplina y para ello no se tiene medidas de seguridad adecuadas para proteger información accedida, tratada o almacenada en emplazamientos de trabajo.

A.7.1.1. Investigación de antecedentes. Al momento de contratar personal para el departamento de sistemas no se verifica su currículo, por lo tanto, no se tiene documentado responsabilidades y sean aptos para las funciones que desarrollan, es un riesgo considerable ya que podría haber riesgos de robo, fraude o falla en las instalaciones y medios de la organización.

A.7.1.2. Términos y condiciones del empleo. El departamento no cumple con identificación de responsabilidades de la seguridad al momento de una contratación

laboral. Al momento de contratar a personal no se firma documentación donde se describa obligaciones para la seguridad de información que se deben cumplir.

A.7.2.2. Concienciación, educación y capacitación en seguridad de la información. No se cuenta con la capacitación y definición de cada una de las responsabilidades asociadas a la seguridad de la información, impidiendo la aplicación efectiva y eficaz de medios de seguridad, no solo en el departamento de sistemas si no también aumenta la vulnerabilidad en los demás departamentos de la organización de una manera drástica.

A.7.2.3. Proceso disciplinario. El departamento no cuenta con un proceso disciplinario formal por si existe inconvenientes en la información, que ayuden a tomar acciones para quienes hayan provocado algunas fallas en la seguridad.

A.8.1.1. Inventario de activos. No cuenta con documentación que verifique que realizan inventario de activos dentro del departamento.

A.8.1.4. Devolución de activos. No se cuenta con documentación firmada para la devolución de dispositivos que se encuentran a su cargo.

A.8.2.1. Clasificación de la información. La información no se encuentra especificada correctamente ya que, al momento de pedir una clasificación, cierto documento no debería ser públicos.

A.8.2.2. Etiquetado de la información. La información no se encuentra adecuadamente etiquetada.

A.8.3.1. Gestión de soportes extraíbles. El departamento de sistemas no mantiene procesos adecuados de traslado de información, es decir, terceras personas pueden acceder a esta información.

A.8.3.2. Eliminación de soportes. No cuentan con procedimientos para la eliminación segura de soportes, que ayudarán a minimizar un riesgo de filtración de información confidencial.

A.8.3.3. Soportes físicos en tránsito. Durante el transporte de documentación no existe medidas de seguridad.

A.9.1.1. Políticas de control de acceso. No se tiene documentación de procesos donde detalle la revisión de políticas de acceso a la información y sobre todo los derechos y restricciones a usuarios.

A.9.1.2. Acceso de las redes y a los servidores de red. No cuenta con limitación a usuarios, es decir, los administrativos pueden ingresar y manipular equipos de red.

A.9.2.1. Registro y baja de usuario. El departamento de sistemas no cuenta con procedimientos formales de registro y retirada de los usuarios.

A.9.2.2. Provisión de acceso de usuario. No se cuenta con procedimientos formales para poder asignar o revocar sus derechos de acceso para cada uno de los usuarios y sistemas.

A.9.2.3. Gestión de privilegios de acceso. No se asigna derechos de accesos privilegiados y debería ser controlada a través de procesos formales de acuerdo con políticas.

A.9.2.4 Gestión de la información secreta de autentificación de los usuarios. No se cuenta con una asignación de la información secreta.

A.9.4.1. Restricción del acceso a la información. No cuentan con políticas que restrinja el acceso, que permitan controlar los derechos a los diferentes usuarios.

A.9.4.3. Sistemas de gestión de contraseñas. Las contraseñas se realizan de manera empírica, no utilizan sistemas seguros para la creación de las mismas.

A.9.4.4. Uso de utilidades con privilegios del sistema. No existe restricción para los usuarios en algunos sistemas o información, la mayoría de administrativos tienen acceso.

A.9.4.5. Control de acceso al código fuente de los programas. El acceso a los programas y fuentes no cuentan con una previa instrucción de su funcionalidad.

A.10.1.1. Política de uso de los controles criptográficos. No cuenta con controles que permitan proteger la información sensible que se transporta a los dispositivos móviles.

A.10.1.2. Gestión de claves. No se cuenta con políticas sobre el uso, la protección y la duración o el cambio de claves.

A.11.2.4 Mantenimiento de los equipos. No se brinda constante mantenimiento a los equipos.

A.12.1.1. Documentación de procedimientos de la operación. No cuentan con documentación que se encuentre a disposición de los usuarios donde se detalle los procedimientos de el correcto manejo de los equipos informáticos.

A.12.1.2. Gestión de cambios. No se considera la gestión de cambios como la identificación y registro de tratamiento de la información y sistemas que afecten a la seguridad dentro de la información.

A.12.3.1. Copias de seguridad de la información. No se realizan copias de seguridad de información de manera contante y cuando estas se realizan no se verifican de manera periódica, no teniendo garantía

A.12.4.1. Registro de eventos. No se revisa periódicamente las actividades que realizan los usuarios, fallos en los equipos donde se ve afectada la seguridad de los datos.

A.12.4.2. Protección de la información del riesgo. No se cuenta con controles que ayuden con la protección contra los cambios no autorizados en los dispositivos y la información almacenada en estos.

A.12.4.3. Registro de administración y operación. No existe revisiones periódicas sobre quien administra y opera los sistemas.

A.12.5.1. Instalación del software en explotación. No se cuentan con directrices donde se hable de la correcta instalación y manejo a la hora de instalar sistemas operativos.

A.12.6.1. Gestión de las vulnerabilidades técnicas. No se tiene la información actualizada de las vulnerabilidades técnicas en los sistemas de información que se utilizan.

A.12.6.2. Restricción en las instalaciones de software. No se establece reglas en las que se puedan regir los administrativos para poder instalar sistemas o aplicaciones necesarias, además, poder actualizarlos de manera segura para evitar vulnerabilidad en los datos.

A.12.7.1. Controles de auditoria de sistemas de información. No se realiza auditorías de seguridad de la información.

A.13.1.1. Controles de red. No existe documentación donde garantice la seguridad de la información de las redes y procedimientos que verifiquen la protección de los servicios conectados frente a los accesos no autorizados.

A.13.1.2 Seguridad de los servicios de red. No existe mecanismos de seguridad, los niveles de servicio y requisitos de gestión de los servicios de red

A.13.1.3. Segregación en redes. No cuenta con segregación de redes, además de no contar con grupos de servicios de información.

A.13.2.1. Políticas y procedimientos de intercambio de información. No se tiene establecido políticas o directrices para proteger la información que se intercambia, copia o modifica.

A.13.2.2. Acuerdo de intercambio de información. No se tiene incorporado directrices de notificaciones de envíos o de recepción donde se informe las acciones que se realizan.

A.13.2.4. Acuerdo de confidencialidad o no revelación. No cuenta con control en casos de intercambio de información y las políticas no están documentadas.

A.14.2.1. Políticas de desarrollo seguro. No se tiene implementado políticas de desarrollo seguro para aplicaciones o sistemas.

A.14.2.2. Procedimiento de control de cambios en sistemas. No cuenta con procedimientos formales al momento de implantar cambios ya sea en sistemas o aplicaciones.

A.14.2.3. Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. Al momento de aplicaciones o sistemas sean probadas no existe revisiones previas que garanticen que no existe efectos adversos.

A.14.2.6. Entorno de desarrollo seguro. No cuentan con entornos de desarrollo seguros para los proyectos o sistemas.

A.14.2.8. Pruebas funcionales de seguridad de sistemas. No se cuenta con pruebas funcionales durante el desarrollo de sistemas.

A.14.2.9. Pruebas de aceptación de sistemas. Los sistemas no se mantienen actualizados a nuevas versiones.

A.14.3.1. Protección de los datos de prueba. Los datos de prueba no son seleccionados, protegidos y documentados.

A.16.1.1. Responsabilidades y procedimientos. No se brinda respuesta a los incidentes de seguridad de la información.

A.16.1.2. Notificación de los eventos de seguridad de la información. No se notifica fallos de la seguridad de la información de manera inmediata.

A.16.1.3. Notificación de puntos débiles de la seguridad. No existe un mecanismo de notificación para los contratistas, empleados o terceras personas encargados de los sistemas.

A.16.1.4. Evaluación y decisión sobre los eventos de seguridad de información. Los eventos no son evaluados según una escala de importancia, y es por ello que pierden su prioridad.

A.16.1.5. Respuesta a incidentes de seguridad de la información. No se evalúan los eventos de manera frecuente y no existen procesos de cómo hacerlo.

A.17.1.2. Implementar la continuidad de la seguridad de la información. No existe documento que informe sobre un plan de contingencia si existe algún tipo de fallo dentro del departamento.

A.17.2.1. Disponibilidad de los recursos de tratamiento de la información. No existe disponibilidad garantizada de instalaciones de procesamiento para la seguridad de información.

A.18.1.4. Protección y privacidad de la información de carácter personal. No garantiza la protección y la privacidad de la información de quien la administra.

A.18.1.5. Regulación de los controles criptográficos. No se cuenta con criptografía a l momento de importar o exportar software.

Plan de contingencia

Objetivo

Mitigar los riesgos identificados en los procesos de auditoría basada en la norma ISO 27002:2013 con el propósito de reducir el impacto provocado por los incidentes del departamento de sistemas en el Municipio del Cantón Espejo GADME.

Periodo auditoría Febrero 2023 - mayo 2023

Equipo auditor

Auditor Leidy Tamara Murillo Ruano

Asesor Msc. Marco Antonio Yandún Velasteguí

Con la siguiente valoración generada por la matriz, se inicia con el listado de riesgos que tienen impactos y probabilidades altas hasta una escala más baja.

Mitigación de Normas ISO 27002:2013

Tabla 13. Estrategias de mitigación ISO 27002:2013

Situación de riesgo	Riesgo	Estrategias de mitigación
A.5.1.2. No cuenta con documentación que identifique los procesos a seguir para mantener la información segura.	Muy grave	• Establecer políticas constitucionales y legislativas específicas en ámbitos como el nivel operativo y técnico. • Definir la implementación de un sistema de gestión para la de seguridad de la información. • Realizar una auditoría de seguridad de la información donde se pueda determinar normativas. • Revisar políticas de seguridad de la información de manera constante. • Seleccionar y utilizar plataformas como Series CCN, DIRECTION CENTRALE DE LA SÉCURITÉ DES SI, Guías NIST, donde se encuentra documentación de descarga libre sobre directrices de seguridad de la información, normas, instrucciones, guías y recomendaciones que garantizan la seguridad de sistemas.
A.6.1.1. No se define roles y responsabilidades.	Muy grave	• Definir claramente los roles y responsabilidades de cada persona en la organización. Esto incluye identificar los procesos críticos que deben ser segregados y los empleados que tendrán acceso a los mismos. • Capacitar a todos los empleados sobre la normativa de segregación de funciones y enfatizar la importancia de su cumplimiento. • Establecer políticas y procedimientos claros para el manejo y acceso a la información y recursos críticos. Estas políticas deben incluir la identificación, autenticación y autorización de los usuarios que necesitan acceso a los recursos. • Revisar y auditar regularmente los procesos y procedimientos para identificar cualquier vulnerabilidad o riesgo de incumplimiento. Esta revisión debe ser realizada por un equipo independiente.

A.6.1.2. No se realiza la separación de responsabilidades.	Muy grave	• Tomar medidas disciplinarias para aquellos empleados que no cumplan con la normativa de segregación de funciones y para aquellos que intenten comprometer la seguridad de los procesos o recursos críticos. • Implementar controles de acceso y monitoreo para asegurar que los empleados sólo tengan acceso a los recursos que necesitan para realizar sus funciones. • Mantener registros detallados y precisos de todas las transacciones realizadas por los empleados que tengan acceso a los recursos y procesos críticos. • Realizar una revisión regular y periódica de la normativa de segregación de funciones para asegurar que se adapta a cualquier cambio en la organización o en los procesos críticos. • Utilizar la documentación del BANCO CENTRAL DE LA REPÚBLICA ARGENTINA, donde trata sobre métodos para separar las responsabilidades de las actividades que se realizan en la organización, GesConsultor es una herramienta de pago que facilita modelos de gestión para roles y responsabilidades en el personal relacionado con seguridad. • Establecer políticas y procedimientos claros que describan qué funciones y responsabilidades deben desempeñar sus empleados. Debe haber una división clara de responsabilidades y tareas, de tal manera que ningún empleado tenga control o influencia excesiva sobre una tarea específica. • Capacitar a los empleados sobre la separación de responsabilidades y cómo identificar conflictos de interés o situaciones donde haya riesgo de fraude o corrupción. • Llevar un registro y evaluación de las actividades de los empleados, especialmente los que están en posiciones críticas, para asegurarse de que se están adhiriendo a las políticas y procedimientos establecidos. • Establecer diferentes capas de supervisión para que se pueda verificar y aprobar las tareas realizadas por los empleados.

A.6.1.3. No se cuenta con procedimientos donde se especifique a quien debe de contactar en el caso de que existan sospechas de haber infringido leyes de seguridad	Muy grave	• Sancionar si existe algún empleado que ha cometido un acto de fraude, corrupción o conflicto de interés. • Implementar un área de auditoría interna que realice controles periódicos de las operaciones internas y asegure el cumplimiento de las políticas y procedimientos establecidos. • El SANS despliega un artículo sobre cómo se debe analizar los roles relevantes que es clave para mantener una organización en la empresa, además presenta el grado de segregación de funciones. • Establecer un código de conducta claro y fácilmente accesible que describa las expectativas de los empleados en relación con la comunicación con las autoridades. El código de conducta debe ser desarrollado en consulta con los abogados para garantizar la plena conformidad con las leyes y regulaciones aplicables. • Proporcionar formación y capacitaciones periódicas sobre el cumplimiento de la normativa en relación con el contacto con las autoridades. La formación debe ser específica para el trabajo de cada empleado y debe incluir información sobre las leyes y regulaciones relevantes. • Implementar un sistema de supervisión para garantizar que los empleados cumplan con la normativa de contacto con las autoridades. Los supervisores deben estar capacitados para detectar comportamientos sospechosos o inapropiados y saber cómo abordarlos. • Establecer procedimientos claros para que los empleados puedan informar de cualquier comportamiento sospechoso o inapropiado sin temor a represalias. La empresa también debe tener un mecanismo de denuncia confidencial a través del cual se puedan hacer informes de manera anónima. • Establecer consecuencias claras para los empleados que violen la normativa de contacto con las autoridades. Debe haber un régimen disciplinario claro que contemple desde amonestaciones verbales hasta el despido si la infracción es grave.

		• Se puede utilizar como ejemplo CITICUS que es una empresa que en caso de que exista algún tipo de fallo esta ayuda a identificar peligros y amenazas potenciales, evaluar y mitigar el impacto de riesgos.
A.6.1.4. No mantiene ninguna relación con equipos de soporte técnico.	Importante	• Contratar los servicios de un equipo de soporte técnico externo que pueda manejar cualquier problema técnico que surja en la empresa. • Establecer políticas de seguridad informática que incluyan la instalación de software de seguridad, la actualización constante de sistemas operativos y aplicaciones, y la capacitación de los empleados sobre el uso seguro de la tecnología. • Establecer políticas de respaldo de datos para garantizar que toda la información importante esté respaldada y almacenada de forma segura. • Asignar responsabilidades para la resolución de problemas técnicos que puedan surgir. • Establecer planes de contingencia en caso de que surja un problema técnico importante que afecte el funcionamiento de la empresa. • Se puede utilizar documentación del Ministerio de Ciencias e Innovación que generó un sistema de gestión de calidad basado en ISO. 9001:2001 con el fin de buscar relación con grupos de interés beneficiando a la eficiencia y eficacia de gestión de información.
A.6.1.5. No consta de métodos de gestión sobre todo en desarrollo de aplicaciones o sistemas.	Muy grave	• Establecer políticas y procedimientos. • Identificar los riesgos de seguridad al momento de iniciar un desarrollo de aplicaciones o la propia instalación de estos. • Capacitar y formar al personal sobre los procedimientos de seguridad. • Monitorear continuamente la seguridad y la gestión de los proyectos que el departamento realice. • Se puede disponer de Bankinfo Security una plataforma que expone métodos de gestión de la información al iniciar con un desarrollo, además despliega noticias y contenido más relevantes de la seguridad de la información comunicando sobre cómo evitar fraude, robo de identidad.

A.6.2.2. No se tiene medidas de seguridad adecuadas para proteger información accedida.	Apreciable	• Identificar y clasificar la información que se maneja y clasificarla en función de su importancia y nivel de confidencialidad. • Establecer políticas de seguridad claras y precisas, estableciendo los procedimientos y medidas necesarios para la protección de la información. • Implementar medidas de seguridad tecnológicas para proteger la información, como antivirus, sistemas de autenticación, cortafuegos, y sistemas de encriptación. • Capacitar al personal sobre los riesgos de seguridad y las medidas de protección necesarias para proteger la información. • Establecer medidas de seguridad físicas como cámaras de seguridad, cerraduras, y controles de acceso, para proteger la información que se encuentra en dispositivos físicos. • Trabajar con proveedores y clientes para establecer acuerdos y políticas de seguridad que protejan la información que se comparte. • Realizar auditorías regulares para revisar el cumplimiento de las políticas de seguridad, identificar vulnerabilidades y tomar medidas preventivas. • Usar contraseñas fuertes que deben cambiarse de manera periódica • Usar las siguientes guías y herramientas que brindan asesoramiento profesional sobre cómo hacer cumplir esta norma, S21 que informa sobre medidas de seguridad al momento de iniciar con un acceso, NIST se trata de una guía para la seguridad del teletrabajo y acceso remoto.
A.7.1.1. No se verifica su currículo.	Muy grave	• Establecer una política clara y específica de verificación de currículum la cual debe ser comunicada a todos los candidatos que deseen ingresar a la empresa. En esta política se deben indicar los documentos y referencias que se van a requerir para verificar la información del currículum. • Realizar una revisión exhaustiva de los documentos proporcionados por el candidato, incluyendo referencias laborales y educativas.

A.7.1.2. No cumple con identificación de responsabilidades de la seguridad al momento de una contratación laboral.	Muy grave	• Verificar la información con las instituciones correspondientes, como universidades, institutos o empresas antiguas donde el candidato haya trabajado. • Evaluar con cuidado los resultados de la revisión, y en caso de que se detecten irregularidades, tomar las medidas necesarias para evitar que el candidato sea contratado. • Mantener un registro de los procesos de verificación de los candidatos, incluyendo la documentación que se haya revisado y las personas que han participado en el proceso. • Continuar vigilando que se siga cumpliendo la norma de verificación de currículum al momento de ingresar a trabajar a la empresa. • Use GesConsultor se trata de una herramienta de pago que trabaja con normas de SGSI (Sistema de seguridad de la información) que indica sobre como verificar con exactitud el currículo mediante integridad, del solicitante. • Establecer políticas y procedimientos claros y precisos que definan las responsabilidades de seguridad de los empleados y contratistas. Esto permitirá que los empleados y los contratistas comprendan sus responsabilidades de seguridad. • Exigir que todos los empleados y contratistas reciban capacitación en seguridad antes de comenzar a trabajar. Esto garantizará que los empleados y los contratistas entiendan los riesgos de seguridad y sepan cómo prevenir accidentes y lesiones en el lugar de trabajo. • Asegurarse de que los contratos con los contratistas incluyan cláusulas que definan claramente las responsabilidades de seguridad del contratista. Esto asegurará que el contratista asuma la responsabilidad de la seguridad de sus empleados. • Establecer mecanismos de supervisión para garantizar que todos los empleados y contratistas cumplan con sus responsabilidades de seguridad. Esto incluye la supervisión de la capacitación en seguridad, las políticas y procedimientos de seguridad, y la implementación de las medidas de seguridad pertinentes.

		• Implementar sanciones por incumplimiento de las responsabilidades de seguridad. Esto garantizará que los empleados y contratistas tomen en serio la seguridad y cumplan con sus responsabilidades de seguridad. • Se puede tomar como ejemplo National Association of Professional Background Screeners es una organización que puede proporcionar opiniones acerca de buenas prácticas sobre responsabilidad y comprobación de antecedentes para contratación de personal.
A.7.2.2. Concienciación y capacitación sobre seguridad informática.	Muy grave	• Identificación de las necesidades: Realiza un análisis exhaustivo de las necesidades de concienciación y capacitación en seguridad informática dentro de tu organización. Identifica los puntos débiles y las áreas donde se requiere mayor atención. • Desarrollo de programas educativos: Diseña programas educativos eficientes que aborden los aspectos clave de la seguridad informática. Estos programas deben ser accesibles, prácticos y adaptados a las necesidades de tu organización. • Sensibilización sobre las amenazas: Educa a los empleados sobre las amenazas comunes en seguridad informática, como el phishing, malware, ransomware, etc. Explica los riesgos asociados y cómo pueden protegerse y tomar medidas preventivas. • Capacitación práctica: Proporciona capacitación práctica sobre cómo utilizar herramientas de seguridad, cómo crear contraseñas seguras, cómo identificar posibles ataques y cómo reportarlos adecuadamente. • Actualizaciones regulares: Mantén a los empleados actualizados sobre las últimas tendencias y amenazas en seguridad informática. Organiza sesiones de actualización periódicas y proporciona recursos actualizados.

A.7.2.3. Proceso disciplinario.	Muy grave	• Promoción de una cultura de seguridad: Fomenta una cultura organizacional donde la seguridad informática sea una prioridad. Anima a los empleados a reportar cualquier incidente de seguridad y promueve la colaboración en la prevención de riesgos. • Evaluación y seguimiento: Realiza evaluaciones periódicas para medir el progreso y la efectividad de los programas de concienciación y capacitación. Realiza ajustes según sea necesario para mejorar los resultados. • Brindar orientación y apoyo: Proporciona a los empleados una orientación adecuada para que comprendan su rol y responsabilidades. Ofrece capacitación y recursos para ayudarles a desempeñarse de manera efectiva. • Comunicación abierta y regular: Fomenta una comunicación abierta y de dos vías con los empleados. Escucha sus preocupaciones, brinda retroalimentación constructiva y mantén una comunicación regular sobre su desempeño. Esto puede ayudar a evitar que los problemas pequeños se conviertan en problemas mayores. • Investigación imparcial: Si se produce un incidente que requiere un proceso disciplinario, asegúrate de llevar a cabo una investigación imparcial y exhaustiva. Escucha a todas las partes involucradas y recopila pruebas para tomar decisiones justas y equitativas. • Aplicación coherente de las políticas: Asegúrate de aplicar las políticas y los procesos disciplinarios de manera coherente para evitar percepciones de favoritismo o trato desigual. Esto ayuda a mantener la confianza y el respeto en el lugar de trabajo. • Proporcionar oportunidades de mejora: Si un empleado comete un error o muestra un comportamiento inapropiado, bríndale la oportunidad de corregirlo y mejorar. Esto puede incluir la capacitación adicional, el establecimiento de metas claras y el seguimiento regular de su progreso.

A.8.1.1. No cuenta con documentación que verifique que realizan inventario de activos.	Muy grave	• Monitoreo y seguimiento continuo: Mantén un monitoreo constante del desempeño y comportamiento de los empleados. Esto permite detectar problemas potenciales de manera temprana y abordarlos antes de que se conviertan en procesos disciplinarios. Establecer una política clara sobre la realización de inventarios, la frecuencia con la que se deben realizar, los plazos que se deben cumplir y las consecuencias por incumplimiento. • Comunicar la política de inventarios de forma clara y concisa a todo el personal de la empresa pública. Es importante que el personal comprenda la importancia de llevar un control adecuado del inventario. • Capacitar a los empleados en la realización de inventarios, para que puedan llevar a cabo esta tarea de manera efectiva. • Designar a una persona responsable de supervisar los inventarios y asegurarse de que se cumplan los plazos establecidos. • Registrar todos los inventarios de forma adecuada, para poder hacer un seguimiento y control de los mismos. • Analizar los resultados y determinar si hay desviaciones. Si se detectan desviaciones, se deben tomar medidas para corregirlas. • Evaluar la política de inventarios periódicamente para asegurarse de que sigue siendo efectiva y realizar los ajustes necesarios para mejorarla. • Utilizar herramientas que permitan más fácil las actividades de inventario tiene un fin positivo como es OCS Inventory NG, es una herramienta gratuita de creación automática de inventarios de HW.
A.8.1.4. No se cuenta con documentación firmada para la devolución de dispositivos.	Muy grave	• Establecer una política clara de devolución de activos que contemple los procedimientos y requisitos necesarios para llevar a cabo la devolución. • Comunicar la política de devolución de activos a todos los empleados y clientes de la empresa para que conozcan las reglas y procedimientos.

A.8.2.1. La información no se encuentra especificada correctamente.	Muy grave	• Establecer un sistema de seguimiento y control para garantizar que todas las solicitudes de devolución de activos se procesen de manera oportuna y adecuada. • Asignar responsabilidades claras a los empleados encargados de procesar las solicitudes de devolución de activos para que sepan qué hacer ante cada situación. • Establecer medidas disciplinarias y sanciones en caso de incumplimiento de la política de devolución de activos. • Realizar revisiones periódicas de la política de devolución de activos y hacer los cambios necesarios para asegurar que la política sigue siendo efectiva y se adapte a las necesidades de la organización. • Utilizar guías o documentación que ayude a cumplir estos objetivos, GLPI que permite realizar de manera gratuita de inventario de activos con su funcionamiento y gestión de los mismos. • Crear una política clara y concisa relacionada con la especificación correcta de la información en la empresa pública. Esta política debe incluir detalles sobre quién es responsable de proporcionar y verificar la información, así como las consecuencias de proporcionar información incorrecta o inexacta. • Comunicar y difundir la política a todos los empleados de la empresa pública, destacando la importancia de la especificación correcta de la información y haciendo hincapié en las consecuencias de no cumplir con la política. • Proporcionar la formación necesaria a los empleados sobre cómo cumplir con la política de especificación correcta de la información. La formación debe incluir la identificación de la información correcta, la importancia de la precisión de los datos y cómo detectar y corregir errores. • Implementar sistemas de gestión de calidad para verificar la precisión de la información, tales como auditorías y revisiones periódicas de los datos proporcionados.

		• Asegurarse de que haya una sanción adecuada para aquellos que incumplen la política de especificación correcta de la información en la empresa pública, lo que debe ser comunicado a todos los empleados para evitar casos similares. • Establecer un sistema de quejas y un canal de comunicación entre los empleados y la dirección para que se puedan reportar problemas y se puedan tomar medidas de manera oportuna. • Usar como ejemplo MEHARIprdia ayuda a cumplir lineamientos establecidos por la norma ISO 27005 del año 2011 acerca de cómo separar la información en escalas de privacidad o pública. .
A.8.2.2. La información no se encuentra adecuadamente etiquetada.	Muy grave	• Establecer una política de etiquetado de información clara y explícita. • Capacitar a todos los empleados sobre la importancia de la política de etiquetado y cómo implementarla correctamente. • Implementar un sistema de etiquetado que sea fácil de usar y que proporcione información clara sobre el tipo de información, el nivel de confidencialidad y cualquier otra etiqueta relevante. • Establecer un mecanismo de supervisión y seguimiento para asegurar el cumplimiento continuo de la política. • Imponer sanciones estrictas para los empleados que no cumplan con la política de etiquetado. • Promover una cultura de seguridad de la información en toda la empresa, para que los empleados se sientan motivados a seguir la política de etiquetado. • Realizar revisiones periódicas de la política de etiquetado para asegurar que está actualizada y que sigue siendo relevante y efectiva en la protección de la información de la empresa. • Usar la documentación de CNI facilita directrices para poder clasificar y tratar la información.
A.8.3.1. El departamento de sistemas no mantiene procesos adecuados de traslado de información.	Muy grave	• Establecer un equipo que se encargue de desarrollar y monitorear los procesos de traslado de información en la entidad. • Identificar los procesos críticos de la entidad que involucren el traslado de información y establecer un plan de acción para garantizar la seguridad de los datos.

		• Establecer políticas y procedimientos claros que definan los roles y responsabilidades de los involucrados en el proceso de traslado de información, así como las medidas de seguridad necesarias para proteger la información. • Capacitar al personal para asegurar que entiendan la política y los procedimientos establecidos, así como las medidas de seguridad necesarias para proteger la información. • Establecer un proceso de monitoreo y auditoría para garantizar el cumplimiento de la política y los procedimientos establecidos y para identificar y corregir cualquier fallo o vulnerabilidad. • Actualizar constantemente de las políticas y los procedimientos a medida que cambien las necesidades de la entidad, las regulaciones y las tecnologías para garantizar que siempre estén alineados con las mejores prácticas de seguridad de la información. • es una herramienta gratuita que permite realizar un borrado seguro de disco duro de manera completa. • Se puede tomar como ejemplo INCIBE que presta sus servicios para almacenar los datos que se van a trasladar de manera segura. • Usar ROHOS que es una aplicación que permite su ingreso de manera gratuita que permite crear un cifrado y ocultar la información y proteger con contraseñas en las USB.
A.8.3.2. No cuentan con procedimientos para la eliminación segura de soportes.	Muy grave	• Implementar métodos de borrado o destrucción aplicable en los soportes. • Generar capacitaciones de procedimientos de borrado seguro, borrado criptográfico, destrucción física y medios para el borrado y la respectiva destrucción • Utilizar AENOR es una norma que presenta y facilita normas UNE-EN para la destrucción segura de soportes confidenciales y los requerimientos para la gestión, control de su recogida, trayecto y su eliminación.
A.9.1.1. No se tiene documentación de procesos donde detalle la	Muy grave	• Identificar recursos y usuarios que necesitan acceder a ellos. • Clasificar según su nivel de seguridad y la información que manejan. • Definir los roles y responsabilidades de los usuarios y la administración de los recursos.

revisión de políticas de acceso.		• Definir las políticas de acceso a los recursos en función de la clasificación y los roles definidos anteriormente. • Implementar medidas de seguridad como autenticación, autorización y control de acceso para garantizar que solo los usuarios autorizados puedan acceder a los recursos. • Monitorear el acceso a los recursos y actualizar las políticas de acceso periódicamente para adaptarse a cambios en la empresa y en el entorno de seguridad. • Capacitar a todos los usuarios que tienen autorización, sobre políticas de acceso y las medidas de seguridad implementadas. • OpenNac permite dar pautas para el control de accesos ya sea LAN o WAN en las empresas, compatible con distintos proveedores de tecnología de red. Admitiendo autenticación basada en políticas, autorización y auditoría de acceso a la red.
A.9.1.2. No cuenta con limitación a usuarios.	Muy grave	• Determinar qué información y recursos son críticos para la empresa, como bases de datos de clientes o información financiera. • Crear perfiles de usuario que diferencien los niveles de acceso y restricciones, según las responsabilidades de cada individuo en la empresa. • Configurar un proceso de autenticación sólido, como contraseñas seguras, o autenticación de dos factores. • Establecer políticas para evitar el acceso no autorizado, por ejemplo, limitar el acceso en horarios no laborables, o a través de dispositivos móviles no seguros. • Utilizar herramientas de seguridad tales como sistemas de encriptación, firewalls, y sistemas que monitorean el acceso a los recursos de la empresa. • Realizar revisiones regulares de las políticas y procedimientos de seguridad, y actualizar las herramientas de seguridad para evitar vulnerabilidades. • Realizar sesiones de capacitación sobre políticas de seguridad para los empleados, desde cómo crear contraseñas seguras hasta el acceso autorizado a información crítica.

A.9.2.1. No cuenta con procedimientos formales de registro y retirada de los usuarios.	Muy grave	• Utilizar como ejemplo Packetfence ofrece una solución de control de acceso a la red de código abierto diseñada para proteger eficazmente redes heterogéneas pequeñas y grandes. • **Registro de usuarios:** • Definir los criterios de elegibilidad para ser usuario de la empresa pública. • Establecer un formulario de registro que incluya la información necesaria para la identificación del usuario y la documentación que deberán presentar para acreditar su elegibilidad. • Una vez que el usuario complete el formulario de registro y presente la documentación correspondiente, se verificará la información suministrada y se comprobará que cumple con los criterios de elegibilidad. Se puede requerir que la documentación sea validada por un tercero o se realice una entrevista personal. • Una vez que se confirme que el usuario es elegible, se procederá a crear un perfil en el sistema de registro y se le entregará su tarjeta de identificación o cualquier otro medio que valide su condición de usuario de la empresa pública. • **Retirada de usuarios:** • Establecer las causales de retirada de usuarios y las acciones a tomar en cada caso, por ejemplo: fallecimiento del usuario, cambio de residencia, pérdida o daño de la tarjeta de identificación, incumplimiento de las políticas de la empresa pública, entre otros. • Elaborar un formulario de retiro de usuario, que permita recopilar la información necesaria para identificar al usuario y su causa de retiro. • Realizar el procedimiento correspondiente que puede ser entrevista, verificación de documentación, validación de información, para validar la causa de retiro del usuario. • Una vez confirmada la causa de retiro, proceder a eliminar el perfil del usuario del sistema de registros y retirar la tarjeta de identificación o cualquier otro medio que identifique al usuario.

		• En caso de que la causa de retiro sea por incumplimiento de políticas, se debe informar al usuario por escrito las razones de su retiro y dejar constancia en el sistema de registros • Utilizar Manage Engine se trata de una solución web que ayuda a automatizar y optimizar el proceso de altas y bajas de usuarios en una organización, proporcionando una mayor seguridad y eficiencia en la administración de recursos y permisos. Puede ayudar a reducir la carga administrativa sobre el Departamento de Recursos Humanos..
A.9.2.2. No se cuenta con procedimientos para poder asignar o revocar derechos de acceso para cada uno de los usuarios y sistemas.	Muy grave	• Identificar y clasificar los datos y recursos críticos que son importantes para la organización y clasificarlos según su nivel de importancia y su grado de confidencialidad. • Definir los roles de acceso a los usuarios que desempeñan en la organización y los derechos de acceso que cada no necesita para realizar sus tareas. • Establecer políticas claras y detalladas que definan quién puede acceder a qué recursos y bajo qué condiciones. • Implementar medidas de seguridad sólidas, tales como contraseñas seguras, autenticación de dos factores, cifrado de datos, entre otras. • Monitorear y auditar los accesos para detectar actividades sospechosas o inusuales y tomar medidas para prevenir futuros incidentes de seguridad. • Revisar y actualizar las políticas de acceso para asegurarse de que sigan siendo relevantes y efectivas en la protección de los datos y recursos críticos de la organización. • Se puede usar Manager Engine es una herramienta que facilita realizar altas y bajas de usuario con la aplicación de políticas por medio de interfaces intuitivos y fáciles de seguir. Creación de cuentas de usuario para nuevos empleados.
A.9.2.3. No se asigna derechos de acceso privilegiado.	Muy grave	• Crear un equipo de gestión para administrar los privilegios de acceso a la información. Este equipo debe ser compuesto de diferentes departamentos como recursos humanos, y el departamento de sistemas, seguridad y auditoría interna.

		• Identificar los recursos y sistemas que requieren políticas de acceso privilegiado. Esta fase ayudará a determinar qué usuarios deben tener acceso a cada recurso y qué tipo de acceso se les permite. • Establecer políticas y procedimientos claros que regulen el acceso privilegiado a los recursos. Debe identificar y documentar las actividades que se requieren para acceder a recursos y sistemas y establecer una política de contraseñas sólida. • Designar administradores de acceso que serán responsables de otorgar y revocar los derechos de acceso privilegiado. Estos administradores deben ser identificados y documentados en las políticas de acceso. • Asignación de roles a los usuarios para un acceso apropiado y garantizar que los usuarios tengan derechos de acceso solamente a los recursos que necesitan para realizar sus tareas. • Establecer un proceso de monitoreo y auditoría continua para supervisar el acceso privilegiado a los recursos. Esta actividad debe ser documentada y verificada regularmente. • Capacitación de usuarios sobre las políticas y procedimientos de acceso privilegiado. Todos los usuarios deben estar informados de sus responsabilidades en la protección de la información y la seguridad de los sistemas. • Revisar y actualizar periódicamente sus políticas y procedimientos de acceso privilegiado en función de los cambios en la tecnología, las regulaciones legales y los riesgos de seguridad. • Usar UserlocK es una medida de seguridad que se utiliza en el acceso a sistemas informáticos y aplicaciones. Cuando se produce un número determinado de intentos fallidos de inicio de sesión con una cuenta de usuario, el sistema puede bloquear automáticamente la cuenta del usuario, impidiendo que se realice un acceso no autorizado. El objetivo de esta medida es proteger la cuenta y los datos personales o confidenciales que pueda contener, además de evitar que un atacante pueda utilizar técnicas de fuerza bruta para adivinar la contraseña correcta y acceder al sistema.

A.9.2.4. Gestión de la información secreta de autenticidad de los usuarios.	Muy grave	• Implementa una fuerte política de contraseñas: Recomienda a los usuarios que utilicen contraseñas seguras que incluyan combinaciones de letras, números y caracteres especiales. • Autenticación de dos factores: Considera utilizar un método de autenticación de dos factores para agregar una capa adicional de seguridad. Esto podría incluir el uso de códigos enviados a dispositivos móviles o aplicaciones de autenticación. • Encriptación de datos: Asegúrate de que la información de autenticidad de los usuarios se almacene y transmita de manera segura utilizando métodos de encriptación robustos. • Seguimiento de accesos: Implementa un sistema de seguimiento y registro de accesos para monitorear y auditar las actividades de los usuarios. • Capacitación en seguridad: Brinda capacitación regular a los usuarios para concienciar sobre las mejores prácticas de seguridad, como no compartir información de autenticidad con terceros, no hacer clic en enlaces sospechosos. • Actualizaciones y parches: Mantén tus sistemas y aplicaciones actualizadas con los últimos parches de seguridad para prevenir vulnerabilidades conocidas.

A.9.4.1. No cuentan con políticas que restrinja el acceso.	Muy grave	• Definir los objetivos de seguridad. • Identificar los riesgos a los que la empresa pública se enfrenta en términos de seguridad. Esto incluye evaluar los posibles riesgos de seguridad, como la filtración de información confidencial, la interrupción de los servicios o el acceso no autorizado a sistemas o información. • Establecer políticas y procedimientos de seguridad basadas en los objetivos y riesgos identificados. Estas políticas deben incluir medidas para restringir el acceso a la información y los sistemas a los que los empleados no están autorizados. • Educar y entrenar a los empleados en la nueva política de seguridad y los procedimientos asociados. Esto debe incluir la educación sobre los riesgos de seguridad y las consecuencias de no cumplir con la política de seguridad. • Monitorear y evaluar regularmente el cumplimiento de las políticas y los procedimientos de seguridad. Esto debe incluir pruebas de vulnerabilidad y de penetración, así como revisiones periódicas de los controles de acceso. • Realizar mejoras continuas de las políticas y procedimientos de seguridad para adaptarse a los cambios en el entorno empresarial y en los riesgos de seguridad. • Se puede utilizar Ophcrack que trata sobre técnicas avanzadas de crackers para recuperar contraseñas de usuarios y administradores en cualquier versión de Windows, incluyendo las últimas. Ofrece una interfaz gráfica de usuario, fácil de usar y es muy efectivo en la recuperación de contraseñas para usuarios con poca experiencia técnica. Ophcrack funciona mediante el uso de ataques de diccionario y fuerza bruta para descifrar las contraseñas de los usuarios y administradores de Windows.
A.9.4.3. Las contraseñas se realizan de manera empírica.	Importante	• Exigir contraseñas fuertes que estén compuestas por al menos ocho caracteres que incluyan números, letras mayúsculas, minúsculas y símbolos. • Cambio de contraseñas periódicamente cada tres meses. • Restricción de uso de contraseñas repetidas, antiguas o repetidas.

		• Bloquear intentos de acceso, después de un número determinado de intentos fallidos, el sistema bloqueará el acceso. • Autenticación de dos factores para acceder a información sensible. Por ejemplo, un código enviado al correo electrónico o al teléfono celular del usuario permite verificar la identidad antes de acceder a la información. • Educar a los usuarios sobre las mejores prácticas de seguridad en la creación y gestión de contraseñas fuertes y seguras. • Políticas de acceso a la información sensible y bajo qué circunstancias se puede permitir este acceso. • Monitoreo de la seguridad de las contraseñas y estar alerta ante posibles intentos de ataques cibernéticos. • Usar PASSWORD GENERATOR es una plataforma de acceso libre que permite generar contraseñas de manera online, al igual que RANDOW PASSWORD GENERATOS ofrece servicios de crear contraseñas seguras. • Se puede usar FIDO Authentication es una herramienta que permite iniciar sesión segura y rápida a la web y aplicaciones, tomando en cuenta Apple, Amazon, Facebook, Google, entre otras entidades financieras.
A.9.4.4. No existe restricción para usuarios en sistemas o información.	Muy grave	• Definir claramente la política de restricción de acceso, especificando quiénes tienen acceso, qué tipo de acceso tienen y en qué momentos. • Implementar medidas de seguridad como el uso de contraseñas seguras, autenticación de usuarios y monitoreo de actividad. • Comunicar la política de restricción de acceso a todos los usuarios involucrados y asegurarse de que comprendan las reglas y las consecuencias de no cumplirlas. • Capacitar a los usuarios en el manejo adecuado de contraseñas y en el uso seguro del sistema de información.

A.9.4.5. Control de acceso al código fuente de los programas.	Muy grave	• Realizar revisiones periódicas de los permisos de acceso de los usuarios, eliminando aquellos que no sean necesarios o no estén siendo utilizados. • Mantener un registro de las actividades de los usuarios, de manera que se puedan identificar posibles infracciones y tomar medidas preventivas. • Establecer un protocolo en caso de incumplimientos a la política de restricción de acceso, que incluya la notificación a las autoridades competentes y la toma de medidas disciplinarias. • Se puede usar Fido Authentication para autenticar la identidad de un usuario de forma segura y eficiente. Esta tecnología utiliza protocolos de autenticación de múltiples factores para habilitar la identificación del usuario a través de dispositivos móviles y ordenadores personales. • Esto proporciona un mayor nivel de seguridad en las actividades en línea, incluyendo el inicio de sesión en sitios web y aplicaciones, la realización de compras en línea, la realización de transacciones bancarias, entre otros. Además, permite a los usuarios utilizar métodos de autenticación más convenientes, como el reconocimiento de huellas dactilares y el reconocimiento facial, en lugar de tener que recordar contraseñas complejas. • Acceso basado en roles: Establece roles y privilegios específicos para los desarrolladores y otras personas que necesiten acceder al código fuente. Limita el acceso solo a aquellos que realmente lo requieran para sus tareas. • Control de versiones: Utiliza sistemas de control de versiones, como Git, para administrar y rastrear los cambios en el código fuente. Esto te permitirá tener un registro de qué cambios se hicieron y quién los realizó. • Monitoreo de acceso: Implementa sistemas de monitoreo y registro de acceso al código fuente. Registra quién accede al código y qué acciones realizan, lo cual puede ser útil para identificar comportamientos sospechosos o maliciosos.

		• Limitación de acceso físico y remoto: Asegúrate de que el acceso físico a las áreas donde se almacena el código fuente esté restringido y solo permitido a personas autorizadas. Además, asegura que las conexiones de acceso remoto al código estén seguras y se utilicen protocolos seguros como SSH. • Encriptación de código fuente: Considera encriptar el código fuente almacenado para agregar una capa adicional de seguridad. Esto ayudará a protegerlo en caso de que alguien obtenga acceso no autorizado a los archivos. • Educación en seguridad: Brinda capacitación y concientización en seguridad a los desarrolladores y otras personas involucradas en el manejo del código fuente. Esto incluye prácticas como no compartir credenciales, utilizar contraseñas seguras y estar atentos a posibles amenazas de seguridad
A.10.1.1. No cuenta con controles que permitan proteger la información sensible.	Muy grave	• Implementar políticas que permitan regular el uso de controles de cifrado para proteger la información. • Sans es un modelo que ayuda con redacción de políticas que se relacionan con el cifrado y la seguridad de información y consta de una interfaz fácil de usar. • GNU Project es una aplicación que permite cifrar y firmar los datos, además, cuenta con un sistema de gestión de claves.
A.10.1.2. No se cuenta con políticas sobre el uso, la protección y la duración o el cambio de claves.	Muy grave	• Desarrollar y aplicar políticas sobre el uso, la protección y el ciclo de vida de las claves criptográficas a lo largo de todo su ciclo de vida. • Usar la plataforma de MANDOSs que permite el reinicio no gestionado o remoto de servidores con sistemas de archivos raíz cifrados. • Usar Crytool se la conoce como una plataforma de código abierto que permite experimentar aspectos de cifrado en Linux, MAC OS X y Windows.

A.11.2.4. No se brinda constante mantenimiento a los equipos.	Muy grave	• Hacer un inventario de los equipos existentes en la empresa, incluyendo su estado de funcionamiento, edad, historial de mantenimiento y vida útil. • Determinar los equipos más críticos para la operación de la empresa y establecer un plan de mantenimiento preventivo y correctivo adecuado y con una periodicidad definida. • Definir políticas claras sobre el tipo de mantenimiento que se realiza a los equipos y definir la periodicidad y el proceso de seguimiento. • Asignar responsabilidades de cada área encargada del mantenimiento de los diferentes equipos, incluyendo la supervisión y el control de la actividad. • Establecer los procedimientos de mantenimiento y protocolos para el mantenimiento adecuado de los equipos, incluyendo actividades de verificación, reemplazo de partes, reparaciones y limpieza. • Establecer un presupuesto para el mantenimiento de los equipos, considerando la frecuencia del mantenimiento, costo de los repuestos y la mano de obra. • Establecer un sistema de seguimiento para el mantenimiento de los equipos, que permita medir los resultados del trabajo realizado y evaluar el cumplimiento de los planes de mantenimiento. • Revisar y actualizar las políticas de mantenimiento de forma regular, para asegurarse de que se estén cumpliendo adecuadamente y de que se estén adaptando a las necesidades de la empresa • Se puede utilizar APC que facilita documentación en inglés y español, sobre protección de equipos. • Se puede usar NFPA presenta estándares de protección contra inconvenientes físicos se puede encontrar manuales en inglés y español.
A.12.1.1. No cuentan con documentación donde se detalle los procedimientos	Muy grave	• Controlar el acceso a los equipos informáticos a aquellos empleados que hayan sido autorizados y capacitados para su uso.

del manejo de los equipos informáticos.		• Usar contraseñas fuertes y que se cambien regularmente. El acceso a las cuentas de administrador estará restringido y solo se permitirá a aquellos empleados responsables y capacitados. • Aplicar restricciones en la descarga e instalación del software en los equipos debe ser aprobado previamente por los departamentos correspondientes. No se permitirá la descarga de software de fuentes desconocidas o no autorizadas. • Proteger los datos y asegurar que los equipos estén protegidos con software antivirus y cortafuegos para evitar la pérdida de datos o ataques cibernéticos. • Respaldar los datos importantes de forma regular en unidades de almacenamiento externas a los equipos. • Actualizar de manera periódicas los equipos y su software con las últimas versiones disponibles para garantizar una buena funcionalidad y evitar vulnerabilidades de seguridad. • Restringir el uso de equipos informáticos solo se pueden usarse para fines laborales únicamente. No se permitirá el uso de los equipos para fines personales. • Eliminar de manera segura de los equipos informáticos que ya no sean necesarios no deberán ser desechados sin una eliminación segura de los datos. Los discos duros y cualquier otro medio de almacenamiento deben ser eliminados de forma segura. • Capacitar regularmente los empleados en el uso adecuado de los equipos informáticos y la implementación de prácticas seguras. • Cumplir y monitorear de forma continua y se tomarán medidas disciplinarias adecuadas en caso de incumplimiento. • Se puede usar plataformas como FFIEC IT operations booklet facilita un checklist útil para auditar procesos de rendimiento en los equipos, como también DoS Denial of Service es una guía que permite un plan de respuesta que sirven contra incidentes, denegando completamente el servicio.

A.12.1.2. No se considera gestión de cambios para la instalación y sistemas de procesamiento de información.	Importante	• Crear un manual de políticas y procedimientos claros y detallados de las reglas y regulaciones específicas relacionadas con la instalación y los sistemas de procedimientos e información. Esto debería incluir las políticas de seguridad, los requisitos técnicos y los procesos de instalación. • Comunicar las políticas claramente a todos los empleados y contratistas que trabajan en la empresa pública. Esto puede hacerse a través de capacitación y orientación, correos electrónicos regulares y lecturas obligatorias de manuales. • Implementar y hacer cumplir las políticas y los procedimientos en todo momento. Esto podría requerir la implementación de medidas disciplinarias para aquellos trabajadores o contratistas que violen las políticas. • Mantener el control de sus políticas y procedimientos y asegurarse de que se cumplan. Esto podría incluir la realización de auditorías regulares para revisar los procesos de instalación y los sistemas de procedimientos e información. • Actualizar constantemente las políticas para reflejar los cambios en la tecnología y los requisitos regulatorios. • Se puede usar FFIEC IT management booklet que se trata de una organización que explica cómo gestionar los riesgos cuanto es el costo si se llega a destruir un equipo informático y controlar los riesgos operativos.
A.12.3.1. No se realizan copias de seguridad de información de manera contante.	Muy grave	• Crear un plan de gestión de riesgos y amenazas a la seguridad de la información de la empresa. • Definir los procedimientos de copias de seguridad y recuperación de datos. • Definir las políticas y los procedimientos para realizar copias de seguridad y restaurar la información, establecer las frecuencias de las copias de seguridad y las personas responsables de realizarlas. • Capacitar a los empleados en la política de copia de seguridad, las frecuencias de las copias de seguridad, y cómo realizar las copias de seguridad de manera efectiva. • Verificar la realización de las copias de seguridad de forma periódica

		• Realizar pruebas de recuperación de datos de forma periódica para verificar que el procedimiento de recuperación sea eficaz y se puedan recuperar los datos perdidos. • Realizar auditorías regulares de la política de copias de seguridad, la realización de copias de seguridad y la recuperación de datos. • Establecer medidas disciplinarias a los empleados que no cumplan con las políticas y procedimientos sobre copias de seguridad. • Se puede usar Cobian backup que presenta procedimientos sobre software freeware para poder realizar backups de diferentes sistemas, es un programa multitareas que facilita generar copias de seguridad en los equipos de una red local como también en servidores FTP.
A.12.4.1. No se revisa periódicamente las actividades que realizan los usuarios.	Muy grave	• Educar a los usuarios sobre la importancia de la revisión periódica de las actividades que realizan y las consecuencias de no cumplir con las normas de la empresa. • Establecer un calendario de revisión a intervalos regulares en el que se realizará la revisión periódica de las actividades de los usuarios. Esto ayudará a los usuarios a planificar sus actividades y prepararse para la revisión. • Comunicar claramente a los usuarios la fecha, hora y lugar de la revisión periódica de sus actividades. También deben informar a los usuarios sobre los requisitos y documentación necesarios para la revisión. • Establecer sanciones para los usuarios que no cumplan con la normativa de la revisión periódica. Estas sanciones pueden incluir una multa, la suspensión temporal o permanente de los servicios de la empresa, o incluso la terminación del contrato. • Supervisar la revisión periódica de las actividades de los usuarios para asegurarse de que se siguen los procedimientos adecuados. Esto garantizará la integridad del proceso y la precisión de los resultados.

A.12.4.2. Protección de la información del registro.	Muy grave	• Se puede usar SAMHAIN se trata de un sistema de detección que aporta con la integridad de los archivos, ayudando también en la monitorización y escaneo de registros, es una herramienta que facilita el control de código malicioso, supervisión de puertos, detección de ejecutables, además proporciona el registro y mantenimiento centralizado. • Considera encriptar la información almacenada en el registro para agregar una capa adicional de seguridad. Esto garantizará que incluso si alguien obtiene acceso no autorizado a los datos, no podrá leerlos sin la clave de encriptación adecuada. • Monitoreo y registro de actividades: Implementa un sistema de monitoreo y registro de actividades en el registro. Esto te permitirá tener un registro detallado de quién accede a la información, qué acciones realizan y cuándo lo hacen. De esta manera, podrás detectar cualquier comportamiento sospechoso o malicioso y tomar medidas apropiadas. • Seguridad de red: Asegura que la red en la que se encuentra el registro esté protegida y segura. Implementa medidas como firewalls, controles de acceso a la red y detección de intrusiones para prevenir ataques externos y proteger la integridad de la información. • Mantén el software y los sistemas utilizados para administrar el registro actualizados con los últimos parches de seguridad. Esto ayudará a cerrar posibles vulnerabilidades y asegurar que estás utilizando las versiones más seguras de los sistemas. • Capacitación en seguridad: Proporciona capacitación regular sobre prácticas de seguridad a las personas que tienen acceso al registro. Esto incluye educar sobre temas como contraseñas robustas, autenticación de dos factores y cómo identificar intentos de phishing u otras amenazas de seguridad.

A.12.4.3. No existe revisiones periódicas sobre quien administra y opera los sistemas.	Muy grave	• Establecer políticas y procedimientos claros que describan las responsabilidades y requisitos necesarios para que los empleados que administren y operen los sistemas cumplan con la normativa de revisión periódica. • Comunicar las políticas y procedimientos a todos los empleados involucrados en la administración y operación de los sistemas para asegurarse de que comprendan las expectativas y las consecuencias en caso de incumplimiento de las normas. • Proporcionar la capacitación necesaria para que los empleados puedan cumplir adecuadamente con la normativa de revisión periódica. • Realizar revisiones periódicas de los sistemas administrados y operados por los empleados para asegurarse de que cumplen con las normas. Estas revisiones deben incluir la evaluación de los controles de seguridad, la integridad de los datos y la adecuada monitorización de los sistemas. • Identificar cualquier incumplimiento de la normativa de revisión periódica, la empresa debe tomar medidas disciplinarias según lo establecido en sus políticas y procedimientos. • Se puede utilizar SPLUNK es una herramienta que permite el monitoreo y análisis de datos masivos ya sea de redes, aplicaciones o equipos informáticos, permitiendo detectar incidentes de seguridad.
A.12.5.1. No se cuentan con directrices donde se hable de la correcta instalación y manejo de equipos y sistemas.	Importante	• Establecer la normativa y directrices claras y detallada sobre cómo se deben usar correctamente los equipos y sistemas informáticos en la empresa pública. También se deben establecer las directrices que los empleados deben seguir para garantizar el uso adecuado de los mismos. • Educar a los empleados sobre la normativa y directrices establecidas. Se puede hacer a través de capacitaciones, talleres o sesiones de entrenamiento. Es importante que los empleados entiendan por qué es importante seguir estas normas y cómo pueden garantizar que estén cumpliendo con ellas.

		• Implementar medidas de seguridad para garantizar que los equipos y sistemas informáticos estén protegidos. Se pueden implementar medidas como contraseñas seguras, cortafuegos, software de protección contra virus, entre otros. • Supervisar el cumplimiento de la normativas y directrices establecidas. • Realizar inspecciones regulares, monitoreo de la actividad del usuario y auditorías periódicas. Si se detecta una violación de la normativa, se deben tomar medidas inmediatas para corregirla. • Establecer consecuencias para el incumplimiento. Las consecuencias pueden incluir desde una advertencia hasta la terminación del contrato. • Se puede usar CIS que brinda un marco de protección en las herramientas como guías de uso de los servidores y aplicaciones.
A.12.6.1. No se actualiza las vulnerabilidades técnicas en los sistemas de información.	Muy grave	• Establecer un equipo de seguridad informática responsable de monitorear y actualizar constantemente las vulnerabilidades técnicas de los sistemas de información de la empresa. • Desarrollar una política de actualización de vulnerabilidades técnicas clara, completa y accesible para todos los empleados de la empresa pública. • Capacitar a todos los empleados de la empresa pública sobre la importancia de actualizar regularmente las vulnerabilidades técnicas en los sistemas de información y las consecuencias de no hacerlo. • Establecer un procedimiento claro para la identificación y gestión de las vulnerabilidades técnicas en los sistemas de información. • Establecer plazos y objetivos claros para la actualización de vulnerabilidades técnicas en los sistemas de información, y hacer que se cumplan. • Utilizar herramientas automáticas de detección de vulnerabilidades técnicas en los sistemas de información para agilizar el proceso de identificación y gestión de vulnerabilidades. • Realizar auditorías regulares para evaluar el cumplimiento de la política de actualización de vulnerabilidades técnicas en los sistemas de información de la empresa pública.

		• Establecer sanciones claras y proporcionales para aquellos empleados que no cumplan con la política de actualización de vulnerabilidades técnicas en los sistemas de información. • Promover una cultura de seguridad cibernética en la empresa pública que valore la importancia de la actualización de las vulnerabilidades técnicas en los sistemas de información y tome medidas concretas para asegurar la protección de la información de la empresa y de sus empleados. • Se puede usar Belarc Advisor que permite construir perfiles detallados del software y hardware instalados, inventario de red, parches faltantes para productos Microsoft, estado del antivirus y pruebas de seguridad, y muestra los resultados en el navegador. Toda la información del perfil es confidencial y nunca se envía al servidor web.
A.12.6.2. No se documenta como instalar sistemas o aplicaciones.	Importante	• Establecer políticas y procedimientos claros sobre cómo deben ser instalados los sistemas o aplicaciones. Estos deben incluir información sobre la configuración de hardware y software requeridos, así como los pasos necesarios para llevar a cabo la instalación. • Capacitar a la personal sobre implementación de normas y procedimientos de instalación. Esto garantiza que se sigan los procedimientos adecuados y se eviten errores costosos. • Realizar revisiones periódicas de los sistemas instalados para asegurarse de que se estén cumpliendo las normas de instalación y que los sistemas estén funcionando correctamente. • Monitorear el proceso de instalación para detectar y resolver rápidamente cualquier problema. • Establecer reglas de seguridad para evitar problemas de seguridad en el proceso de instalación. Esto incluye la necesidad de contraseñas seguras, el uso de firewalls y la actualización regular de software para prevenir vulnerabilidades. • Se puede usar GFI es una herramienta que brinda gestión de vulnerabilidades, auditoría de redes y software, inventario, gestión de cambios, análisis de riesgos y cumplimiento de normativas.
A.12.7.1. No se realiza auditorías de seguridad de la información.	Muy grave	• Definir políticas detalladas que delineé el alcance, objetivos y requisitos de la auditoría de seguridad de la información.

		• Crear un equipo de auditoría de seguridad de la información que se encargue de llevar a cabo las evaluaciones. • Establecer cronogramas de auditoría y cumplir los plazos de manera regular, para asegurar el cumplimiento de la política. • Establecer medidas de seguridad estándar para servidores, redes, software y hardware, y asegurarse de que se implementen adecuadamente. • Realizar capacitaciones para el personal sobre las políticas de seguridad de la información y los requerimientos de auditoría. • Evaluar regularmente la eficacia de la política y hacer cambios cuando sea necesario para asegurar la seguridad de la información de la empresa pública. • Aplicar consecuencias a aquellos empleados o terceros que incumplen los requisitos de seguridad de la información y las políticas de auditoría. Esto demostrará que la empresa se toma en serio la seguridad de la información y la política implementada. • Se puede usar la herramienta Center for Internet Security que puede ayudar con auditoria a los sistemas, Microsoft presenta un guía de planeamiento que permite la supervisión de seguridad y detección de ataques acerca de información general. • Usar DRADIS brinda informes muy importantes que servirán de ayuda para adquirir habilidades para comunicar sobre seguridad de la información. • Usar IT Audit Framework que describe estándares y mejores prácticas para iniciar procesos de auditoría.
A.13.1.1. No existe documentación donde garantice la seguridad de la información de las redes.	Muy grave	• Implementar controles que permitan administrar redes para proteger la información tanto en sistemas como en aplicaciones. • Se puede usar IPVoid que permite a los administradores escanear una dirección IP para proteger la detección de posibles IP que son peligrosas.

A.13.1.2 No existe mecanismos de seguridad.	Muy grave	• Utilizar SPICEWORKS también presenta una solución completa para la gestión y monitoreo de informes prácticos y dirigidos a empresas públicas o privadas. • Utilizar también TRASIR que brinda información para poder identificar direcciones IP, DNS, e-mail o link de páginas. • Realizar un análisis detallado de los riesgos que enfrenta la empresa en términos de seguridad de la información. Este análisis puede incluir la identificación de activos críticos, vulnerabilidades, amenazas y posibles consecuencias para la operación de la empresa. • Desarrollar políticas y procedimientos de seguridad de la información para la empresa. Estas políticas deben incluir la forma en que se gestionará, protegerá y mantendrá la información de la empresa, así como la forma en que se responderá a incidentes de seguridad. • Sensibilizar al personal de la empresa en cuanto a la seguridad de la información. Todos los empleados deben conocer las políticas y procedimientos de seguridad de la información de la empresa, cómo manejar los datos confidenciales, los pasos a seguir ante amenazas y cómo detectar ataques. • Implementar tecnología de seguridad de la información apropiada como software antivirus, firewalls, encriptación de datos, entre otras opciones. La elección de la tecnología dependerá de los resultados del análisis de riesgos y las políticas de seguridad de la empresa. • Evaluar y mejorar de manera continua y mantenerse en constante evolución. La empresa debe realizar evaluaciones regulares y actualizar sus medidas de seguridad para mantenerse en línea con los riesgos actuales. • Auditorías de seguridad periódicas son una forma imprescindible de verificar que se estén aplicando los procedimientos de seguridad como se ha establecido, y se estén cumpliendo los estándares que se han implementado. Estas auditorías nos darán información actualizada a cerca de la seguridad, y de la normativa y requisitos actuales que se deben cumplir para garantizar la protección de los datos de la empresa.

		• Se puede usar CyberGhost VPN que permite su instalación para evitar el robo de datos. Esta protección se realiza en dos etapas, empezando por el establecimiento de la conexión. La conexión se establece mediante cifrado SSL de 1024 bits y cada conexión recibe una clave AES única de 128 bits.
A.13.1.3. No cuenta con segregación de redes.	Muy grave	• Identificar los sistemas críticos y servicios que requieren mayor protección y aislamiento. • Elaborar políticas y procedimientos para el uso de la red, que aseguren la protección de los recursos y la privacidad de la información. • Separar las redes por función, según las funciones y niveles de seguridad requeridos. Las redes de uso público y las que contienen datos críticos deben estar separadas. • Implementar firewalls y filtros para controlar el acceso a la red y protegerla de intrusiones externas. • Configurar servicios de autenticación y autorización para controlar el acceso a cada segmento de la red. • Establecer políticas de acceso a la red, que definan quiénes pueden acceder a cada segmento y qué permisos tienen. • Supervisar y evaluar el tráfico de red y realizar auditorías de seguridad, para detectar cualquier actividad inusual y tomar medidas preventivas. • Capacitar al personal y los usuarios, para que conozcan los procedimientos de seguridad y sepan cómo actuar en caso de incidentes de seguridad. • Se puede usar IPVoid que permite analizar las direcciones IP utilizando varios mecanismos de reputación y listas negras para identificar direcciones IP potencialmente maliciosas.
A.13.2.1. No se tiene establecido políticas para proteger la información que se intercambia, copia o modifica.	Muy grave	• Establecer un protocolo de seguridad de la información que se aplicará en todos los niveles de la organización, incluyendo los empleados, socios y proveedores. • Realizar una evaluación de riesgos que permita identificar aquellos datos críticos que requieren una protección especial. De esta forma, se podrán desarrollar medidas específicas para proteger la información y mitigar los riesgos.

		• Establecer una política clara de contraseñas, que incluya la obligatoriedad de utilizar una contraseña segura, el cambio de esta en intervalos regulares y la prohibición de compartirla con terceros. • Restringir los datos de acceso en función del rol y la necesidad de los empleados. Es fundamental limitar el acceso a los datos críticos solo aquellos empleados que realmente necesiten acceder a ellos. • Implementar una política de clasificación de la información, de modo tal que se pueda establecer el nivel de acceso necesario en función de la información y su importancia. • Encriptar los datos, de esta forma, se dificulta el acceso no autorizado a la información y se evita la posibilidad de interceptación de la información por parte de actores malintencionados. • Mantener formación continua de los empleados en materia de seguridad de la información. Los empleados deben estar informados de los riesgos y de las mejores prácticas para proteger la información de la compañía. • Se puede usar ROHOS es una herramienta que permite crear particiones con cifrado en unidades USB flash, permite trabajar en un ordenador aun sin derechos administrativos, creando una partición protegida con estándares accesibles solo con la clave que se establezca.
A.13.2.2. No se notifica acciones delicadas.	Importante	• Establecer procedimientos de denuncia de irregularidades para los trabajadores de la empresa. • Establecer auditorías internas y externas para supervisar los procesos y proponer mejoras. • Proporcionar formación y recursos para que los empleados comprendan y sigan políticas y procedimientos éticos. • Garantizar la accesibilidad de la información para el público. • Fomentar la participación ciudadana a través de mecanismos como la audiencia pública y la respuesta a comentarios. • Se puede usar FOCA es una herramienta que permite la extracción de metadatos en documentación publica antes de iniciar con un envío enviará notificaciones sobre cómo se

		protege todos los documentos, los que deben validarse antes de pasar a los clientes a través de rutas ocultas, como metadatos y fugas de información ocultas en el documento, el módulo IIS 7 elimina los metadatos de los documentos de Office, por lo que, una vez instalado este módulo, se eliminarán los metadatos de todos los documentos que se hagan públicos a través del portal.
A.13.2.4. No cuenta con control en intercambio de información.	Importante	• Definir los objetivos de la política, como, por ejemplo, proteger los datos confidenciales de la empresa o garantizar la privacidad de los usuarios. • Identificar los posibles riesgos a los que se enfrenta la empresa al intercambiar información, como el riesgo de pérdida de datos o de robo de información confidencial. • Establecer las normas y reglas que los empleados y colaboradores deben seguir al intercambiar información, como, por ejemplo, no compartir información confidencial sin autorización previa o utilizar herramientas seguras para el intercambio de información. • Comunicar la política a todos los empleados y colaboradores, para que conozcan las normas y se sientan responsables de cumplirlas. • Capacitar al personal en el uso de herramientas seguras para el intercambio de información y en el cumplimiento de las normas establecidas en la política. • Monitorear y hacer cumplir la política para detectar posibles violaciones a la política y hacer cumplir las consecuencias establecidas en caso de infracciones. • Actualizar y evaluar la política de control de intercambio de información y evaluar su efectividad periódicamente para tomar acciones correctivas en caso de ser necesario. • Se puede usar Metashiel Protector dado que la información puede filtrarse a través de canales ocultos, como los metadatos y la información oculta en los documentos, tiene la opción de eliminar los metadatos de los documentos de Office, en cuanto instale este módulo, se eliminarán los metadatos de todos los documentos que estén a disposición del público a través del portal.
A.14.2.1. No se tiene políticas de desarrollo	Muy grave	• Implementar normas para el desarrollo de software y sistemas e implantarlas en su organización. • Efectuar técnicas de programación seguras.

seguro para aplicaciones o sistemas.		• Utilizar técnicas de reutilización de código porque las normas aplicables al desarrollo no se conocen o no son coherentes con las prácticas recomendadas actuales • Realizar capacitaciones en beneficiario para desarrollo interno y externo. • Se puede usar Signal una herramienta de código abierto que facilita la comunicación mediante llamadas y mensajería segura con la finalidad de comunicarse con desarrolladores o personas que ayuden con el desarrollo de sistemas.
A.14.2.2. No cuenta con un plan de cambios en sistemas o aplicaciones.	Muy grave	• Identificar las áreas de la empresa que necesitan ser mejoradas • Identificar los problemas específicos que se deben solucionar • Analizar los sistemas y aplicaciones actuales y determinar cuáles no funcionan bien y cuáles necesitan ser mejorados • Identificar las metas y objetivos del plan de cambios • Desarrollar políticas en torno a los sistemas y aplicaciones, como políticas de seguridad, privacidad y cumplimiento regulatorio • Establecer un equipo de gestión de cambios y un plan de implementación detallado • Asegurarse de que la capacitación adecuada se proporcione a los empleados afectados • Realizar pruebas antes de implementar los cambios en producción • Monitorear la implementación del plan de cambios y realizar ajustes según sea necesario • Evaluar el éxito del plan de cambios una vez que se haya implementado por completo. • Usar CVS que es una herramienta que facilita manuales que hablan sobre el control de versiones de software y permite el desarrollo adecuado de manera segura y eficaz.
A.14.2.3. No existe revisiones al momento de emplear un sistema.	Muy grave	• Crear una política clara y detallada que explique cuándo y cómo se deben realizar las revisiones al sistema. • Comunicar la política de revisiones a todos los empleados que usarán el sistema. Esto se puede hacer a través de reuniones, correos electrónicos y manuales de usuario.

A.14.2.6. No cuentan con entornos de desarrollo seguros.	Muy grave	• Establecer los procedimientos necesarios para llevar a cabo las revisiones. Esto incluye la selección de empleados encargados de realizar las revisiones, la frecuencia de las revisiones, los criterios de evaluación y los informes de seguimiento. • Capacitar a los empleados para que sepan cómo realizar las revisiones y para que entiendan la importancia de la política de revisiones. • Evaluar regularmente el sistema para asegurarse de que cumple con los estándares de calidad y seguridad establecidos. También se deben tener en cuenta las sugerencias de los empleados para mejorar el sistema. • Monitorear el cumplimiento de la política de revisiones para asegurarse de que se está llevando a cabo como se ha establecido. Si se detectan problemas, se deben tomar medidas para solucionarlos y garantizar que no vuelvan a ocurrir. • Actualizar la política regularmente para reflejar los cambios en el sistema o en los procedimientos de revisión. • Se puede usar Burpsuite se utiliza habitualmente para probar aplicaciones web. Está escrito en Java y funciona conjuntamente con PortSwigger que proporciona una interfaz gráfica de usuario con muchas funciones y herramientas útiles en todas las fases, incluidas las intrusiones. • Utilizar herramientas de seguridad como antivirus, firewalls, y sistemas de detección de intrusiones que pueden ayudar a detectar y prevenir ataques cibernéticos. • Garantizar la seguridad física en los entornos de desarrollo es esencial para evitar la pérdida o robo de información. Se deben implementar medidas de seguridad como la utilización de cámaras de seguridad, controles de acceso, y monitoreo de las áreas de trabajo. • Garantizar que solo los usuarios autorizados tengan acceso a la información crítica. Esto se puede lograr implementando sistemas de autenticación y autorización, y utilizando contraseñas robustas. • Monitorear los sistemas y las actividades de los usuarios para detectar posibles riesgos o amenazas. La detección temprana puede evitar daños mayores.

A.14.2.8 Pruebas funcionales de seguridad de sistemas.	Muy grave	• Educar a los empleados sobre las medidas de seguridad y los protocolos a seguir en el entorno de desarrollo para minimizar la posibilidad de errores humanos, que pueden ser tan perjudiciales como los ataques cibernéticos. • Mantener actualizados los sistemas y aplicaciones es esencial para evitar vulnerabilidades de seguridad. Se deben aplicar parches y actualizaciones regularmente para reducir el riesgo de exposición a riesgos cibernéticos. • Evaluar de manera periódica de la seguridad y la eficacia de las políticas y prácticas actuales para mejorar y adaptar dichas políticas • Se puede usar OllyDbg es una herramienta de análisis de código que beneficia a pesar de que el código fuente no se encuentre disponible. • Definir el alcance: Determina el alcance de las pruebas de seguridad funcionales que deseas realizar. Identifica los sistemas o componentes que serán evaluados y las funcionalidades específicas que se someterán a prueba. • Identificar requisitos de seguridad: Analiza los requisitos de seguridad relevantes para el sistema en cuestión. Esto te ayudará a identificar los aspectos clave que deben ser evaluados durante las pruebas. • Diseñar casos de prueba: Crea casos de prueba detallados que aborden tanto la funcionalidad general como los aspectos de seguridad específicos del sistema. Asegúrate de cubrir diferentes escenarios y riesgos potenciales. • Ejecutar pruebas: Lleva a cabo las pruebas siguiendo los casos de prueba diseñados. Realiza pruebas técnicas que pongan a prueba la seguridad del sistema, como la verificación de la autenticación, la autorización adecuada y la protección contra ataques comunes, como la inyección de código maligno.

A.14.2.9. Los sistemas no se mantienen actualizados a nuevas versiones.	Muy grave	• Registrar resultados y analizar: Documenta los resultados de las pruebas y analiza los hallazgos. Identifica cualquier vulnerabilidad o debilidad encontrada y evalúa su impacto potencial. Clasifica los problemas según su gravedad y prioridad. • Mitigar riesgos: Desarrolla un plan de acción para abordar los problemas de seguridad identificados. Esto puede implicar la implementación de medidas de seguridad adicionales, como parches, actualizaciones de software, mejoras en la autenticación o cambios en la configuración del sistema. • Realizar pruebas de regresión: Después de implementar las medidas de mitigación, vuelve a ejecutar las pruebas para asegurarte de que los problemas identificados se hayan resuelto correctamente y de que no se hayan introducido nuevas vulnerabilidades. • Monitorear de manera continua: Establece un monitoreo continuo de la seguridad del sistema para detectar y responder rápidamente a nuevas amenazas y vulnerabilidades. Esto puede incluir la implementación de herramientas de detección de intrusiones y el establecimiento de procedimientos para la gestión de incidentes de seguridad. • Establecer un programa regular de actualización de software y los sistemas con regularidad. Esto puede incluir la definición de fechas límite para las actualizaciones y la creación de un calendario de actualizaciones. • Realizar una evaluación de riesgos asociados con la actualización. Se deben evaluar los posibles riesgos de seguridad, la compatibilidad del software y los problemas de rendimiento. • Implementar parches de seguridad para mantener la seguridad de los sistemas. Estos parches corrigen vulnerabilidades del software que pueden ser explotadas por los ciberdelincuentes. • Establecer una política de respaldo. Para garantizar que los datos estén seguros y se puedan recuperar en caso de un fallo, es importante tener una política de respaldo confiable y regular. • Capacitar al personal sobre cómo realizar actualizaciones de software y cómo detectar y corregir errores. Esto puede reducir la necesidad de asistencia técnica y evitar errores costosos.

		• Realizar pruebas de integración para garantizar que las actualizaciones de software funcionen correctamente con los sistemas existentes. • Monitorear el sistema en busca de problemas. Esto puede ayudar a detectar problemas antes de que se conviertan en un problema grave. • Se puede usar OSC Inventory NG que permite comprobar e inventariar todo el hardware de su departamento informático, una vez que tenga toda la información necesaria sobre el hardware y el software, puede utilizar paquetes de software para proteger su entorno. Existen muchos que le ayudarán a personalizar el inventario de OCS para adecuar a un sistema.
A.14.3.1. Los datos de prueba no son protegidos.	Muy grave	• Identificar y clasificar los datos de prueba por su nivel de confidencialidad. • Implementar restricciones para evitar que los datos de prueba sean accedidos por personas no autorizadas. • Identificar datos de prueba para evitar que la información de identificación personal se revele accidentalmente. • Realizar pruebas en entornos seguros para evitar que los datos de prueba se filtren o se revelen públicamente. • Eliminar los datos de prueba cuando ya no se necesitan, esto garantizará que los datos confidenciales no se queden sin protección • Se puede usar FFIEC presenta manuales y folletos sonde describen el riesgo basados en programas y como tratarlos.
A.16.1.1. No se brinda respuesta a los incidentes de seguridad.	Muy grave	• Identificar qué constituye un incidente de seguridad, ya que esto permitirá tener un criterio compartido a nivel organizacional y tomar medidas de manera oportuna.

A.16.1.2. No se notifica fallos de seguridad.	Muy grave	• Formar un equipo de respuesta a incidentes, este equipo debe contar con personas capacitadas en análisis forenses, administración de sistemas y redes, gestión de crisis y comunicación. • Establecer un plan de contingencia y protocolos específicos para diferentes tipos de incidentes. • Establecer roles y responsabilidades en caso de un incidente de seguridad. También se debe establecer una cadena de mando y cómo se comunicarán las decisiones y acciones. • Definir niveles de gravedad y prioridad tomar en cuenta qué medidas se deben tomar en cada caso. Esto permitirá que el equipo de respuesta pueda actuar de manera adecuada teniendo en cuenta los riesgos involucrados. • Documentar todo el proceso, las acciones tomadas en respuesta a un incidente deben ser documentadas de forma detallada. Esto permitirá una mejor evaluación posterior del incidente y la implementación de medidas preventivas para evitar futuros incidentes similares. • Hacer pruebas y simulaciones de incidentes: Es importante realizar pruebas de forma periódica para verificar la efectividad del plan de respuesta y detectar posibles brechas. También se pueden realizar simulaciones de incidentes para entrenar al equipo de respuesta y evaluar su capacidad de tomar decisiones y actuar en situaciones de crisis. • Evaluar y mejorar constantemente, después de cada incidente, se debe realizar una evaluación detallada de los aspectos positivos y negativos del proceso de respuesta. Esto permitirá identificar áreas de mejora y hacer ajustes en el plan de respuesta y en las políticas implementadas para brindar respuestas a incidentes de seguridad. • Se puede usar ENISA muestra una guía completa de buenas prácticas para la gestión de incidentes que tienen que ver con seguridad de red y de la información. • Definir los canales de notificación que se utilizarán para reportar los fallos de seguridad, tales como correo electrónico o un formulario en línea.

A.16.1.3. No existe un mecanismo de notificación para los administrativos.	Muy grave	• Definir un procedimiento claro y detallado para notificar los fallos de seguridad de forma efectiva y segura. Este procedimiento debe incluir los requisitos que debe cumplir el reporte de fallo, los plazos de respuesta y la manera de comunicación con los informantes. • Designar un equipo de respuesta de seguridad es el encargado de gestionar las notificaciones de fallos de seguridad. Debe estar conformado por especialistas en seguridad informática y otros profesionales que sean capaces de analizar y solucionar los fallos reportados. • Establecer los niveles de prioridad de los fallos reportados, con el fin de definir la urgencia de la solución, de acuerdo con la magnitud del problema y su impacto en el sistema. • Garantizar que su identidad y los detalles del fallo reportado serán tratados con confidencialidad, y que sólo se utilizarán para resolver el problema. • Establecer un plan de seguimiento para verificar que la solución fue efectiva y que no quedaron problemas pendientes. • Capacitar al personal en cuanto al procedimiento de notificación de fallos de seguridad y el manejo de la información confidencial, así como en las mejores prácticas de seguridad informática para prevenir la aparición de nuevos fallos. • Se puede usar ENISA presenta una interfaz confiable donde cuenta con información de escenarios cibernéticos permitiendo respuestas tempranas a un accidente y procesos a seguir. • Determinar qué información es crítica para el funcionamiento adecuado de la organización y establecer qué procesos y sistemas se encargan de recopilar y monitorear dicha información. • Designar a uno o varios empleados responsables de supervisar el monitoreo de la información y notificar a los administrativos en caso de que se detecte un problema. • Establecer indicadores que permitan detectar fallos o inconsistencias en la información de manera temprana. Estos indicadores pueden ser numéricos, como umbral de valores críticos, o pueden ser basados en patrones de comportamiento inusual.

		• Establecer un protocolo de notificación claro y específico sobre cómo se va a notificar a los administrativos en caso de identificar un fallo o una inconsistencia en la información. El protocolo debe incluir detalles como el formato de la notificación, la frecuencia de la notificación y el grado de urgencia. • Realizar pruebas periódicas para evaluar la eficacia del protocolo de notificación. De esta manera, se pueden identificar oportunidades de mejora y ajustar la normativa según las necesidades de la organización. • Se puede utilizar NIST con documentos que aportan con respuestas de gestión a tomar en caso de incidentes de seguridad que ocurran en la organización.
A.16.1.4. Los eventos no son evaluados según una escala de importancia.	Importantes	• Evaluar cuáles son las características fundamentales que definen la importancia de un evento. Esto puede incluir el impacto económico, el riesgo para la seguridad, la repercusión en la reputación de la organización, el nivel de atención mediática, entre otros. • Establecer una escala de valor que defina la jerarquía de importancia de los eventos de acuerdo a los criterios definidos anteriormente. Esta escala puede ser numérica, como del 1 al 5, o utilizar una codificación por colores o letras. • Definir los procedimientos de evaluación necesarios para evaluar los eventos y determinar su importancia. Esto puede incluir la designación de un equipo de evaluación, la recopilación de datos y la identificación de los efectos secundarios. • Implementar las políticas, esto puede requerir hacer ajustes y modificaciones según la situación. • Revisar y ajustar las políticas según sea necesario para asegurarse de que sigan siendo efectivas. Esto puede incluir la actualización de los criterios, la revisión de la escala de valor y la adaptación de los procedimientos de evaluación. • Se puede tomar en cuenta AVG Rescue es un tipo de herramienta que facilita salvar a los equipos si existe algún tipo de inconvenientes donde se infecten.

A.16.1.5. No se evalúan los eventos de manera frecuente.	Muy grave	• Definir una frecuencia para las evaluaciones y establecer un calendario para llevarlas a cabo. Por ejemplo, trimestralmente, semestralmente o anualmente. • Definir los objetivos específicos que se espera alcanzar con la misma. Esto permitirá medir con precisión el éxito de la evaluación. • Identificar los indicadores que permitirán medir el desempeño y el impacto del evento. Estos deben ser relevante y cuantificables. • Formar un equipo encargado de llevar a cabo las evaluaciones. Este equipo debe estar compuesto por personas capacitadas en el área a evaluar y tener un enfoque objetivo e imparcial. • Recopilar datos relevantes para la evaluación. Esto puede incluir registros de asistencia, encuestas de satisfacción, comentarios de los participantes, información financiera, entre otros. • Analizar de manera objetiva para obtener conclusiones claras y precisas sobre el éxito del evento. Se debe prestar especial atención a los indicadores clave identificados previamente. • Tomar medidas para mejorar y optimizar el evento en el futuro. Esto podría incluir ajustes en el formato, el contenido, los horarios, la ubicación, entre otros aspectos relevantes. • Comunicar los resultados de la evaluación a todas las partes interesadas, incluyendo al equipo organizador, los patrocinadores, los asistentes, entre otros. Esto permitirá que todos los involucrados entiendan el impacto del evento y se pueda trabajar para mejorarlo en el futuro. • Se puede usar BSI se trata de una práctica que permite la gestión de operaciones hacia dispositivos de atención y vigilancia. • Utilizar 101 utilidades forenses que trata de un blog que puede ayudar a verificar casos de utilidades para poder salvaguardar un fallo y cómo actuar ante esta situación.
A.17.1.2. No existe documento que informe	Muy grave	• Definir cómo la organización recuperará sus operaciones después de una interrupción. • Establecer objetivos de tiempo de recuperación para cada uno de los sistemas críticos de la organización.

sobre un plan de continuidad.		• Definir los procedimientos para la gestión de contingencias, incluyendo la identificación y evaluación de riesgos, la planificación de contingencias y la implementación de medidas de mitigación. • Definir los procedimientos para la realización de copias de seguridad regulares de los datos críticos de la organización. También puede incluir procedimientos para la recuperación de datos y la prueba de los sistemas de respaldo. • Establecer requisitos de redundancia para garantizar la disponibilidad continua. • Definir los requisitos de entrenamiento para el personal involucrado en la implementación del plan de continuidad. También establece los procedimientos para la realización de pruebas regulares del plan de continuidad para garantizar su eficacia en situaciones de emergencia. • Establecer procedimientos para la revisión y mejora continua del plan de continuidad. Incluye la evaluación de los resultados de las pruebas y la identificación de oportunidades de mejora para garantizar la continuidad y la eficacia del plan. • Se puede utilizar BSI 100-4 proporciona métodos que facilitan la continuidad de una organización a pesar de que haya tenido inconvenientes en su sistema ayuda a desarrollar, establecer y sobre todo mantener sistemas mediante el empleo de ISO 22301, ISO 27001, ISO 20000 y otros marcos que proporcionen ayuda.
A.17.2.1. No existe disponibilidad de instalaciones de procesamiento para la seguridad de información.	Importante	• Identificar los requisitos de disponibilidad e instalaciones necesarias para procesar la información. • Establecer objetivos claros para la política de disponibilidad e instalaciones. • Diseñar cuidadosamente para asegurar que los objetivos sean logrados. • Comunicarla a todas las partes interesadas, incluyendo el personal, los proveedores y los clientes. • Implementar la política de disponibilidad e instalaciones debe ser cuidadosamente planificada para asegurar que se logren los objetivos y se minimice el impacto en la operación diaria. • Monitorear su desempeño y evaluar los resultados para hacer ajustes si es necesario. • Asegurar que se cumpla con las necesidades cambiantes de la organización.

A.18.1.4. No garantiza la protección y la privacidad de la información de quien la administra.	Muy grave	• Se puede utilizar DRI que proporciona manuales de buenas prácticas que permiten planificar la gestión de continuidad de una organización. • Identificar los tipos de información que se manejan en la organización, ya sea personal, financiera, de negocios, entre otros. • Establecer políticas claras que indiquen qué información se puede compartir y con quién. Es importante que se establezcan sanciones en caso de incumplimiento. • Definir roles de cada persona en la organización y asignar responsabilidades específicas en cuanto a la protección y privacidad de la información. • Capacitar sobre la privacidad de la información y los procesos necesarios para protegerla. También se pueden realizar simulaciones de situaciones de riesgo para que los colaboradores estén preparados para actuar en caso de emergencia. • Actualizar periódicamente en función de los cambios en la organización y los avances tecnológicos. • Implementar medidas de seguridad tecnológicas, físicas y operativas para proteger la información como contraseñas, firewalls, antivirus, backup, entre otros. • Hacer seguimiento del cumplimiento de las políticas y tomar medidas en caso de incumplimiento. También se pueden realizar auditorías internas o externas para evaluar el nivel de cumplimiento. • Se puede ingresar a Agencia Española de protección de datos se trata de información acerca de cómo se resguarda la información que es privada de los individuos. • Se puede revisar información en el centro de protección de las infraestructuras críticas tiene como objetivo principal facilitar manuales que permiten mantener la infraestructura de manera segura. • Se muestra información en RED IBEROAMPERICA DE PROTECCIÓN DE DATOS es una red que nace con el motivo de brindar asistencia a la protección de los datos desde un portal que da información a los países que lo requieren.

A.18.1.5. No se cuenta con criptografía al momento de importar o exportar software.	Muy grave	• Determinar cuáles son los datos que se consideran confidenciales y que requieren ser protegidos. • Selección de algoritmos de cifrado adecuados que se utilizarán para proteger los datos. Es importante seleccionar algoritmos que sean seguros y que estén en línea con los estándares de seguridad actuales. • Configuración de las claves de cifrado, en este paso, se deben definir las claves de cifrado, asegurándose de que sean lo suficientemente fuertes y difíciles de adivinar. • Implementar el cifrado en el software • Realizar pruebas de seguridad para garantizar que los datos se estén protegiendo adecuadamente. Las pruebas pueden involucrar técnicas como el análisis de vulnerabilidades y la simulación de ataques. • Obtener una certificación de seguridad de un tercero de confianza para garantizar que el software cumpla con los estándares de seguridad requeridos. Esto puede incluir certificaciones como ISO/IEC 27001. • Se puede ingresar a AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS es una herramienta que permite solucionar inconvenientes de los datos y facilita documentación donde indica los recursos y las policías para cumplir. • Se puede utilizar Security Breaches escrito en cuatro idiomas permite abrir conversatorios o noticias actualizadas sobre leyes a emplear o actualización de las mismas, para mejorar la protección y suplantación de identidad en los ordenadores.

Mitigación de Normas del control interno de la contraloría general del estado

Tabla 14. Validación de controles 410 Tecnología de la información

Situación de riesgo	Riesgo	Estrategias de mitigación
410- 01 Organización informática	Apreciable	• Realizar una evaluación exhaustiva de los riesgos potenciales que enfrenta la organización informática. Identificar las vulnerabilidades y amenazas específicas a las que se puede enfrentar. • Asegurarse de que los activos físicos, como servidores o equipos de red, estén protegidos adecuadamente contra robos, incendios u otros daños físicos. • Definir y comunicar claramente las políticas de seguridad de la organización. Esto incluye el uso de contraseñas seguras, el acceso restringido a ciertos datos y la prohibición del uso de dispositivos no autorizados. • Utilizar software y sistemas operativos actualizados con las últimas correcciones de seguridad. Esto ayuda a evitar vulnerabilidades conocidas que podrían ser explotadas por hackers. • Realizar copias de seguridad de manera regular y almacenarlas en un lugar seguro. Esto asegura que los datos puedan ser recuperados en caso de un incidente o pérdida de datos. • Configurar y mantener activos los cortafuegos y sistemas de detección de intrusiones para prevenir y detectar cualquier intento de acceso no autorizado. • Proporcionar formación continua sobre seguridad informática a todo el personal. Esto incluye la concientización sobre phishing, uso seguro de contraseñas y otras prácticas de seguridad. • Realizar pruebas de penetración regularmente para identificar puntos débiles en la infraestructura y los sistemas. Esto permite tomar medidas proactivas para fortalecer la seguridad. • Estar al tanto de las actualizaciones y parches de seguridad lanzados por los proveedores de software y aplicarlos de manera oportuna.
410-02 Segregación de funciones	Muy grave	• Identifique todas las funciones y responsabilidades dentro de su organización que están relacionadas con la segregación de funciones.

		• Realice una evaluación exhaustiva de los riesgos asociados con la falta de segregación de funciones en su organización. • Desarrolle pautas claras y específicas sobre cómo se deben asignar las funciones y responsabilidades para garantizar una segregación adecuada. • Establezca controles internos efectivos, como revisiones y aprobaciones independientes, para garantizar que las funciones estén segregadas correctamente. • Realice monitoreo continuo y auditorías periódicas para asegurarse de que se esté cumpliendo la segregación de funciones y de que los controles internos estén funcionando correctamente. • Es recomendable buscar asesoramiento profesional o consultar las regulaciones y mejores prácticas relevantes en su industria.
410- 03 Planes para mejora	Muy grave	• Realice una evaluación exhaustiva de los posibles riesgos asociados con la implementación de planes de mejora en su organización. • Clasifique los riesgos identificados según su nivel de impacto y probabilidad de ocurrencia. • Desarrolle estrategias específicas para mitigar cada riesgo identificado. Estas estrategias pueden incluir acciones preventivas, controles adicionales o ajustes en el plan de mejora. • Ponga en práctica las estrategias desarrolladas, asegurándose de asignar responsabilidades claras y proporcionar los recursos necesarios. • Realice un seguimiento regular de la implementación de las estrategias de mitigación y evalúe su efectividad para reducir los riesgos identificados. Ajuste las estrategias según sea necesario. • Comunique a todos los involucrados sobre los riesgos identificados y las estrategias de mitigación implementadas. Proporcione capacitación adecuada para garantizar que todos comprendan sus roles y responsabilidades.
410- 04 Políticas y procedimientos	Muy grave	• Realice una evaluación exhaustiva de los posibles riesgos relacionados con las políticas y procedimientos existentes en su organización.

410-05 Modelo de información	Muy grave	• Clasifique los riesgos identificados según su nivel de impacto y probabilidad de ocurrencia. Esto le permitirá priorizar los riesgos más significativos y asignar recursos adecuados para su mitigación. • Desarrolle medidas de control específicas para cada riesgo identificado. Estas pueden incluir la revisión y actualización de políticas y procedimientos, la implementación de controles adicionales o la capacitación del personal. • Ponga en práctica las medidas de control desarrolladas, asegurándose de asignar responsabilidades claras y proporcionar los recursos necesarios. Esto puede implicar la actualización de documentos, la comunicación y capacitación del personal, y el establecimiento de mecanismos de seguimiento y cumplimiento. • Realice un seguimiento regular de la implementación de las medidas de control y evalúe su efectividad para mitigar los riesgos identificados. Ajuste las medidas según sea necesario para garantizar su eficacia a lo largo del tiempo. • Realice revisiones periódicas de las políticas y procedimientos existentes para identificar nuevas áreas de riesgo o mejoras potenciales. Incorpore las lecciones aprendidas de incidentes anteriores y las mejores prácticas de la industria. • Realice una evaluación exhaustiva de los posibles riesgos asociados con los modelos de información utilizados en su organización. Esto puede incluir riesgos como la falta de precisión, la falta de integridad de los datos o la vulnerabilidad a ataques cibernéticos. • Clasifique los riesgos identificados según su nivel de impacto y probabilidad de ocurrencia. Esto le permitirá priorizar los riesgos más significativos y asignar recursos adecuados para su mitigación. • Desarrolle medidas de control específicas para cada riesgo identificado. Estas pueden incluir la implementación de controles de calidad de datos, la adopción de buenas prácticas de modelado, la implementación de medidas de seguridad cibernética y la realización de pruebas y validaciones periódicas.

		• Ponga en práctica las medidas de control desarrolladas, asegurándose de asignar responsabilidades claras y proporcionar los recursos necesarios. Esto puede implicar la revisión y actualización de los modelos de información, la capacitación del personal y la implementación de tecnologías y herramientas de seguridad adecuadas. • Realice un seguimiento regular de la implementación de las medidas de control y evalúe su efectividad para mitigar los riesgos identificados. Monitoree la calidad de los datos utilizados en los modelos, realice auditorías de seguridad cibernética y realice revisiones periódicas de los modelos de información para identificar posibles mejoras. • Realice revisiones periódicas de los modelos de información para identificar nuevas áreas de riesgo o mejoras potenciales. Incorpore las lecciones aprendidas de incidentes anteriores y las mejores prácticas de la industria. Manténgase actualizado con los avances tecnológicos y las regulaciones pertinentes que puedan afectar a los modelos de información
410-06 Administración de proyectos tecnológicos	Importante	• Definir claramente los objetivos y alcance del proyecto tecnológico. • Establecer un plan de proyecto detallado que incluya todas las tareas, plazos y recursos necesarios. • Asignar roles y responsabilidades claras a los miembros del equipo de proyecto. • Establecer un sistema de comunicación efectivo para mantener a todos los miembros del equipo informados sobre el progreso del proyecto. • Realizar un seguimiento regular del progreso del proyecto y realizar ajustes según sea necesario. • Identificar y gestionar los riesgos potenciales del proyecto, desarrollando planes de contingencia en caso de que ocurran. • Establecer métricas y criterios de éxito para evaluar el rendimiento del proyecto. • Fomentar la colaboración y el trabajo en equipo entre los miembros del equipo de proyecto. • Utilizar herramientas y tecnologías adecuadas para facilitar la gestión del proyecto. • Realizar una evaluación final del proyecto para identificar lecciones aprendidas y áreas de mejora para futuros proyectos tecnológicos.

410-07 Desarrollo y adquisición de software aplicativo	Muy grave	• Realizar un análisis exhaustivo de los requisitos y necesidades del software aplicativo antes de iniciar el desarrollo o adquisición. Esto ayudará a asegurar que el software cumpla con las expectativas y requerimientos del proyecto. • Establecer un proceso de selección riguroso para elegir el proveedor o equipo de desarrollo adecuado. Esto puede incluir la revisión de su experiencia, referencias y capacidad para cumplir con los plazos y presupuesto establecidos. • Establecer un contrato claro y detallado que especifique los entregables, plazos, costos y cualquier otro aspecto relevante del proyecto. Esto ayudará a evitar malentendidos y conflictos durante el desarrollo o adquisición del software. • Realizar pruebas exhaustivas del software durante el proceso de desarrollo o adquisición. Esto incluye pruebas de funcionalidad, rendimiento, seguridad y usabilidad. Las pruebas deben ser realizadas tanto por el proveedor o equipo de desarrollo como por el cliente o usuario final. • Establecer un proceso de revisión y aprobación de los entregables del software. Esto asegurará que el software cumpla con los estándares y requisitos establecidos antes de su implementación. • Establecer un plan de capacitación y formación para los usuarios finales del software. Esto ayudará a asegurar que los usuarios estén familiarizados y puedan utilizar eficientemente el software una vez implementado. • Establecer un plan de mantenimiento y soporte post-implementación del software. Esto incluye la resolución de problemas, actualizaciones y mejoras continuas del software para garantizar su funcionamiento óptimo a lo largo del tiempo. • Realizar una evaluación de impacto del software una vez implementado. Esto ayudará a identificar los beneficios y resultados obtenidos, así como posibles áreas de mejora para futuros proyectos de desarrollo o adquisición de software.
410-08 Adquisición de infraestructura tecnológica	Muy grave	• Realiza una planificación exhaustiva antes de iniciar el proyecto. Define claramente los objetivos, scope, entregables y plazos. Identifica los riesgos potenciales y elabora estrategias de mitigación.

		• Asegúrate de tener los recursos necesarios, tanto humanos como técnicos, para llevar a cabo el proyecto. Evalúa las habilidades y capacidades del equipo y asigna roles y responsabilidades de manera adecuada. • Establece canales de comunicación claros y abiertos con todos los miembros del equipo y las partes interesadas. Programa reuniones regulares para mantener a todos actualizados sobre el progreso del proyecto y abordar cualquier problema o preocupación. • Realiza un análisis de riesgos exhaustivo al comienzo del proyecto y establece medidas preventivas y de contingencia. Monitorea de cerca los riesgos durante todo el ciclo de vida del proyecto y toma acciones correctivas según sea necesario. • Establece métricas de rendimiento claras y realiza un seguimiento regular del progreso del proyecto. Utiliza herramientas de gestión de proyectos para monitorear las tareas, el tiempo y el presupuesto. Si es necesario, realiza ajustes al plan para asegurar que el proyecto se mantenga en el camino correcto.
410-09 Mantenimiento y control de la infraestructura tecnología	Importante	• Comienza por hacer un inventario exhaustivo de todos los componentes de la infraestructura tecnológica, como servidores, equipos de red, sistemas de almacenamiento, etc. Esto te ayudará a tener un panorama claro de lo que necesitas mantener y controlar. • Define políticas y procedimientos claros para el mantenimiento y control de la infraestructura tecnológica. Estas políticas deben abordar aspectos como las actualizaciones de software, los procedimientos de respaldo y recuperación de datos, la seguridad de la red, entre otros. • Establece un calendario para llevar a cabo mantenimientos regulares en la infraestructura tecnológica. Esto incluye tareas como la limpieza física de los equipos, la verificación de cables y conexiones, la actualización de software y firmware, y la optimización de la configuración. • Asegúrate de realizar copias de seguridad periódicas de los datos críticos almacenados en la infraestructura tecnológica. Esto te permitirá recuperar la información en caso de pérdida o fallos del sistema.

		• Utiliza herramientas de monitoreo y supervisión para evaluar el rendimiento de la infraestructura tecnológica. Esto te ayudará a identificar posibles problemas y tomar medidas correctivas de manera proactiva. • Mantén todos los sistemas y componentes de la infraestructura tecnológica actualizados con las últimas versiones de software y firmware. Esto te permitirá beneficiarte de mejoras en cuanto a seguridad, rendimiento y funcionalidad.
410- 10 Seguridad de la tecnología de información	Muy grave	• Realiza una evaluación completa de los riesgos de seguridad de la tecnología de información en tu organización. Esto implica identificar los posibles puntos débiles y las amenazas involucradas. • Implementa políticas de seguridad claras y efectivas que aborden diferentes aspectos, como el acceso a la información, el uso de contraseñas seguras, el cifrado de datos y la gestión de dispositivos. • Brinda regularmente capacitación y concientización en seguridad de la tecnología de información a todos los empleados de tu organización. Esto incluye educar sobre las mejores prácticas para la protección de datos, la identificación de ataques de phishing y la seguridad en el uso de dispositivos. • Adopta medidas de seguridad técnicas adecuadas, como el uso de firewalls, antivirus y software de detección de intrusiones. También es importante mantener el software y los sistemas actualizados con los últimos parches de seguridad. • Establece controles de acceso apropiados y limita los privilegios de los usuarios para reducir el riesgo de accesos no autorizados a la información confidencial. • Realiza copias de seguridad regulares de los datos importantes y almacénalos en un lugar seguro. Esto ayudará a recuperar la información en caso de pérdida o daño de los datos. • Implementa sistemas de monitoreo de seguridad para detectar y responder rápidamente a cualquier actividad sospechosa o irregular en los sistemas de tecnología de información. • Al seleccionar proveedores externos para servicios de tecnología de información, evalúa cuidadosamente sus medidas de seguridad y su cumplimiento con las regulaciones de seguridad pertinentes.

410-11 Plan de contingencia	Muy grave	• Elabora y prueba un plan de respuesta ante incidentes para abordar cualquier brecha de seguridad o violación de datos de manera efectiva y mitigar los impactos negativos. • Realiza auditorías periódicas para evaluar y mejorar continuamente la seguridad de la tecnología de información en tu organización. Esto ayudará a identificar áreas de mejora y garantizar el cumplimiento de las políticas y normas de seguridad establecidas. • Realiza una evaluación exhaustiva de las posibles amenazas y riesgos que podrían afectar a tu organización, como desastres naturales, fallas en los sistemas, ciberataques, entre otros. • Determina cuáles son las funciones y activos críticos para el funcionamiento de tu organización. Estos deben ser identificados como prioridades en caso de contingencia. • Crea un plan de contingencia detallado que incluya acciones a seguir en caso de diferentes escenarios de emergencia. Este plan debe incluir personas responsables, recursos necesarios, acciones específicas a tomar y una comunicación clara. • Lleva a cabo simulacros de contingencia para evaluar la efectividad de tu plan y realizar mejoras si es necesario. Esto ayudará a familiarizar al personal con las acciones a tomar y a identificar posibles brechas o debilidades. • El plan de contingencia debe ser revisado y actualizado regularmente para reflejar los cambios en la organización, las tecnologías y los riesgos identificados. Asegúrate de que todas las personas responsables conozcan las actualizaciones. • Establece una estrategia de comunicación clara durante situaciones de contingencia. Debes tener una lista de contactos actualizada y canales de comunicación alternativos en caso de que los medios de comunicación habituales no estén disponibles. • Adopta medidas preventivas para reducir la probabilidad de ocurrencia de las amenazas identificadas. Por ejemplo, puedes implementar sistemas de seguridad adicionales, realizar copias de seguridad periódicas de los datos críticos y capacitar al personal en prácticas de seguridad.

410- 12 Administración de soporte de tecnología de información	Muy grave	• Considera establecer acuerdos de continuidad del negocio con proveedores y socios clave. Esto puede garantizar servicios y recursos adicionales en caso de contingencia. • Realiza un seguimiento y monitoreo continuo del plan de contingencia para asegurarse de que esté actualizado y funcione según lo previsto. Realiza evaluaciones periódicas de su efectividad y realiza ajustes según sea necesario. • Analiza y documenta cualquier incidente o situación de contingencia pasada para aprender de ellas y mejorar el plan de contingencia en el futuro. • Realiza un inventario detallado de todos los activos de tecnología de información de tu organización, como hardware, software, licencias, contratos de servicios, etc. Esto te ayudará a tener una visión clara de los recursos disponibles y facilitará la administración eficiente. • Establece un proceso formal para administrar los cambios en la infraestructura de TI y las aplicaciones. Esto implica realizar pruebas rigurosas antes de implementar los cambios, asignar roles y responsabilidades claras, y documentar todos los cambios realizados. Esta gestión de cambios estructurada ayudará a minimizar los errores y maximizar la disponibilidad del sistema. • Establece un proceso claro para la gestión de incidentes de TI, incluyendo la forma de reportar, rastrear y solucionar problemas. Implementa un sistema de seguimiento de tickets o un centro de soporte para una mejor organización y seguimiento de los problemas. También es importante establecer niveles de prioridad y tiempos de respuesta para garantizar una resolución oportuna. • Utiliza herramientas de monitoreo de sistemas para supervisar proactivamente el rendimiento de tus sistemas y detectar posibles problemas antes de que se conviertan en interrupciones del servicio. Esto te permitirá tomar medidas preventivas y mitigar los riesgos antes de que afecten a los usuarios finales. • Establece políticas de seguridad claras y asegúrate de que todos los activos de TI estén protegidos con las últimas medidas de seguridad, como firewalls, antivirus, autenticación de dos factores, entre otros. Realiza auditorías de seguridad regularmente y capacita a los empleados sobre las mejores prácticas de seguridad para minimizar los riesgos de seguridad de la tecnología de información.

		• Establece un plan de copias de seguridad regular para proteger los datos críticos de tu organización. Asegúrate de que las copias de seguridad se realicen de manera regular y que los datos se almacenen en ubicaciones seguras lejos del sitio principal. También es importante realizar pruebas periódicas de recuperación de datos para garantizar que los datos se puedan restaurar correctamente en caso de una pérdida. • Define acuerdos de nivel de servicio claros con proveedores de servicios de TI y usuarios internos. Estos acuerdos deben incluir el tiempo de respuesta, la disponibilidad del sistema y otros indicadores clave de rendimiento. Esto ayudará a garantizar que todos los involucrados tengan expectativas claras y brindará una base para evaluar y mejorar continuamente los servicios de TI.
410-13 Monitoreo y evaluación de los procesos o servicios	Importante	• Determina qué es lo que deseas medir y monitorear. Asegúrate de que estos objetivos estén alineados con los objetivos generales de la organización. • Los indicadores son herramientas que te permiten medir el rendimiento de un proceso o servicio. Asegúrate de que estos indicadores sean medibles, relevantes y oportunos. • Define los procedimientos de monitoreo y evaluación que utilizarás, así como la frecuencia con la que los implementarás. Asegúrate de que el plan de monitoreo esté bien estructurado y diseñado para cumplir con tus objetivos clave. • Utiliza herramientas y software para automatizar la recopilación y el análisis de datos. Esto puede ayudarte a minimizar la cantidad de tiempo y recursos que dedicas a los procesos de monitoreo y evaluación. • Si encuentras problemas en tu proceso o servicio, asegúrate de tomar medidas inmediatas para resolverlos. Esto puede ayudarte a mejorar continuamente tus procesos y a evitar problemas en el futuro. • Asegúrate de que tu equipo esté capacitado para realizar el monitoreo y la evaluación. Esto les permitirá comprender los objetivos clave, los indicadores y el plan de monitoreo.
410-14 Sitios web, servicios de internet e intranet	Muy grave	• Identifica los riesgos potenciales que podrían afectar la seguridad de tu sitio web o servicios de internet e intranet. Haz una lista de posibles amenazas y evalúa su impacto.

			• Utiliza medidas de seguridad como cifrado SSL, autenticación de usuarios, firewalls, antivirus, y cualquier otra herramienta que pueda ayudarte a proteger la información y el acceso a tu sitio web. • Realiza un monitoreo constante de tu sitio web y servicios de internet e intranet para detectar actividades sospechosas o intentos no autorizados de acceso. Supervisa y registra la actividad del sitio para detectar anomalías. • Contrata a un equipo especializado en seguridad informática para realizar pruebas de penetración, en las que se simulan ataques para identificar vulnerabilidades y cerrarlas antes de que sean explotadas. • Mantén tus herramientas de seguridad actualizadas para asegurarte de que estén en la última versión y de que estén al día con las últimas amenazas potenciales. • Prepara un plan de contingencia para hacer frente a incidentes de seguridad, y capacita a tus empleados para que sepan cómo responder y actuar de forma segura en caso de una violación de seguridad. • Infundir conocimiento en tus usuarios (empleados, usuarios finales, etc.) acerca de las mejores prácticas de seguridad puede ayudar a reducir el riesgo de que ocurran incidentes. Entrena a tu personal sobre la importancia de la contraseña segura, el uso compartido de información y las tácticas de phishing para reducir el riesgo de que suceda un incidente de seguridad.
410-15 informática	Capacitación	Muy grave	• Realiza una evaluación de habilidades para identificar las áreas en las que se necesitan capacitación adicional. Esto te permitirá desarrollar un plan de capacitación personalizado para satisfacer las necesidades de tus empleados. • Define los objetivos de aprendizaje que deseas alcanzar con la capacitación informática, y asegúrate de que sean específicos, medibles y realistas. Los objetivos claros ayudarán a tus empleados a enfocarse y a maximizar su tiempo de capacitación. • Considera diferentes opciones de capacitación, como sesiones en línea, capacitación presencial, videos tutoriales, manuales y capacitaciones en el trabajo. Al proporcionar una variedad de opciones, tus empleados pueden elegir la vía que les resulte más cómoda y efectiva.

410-16 Comité informático	Muy grave	• Programa sesiones de capacitación de forma regular, de modo que los empleados tengan oportunidades frecuentes para aprender y mejorar sus habilidades en tecnología informática. • Diseña la capacitación de modo que incluya muchas oportunidades prácticas para que los empleados puedan poner en práctica lo que han aprendido. Los ejercicios prácticos y simulaciones pueden ayudar a consolidar los conocimientos adquiridos y a preparar a los empleados para aplicarlos en la vida real. • Después de una capacitación, realiza una evaluación para medir el éxito de la capacitación y determinar si se necesitan ajustes o cambios en el enfoque de capacitación. Además, realiza un seguimiento en el tiempo para asegurarte de que tus empleados estén aplicando eficazmente lo que han aprendido. • Ofrece incentivos para promover y aumentar la motivación de tus empleados a medida que avanzan en su capacitación, por ejemplo, ofreciendo el acceso a herramientas informáticas, nuevas oportunidades de trabajo, y aumentos de sueldo. Estos incentivos también pueden ayudar a fomentar la participación y el compromiso en las sesiones de capacitación. • Realizar una evaluación exhaustiva de los riesgos de seguridad informática a los que está expuesto el comité informático. Esto puede incluir amenazas como ataques cibernéticos, robo de datos, malware, entre otros. • Desarrollar e implementar políticas y procedimientos de seguridad informática para proteger los sistemas y datos del comité. Esto puede incluir el uso de contraseñas seguras, cifrado de datos, firewalls, antivirus y software de detección de intrusiones. • Proporcionar capacitación regular sobre seguridad informática a todos los miembros del comité. Esto puede incluir la concienciación sobre las mejores prácticas de seguridad, la identificación de posibles amenazas y la forma de responder ante ellas. • Realizar auditorías periódicas de seguridad informática para identificar posibles vulnerabilidades y brechas en la seguridad. Esto puede incluir pruebas de penetración, análisis de vulnerabilidades y revisiones de políticas y procedimientos.

410-17 Firmas electrónicas	Muy grave	• Mantener actualizados todos los sistemas operativos, aplicaciones y software utilizados por el comité informático. Esto incluye la instalación de parches de seguridad y actualizaciones regulares para protegerse contra las últimas amenazas. • Realizar copias de seguridad regulares de todos los datos críticos del comité informático. Esto garantiza que los datos puedan ser restaurados en caso de pérdida o daño debido a un incidente de seguridad. • Desarrollar y poner en marcha un plan de respuesta a incidentes que detalle los pasos a seguir en caso de una violación de seguridad o un incidente cibernético. Esto incluye la notificación de las partes afectadas, la mitigación del incidente y la recuperación de los sistemas. • Realizar los registros de seguridad: Implementar herramientas de monitoreo y análisis de registros de seguridad para detectar y responder rápidamente a posibles amenazas o actividades sospechosas. • Realizar evaluaciones periódicas de la seguridad informática del comité y realizar mejoras según sea necesario. Esto puede incluir la implementación de nuevas tecnologías de seguridad, la actualización de políticas y procedimientos, y la capacitación adicional del personal. • Antes de implementar una solución de firma electrónica, es importante evaluar las necesidades y requisitos específicos de la organización. Esto incluye determinar qué tipo de documentos se firmarán electrónicamente, qué nivel de seguridad se requiere y qué integraciones con otros sistemas son necesarias. • Existen diferentes soluciones de firma electrónica en el mercado, por lo que es importante investigar y seleccionar la que mejor se adapte a las necesidades de la organización. Algunos factores a considerar incluyen la seguridad, la facilidad de uso, la compatibilidad con los sistemas existentes y el costo. • Una vez seleccionada la solución de firma electrónica, es necesario implementarla en la organización. Esto puede incluir la instalación de software o la configuración de una plataforma en línea. Es importante seguir las instrucciones del proveedor y asegurarse de que la solución esté correctamente integrada con los sistemas existentes.

		• Es fundamental capacitar al personal sobre cómo utilizar la solución de firma electrónica de manera adecuada y segura. Esto incluye enseñarles cómo crear y firmar documentos electrónicamente, así como cómo verificar la autenticidad de las firmas electrónicas. • Es importante establecer políticas y procedimientos claros sobre el uso de la firma electrónica en la organización. Esto incluye definir quién tiene autoridad para firmar electrónicamente, cómo se deben almacenar y proteger los documentos firmados y cómo se deben manejar las discrepancias o disputas relacionadas con las firmas electrónicas. • Es recomendable monitorear y auditar regularmente el uso de la firma electrónica en la organización para detectar cualquier actividad sospechosa o irregular. Esto puede incluir revisar los registros de actividad de la solución de firma electrónica y realizar auditorías internas o externas. • Las regulaciones y estándares relacionados con la firma electrónica pueden cambiar con el tiempo, por lo que es importante mantenerse actualizado sobre las últimas novedades. Esto incluye estar al tanto de las leyes y regulaciones locales e internacionales, así como de los estándares de seguridad y privacidad relacionados con la firma electrónica. • Es importante evaluar regularmente la eficacia y seguridad de la solución de firma electrónica y realizar mejoras según sea necesario. Esto puede incluir la actualización de la solución de firma electrónica, la revisión de las políticas y procedimientos, y la capacitación adicional del personal.

4.2 DISCUSIÓN

De acuerdo a los resultados de este trabajo de investigación y recolección de información mediante instrumentos como la entrevista y encuesta a los administrativos de la institución.

Tabla 15. Escala de calificación

Nivel de cumplimiento	Del:	Al:	Semaforización
No cumple.	0,00%	09,00%	
Cumplimiento muy deficiente.	10,00%	29,99%	
Bajo nivel de cumplimiento.	30,00%	59,99%	
Nivel de cumplimiento aceptable.	60,00%	79,99%	
Alto nivel de cumplimiento.	80,00%	89,99%	
Cumplimiento máximo.	90,00%	100%	
No Aplicable.	1-100%	1-100%	

A continuación, se detalla el cumplimiento de la ISO 27002 en la parte administrativa del GAD Espejo que es de un 13,15% encontrándose en cumplimiento muy deficiente. El departamento de sistemas cuenta con 6,14%, por lo que demuestra que no cumple en absoluto la norma ISO 27002, con un total de 19,29% de cumplimiento muy deficiente a nivel de toda la institución.

Porcentaje actual de cumplimiento de controles que se establecen en la norma ISO 27002.

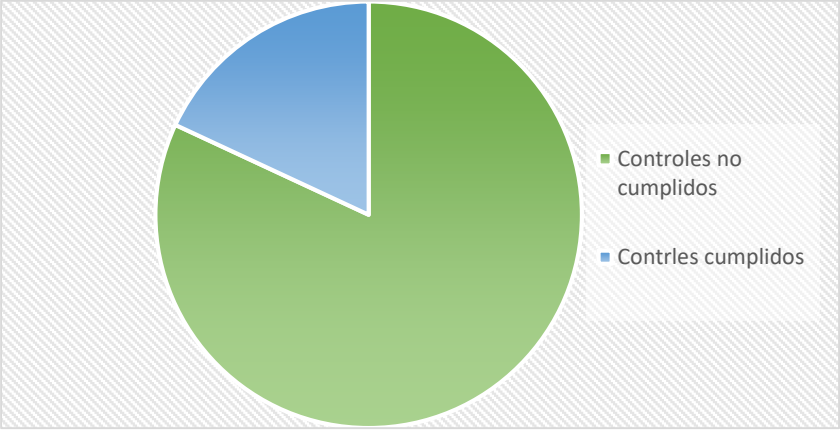


Figura 41. Cumplimiento

Tabla 16. Estado actual de cumplimiento en el GADME

Estado	Significado	Administrativo	Sistemas
Inexistente	Total falta de un proceso reconocible, la institución no ha reconocido que existen problemas que resolver.	59,65%	64,91%
Inicial	Hay evidencias de que la organización ha reconocido problemas, sin embargo, no existen procesos estandarizados y no se gestionan. Se basa en su mayoría de esfuerzo personal.	8,77%	2,63%
Repetible	Los procesos similares se llevan en forma similar y se normalizan las buenas prácticas en base a las experiencias al método. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo. Depende del grado de conocimiento de cada individuo.	0%	0%
Definido	La organización conoce los controles, los procesos se encuentran implementados, documentados y comunicados, pero no se encuentran capacitados.	1,75%	0,88%
Administrado	El control se lleva a cabo de acuerdo con un procedimiento documentado, aprobado y formalizado, se cuenta con documentación para mejorar la calidad y la eficiencia.	0%	2,63%
Optimizado	El control se aplica de acuerdo con un procedimiento documentado, aprobado y formalizado, los procesos se encuentran constantemente en mejora, en base a criterios y se optimizan los procesos.	2,63%	0%
No Aplicable	Todos los requerimientos principales de ISO/IEC 27002 no son obligatorios. De otro modo, pueden ser ignorados por la parte administrativa.	27,19%	28,95%
	Total	100%	100%

De acuerdo a este análisis de la normativa internacional ISO/IEC 27002 con 14 dominios, 35 objetivos de control y 114 controles de seguridad de la información, que se realizó al departamento de sistemas del Gobierno Autónomo Descentralizado del

Cantón Espejo (GADME), se plantea un plan de contingencia, el cual fue capacitado con la finalidad de alcanzar un cumplimiento del 71,04% adquiriendo un nivel de cumplimiento aceptable, defiriendo en la complementación de EGSI que consta de normativas, tomando en cuenta que este porcentaje corresponde a un rango que proporcionará mejoras de eficiencia y que la norma ISO 27002 de gestión de riesgos puede utilizarse para alcanzar un rango superior en todo el sistema nacional.

Porcentaje actual de cumplimiento de controles que se establecen en la norma ISO 27002 si se aplica el plan de contingencia.

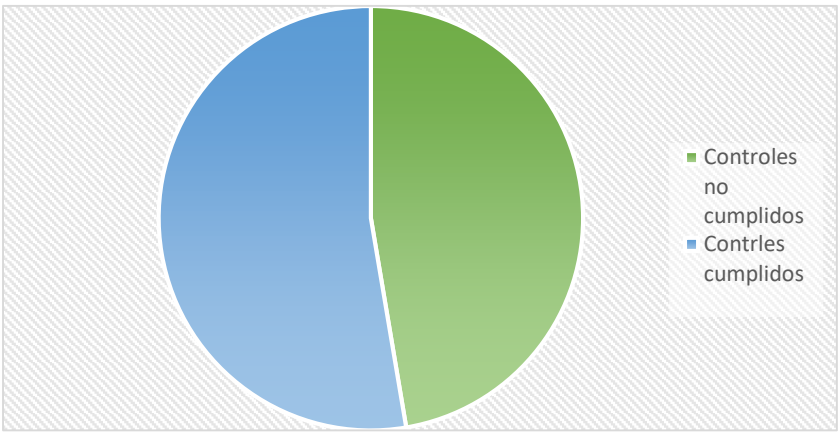


Figura 42. Si se aplica.

El proceso de implementación de un plan de contingencia, consta de varios pasos que se complementan de forma sistemática para lograr resultados eficaces, esto permite preparar documentos que tengan en cuenta el impacto y la frecuencia de cada uno de los riesgos prevenibles y vulnerabilidades descritos en esta guía, y proporcionar las medidas de mitigación adecuadas. A la hora de seleccionar los riesgos, se da una gran proporción y prioridad a los riesgos identificados con alto impacto y frecuencia, es importante dar prioridad a las vulnerabilidades que ya que no tratarlos trae más inconvenientes para la institución.

De acuerdo a la investigación de (Moron Peredo & Atalaya Urrutia, 2023) menciona que antes de implementar cualquier control de seguridad de la información, es necesario realizar una evaluación de riesgos para identificar las posibles amenazas y vulnerabilidades a las que la organización se enfrenta. Esta evaluación ayudará a determinar qué controles son necesarios y cómo se deben implementar.

La ISO 27002 abarca una amplia gama de controles, desde medidas técnicas como firewalls, encriptación y hasta medidas organizativas (por ejemplo, contratos de confidencialidad y políticas de acceso, la implementación de estos controles puede

requerir cambios en los sistemas y procesos existentes, así como la asignación de responsabilidades claras.

Por otro lado, (ISO\IEC 27002:2022, 2022)proporciona una lista exhaustiva de controles de seguridad que se pueden implementar. Es importante que la organización adapte estos controles a su entorno específico y diseñe políticas y procedimientos claros para su implementación. Estas políticas y procedimientos deben ser comunicados y entendidos por todos los miembros de la organización. En resumen, la implementación de la ISO 27002 requiere una evaluación de riesgos, diseño de políticas y procedimientos, implementación de controles técnicos y organizacionales, capacitación y concientización, y monitoreo continuo. Al seguir estas pautas, una organización puede fortalecer su seguridad de la información y protegerse contra posibles amenazas y vulnerabilidades.

V. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- Se concluye que mediante el uso de la metodología mixta se puede identificar datos precisos y proporcionar una comprensión profunda sobre la importancia de la seguridad de la información.
- La organización y el desarrollo de la tecnología en el municipio permiten la automatización y la gestión de servicios reales, ya que ayuda a optimizar los recursos y mejorar la calidad de vida de las personas, optimizando la eficiencia en la gestión de recursos públicos.
- Se logra conocer que en las instituciones públicas se estableció normas para capacitar, garantizar la seguridad física, usar protocolos de encriptación de datos y realizar auditorías de seguridad incluyendo la norma ISO 27002:2013.
- En base a el tipo de auditoria que se emplea como es de seguridad de la información que se enfoca en evaluar los sistemas informáticos de la empresa en cuanto a su capacidad para proteger la información crítica de la organización, su disponibilidad y su integridad.
- Aplicando la norma ISO 27002:2013 al Municipio del Cantón Espejo se tuvo como conclusión que es importante implementar un plan de mejora para saber cómo actuar en caso de una emergencia, incluyendo identificación de roles, responsabilidades y protocolos necesarios para minimizar el impacto de la emergencia.
- Finalmente se determinó que 63 de no conformidades aplicados en la auditoría, los mismos que se priorizaron en el plan de contingencia en base al impacto y probabilidad. Posteriormente se emitieron estrategias de mitigación los cuales fueron socializados al personal del Gobierno Autónomo De centralizado Del Cantón Espejo.

5.2 RECOMENDACIONES

- Se recomienda realizar una evaluación constante de los riesgos, implementando la normativa ISO 27002 la cual incluye estrategias y recursos de gestión de la seguridad de la información, es fundamental establecer un plan de respuestas a incidentes para mitigar el daño y recuperarse rápidamente.
- Es recomendable que el municipio gestione estrategias emitidas en el plan de contingencia de riesgos, para de esta manera poder cumplir con los parámetros solicitados, considerando que los controles se han identificado y gestionado, obteniendo una adecuada optimización de recursos.
- Es importante que el departamento de sistemas realice auditorías y pruebas regulares para evaluar así los controles de seguridad incluyendo pruebas de penetración, análisis de vulnerabilidades y monitoreo continuo de los sistemas.
- Se recomienda incluir medidas técnicas para proteger los sistemas y la información. Esto puede incluir la instalación de firewalls, sistemas de detección y prevención de intrusiones, software antivirus y antispyware actualizado, cifrado de datos, copias de seguridad y actualizaciones regulares de software y hardware.

VI. REFERENCIAS BIBLIOGRÁFICAS

Parra Zambrano, E., & Pincheira Jiménez , R. (19 de Mayo de 2019). Integración curricular de las TIC. *Las TIC* , págs. 13- 16.

Aguilar, G. H. (2021). *Auditoría Informática.* México: studocu.

Albán, M. (2018). *MINISTERIO DE TELECOMUNICACIONES Y DE LA SOCIEDAD DE LA INFORMACION.* Quito: Siteal.

Alvarado, R., Acosta, K., & Mata de Buonaffina , Y. (12 de Marzo de 2018). Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones. *Necesidad de los sistemas de información gerencial para la toma de decisiones en las organizaciones*, págs. 4-7.

Álvarez, C. (2011). *Cuantitativa y Cualitativa Guía didáctica.* Universidad Surcolombiana.

Ayala, A. M. (2022). *Agenda Digital* . Quito : Agencia Digital del Ecuador.

Baltazar, T. (2019). La transversalidad de las tecnologías de información y comunicación. *La transversalidad de las tecnologías de información y comunicación*, 12.

Bernal, C. (2010). *Metodología de la Investigación.* Pearson Educación.

Blog de UTEL. (2019). *Las funciones básicas de la empresa según Henry Fayol*, 1-10.

Cabello, E. (09 de Noviembre de 2019). *Auditoría Informática.* Obtenido de Auditoría Informática: https://es.slideshare.net/100001813725084/auditoria-informatica-191843074

Cano, F., Cano, A., & Pineda, D. (2018). Modelo de gobierno de tecnologías de la información para mejorar el desempeño de proyectos de negocio miniorista. *Modelos de negocio en investigación administrativa*, 4-9.

Cueva, S., Espinoza, J., & Jaramillo, E. (2020). *Informe de rendición de cuentas en materia* . Quito: http://www2.competencias.gob.ec/wp-content/uploads/2021/03/Evaluaci%C3%B3n-de-la-gesti%C3%B3n-institucional.pdf.

Fernández, C., Enrique, E., Herrera, G., & Jesús, R. d. (2020). Prevención de riesgos por ciberseguridad desde la auditoria forense: conjugando el talento humano

organizacional. *NOVUM, revista de Ciencias Sociales Apliacadas, vol. I, núm*, 62-63-64.

GSITIC. (2019). BIII17. La calidad del software y su medida. Modelos, métricas,normas y estándares. *BIII17. La calidad del software y su medida. Modelos, métricas,normas y estándares.*, https://gsitic.wordpress.com/blog/.

Hernández, R., Fernández, C., & Baptista, P. (2014). *Metodología de la investigación* (Vol. 4). Editorial Mc Graw Hill Interamericana Editores SA.

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jácome, J. (2020). Análisis de las principales dificultades en la auditoría. En D. Imbaquingo, J. Díaz, T. Saltos, S. Arciniega, J. De La Torre, & J. Jácome, *Análisis de las principales dificultades en la auditoría* (pág. 427). Argentina: risti.

ISO\IEC 27002:2022. (2022). *ISO/IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber*. Obtenido de ISO/IEC 27002:2022 Controles Organizacionales. Todo lo que necesita saber: https://www.isotools.us/2022/07/29/iso-iec-270022022-controles-organizacionales-todo-lo-que-necesitas-saber/

Jorge, R. B. (05 de Enero de 2021). *AUDITORIA DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MASTER-SECURITY S.A. PARA DETERMINAR EL NIVEL DE CUMPLIMIENTO DE LOS CONTROLES DEFINIDOS POR LA NORMA ISO/IEC 27005.* Obtenido de AUDITORIA DE SEGURIDAD DE LA INFORMACIÓN PARA LA EMPRESA MASTER-SECURITY S.A. PARA DETERMINAR EL NIVEL DE CUMPLIMIENTO DE LOS CONTROLES DEFINIDOS POR LA NORMA ISO/IEC 27005: http://repositorio.ug.edu.ec/handle/redug/59681

Kenedy, R. P. (2020). Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la Red en la Oficina Departamental de Estadística e Informática de Junín. En R. P. Kenedy, *Implementación de políticas de seguridad informática para mejorar el acceso y la seguridad lógica de la Red en la Oficina Departamental de Estadística e Informática de Junín* (pág. http://hdl.handle.net/20.500.12894/5434). Huancayo: UNCP.

Lazcano, E., Fernández, E., Salazar, E., & Hernández, A. (2000). Estudios de cohorte. Metodología, sesgos y aplicación. *Salud pública de México, 42*(3), 230-241. https://saludpublica.mx/index.php/spm/article/view/6234.

López, J., Ramírez, J., Espinosa, E., Venegas, C., Díaz, D., & Mantilla, E. (06 de Noviembre de 2019). *Las TIC en el territorio digital-Análisis del libro Blanco de la*

defensa. Guayaquil: 2019. Obtenido de Las TIC en el territorio digital: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/11/LBTD_actualizado_25-11-2019_a.pdf

López, M., Sánchez, C., & Llano Monelos, P. (2022). *Mapa de Riesgos: Identificación y Gestión de Riesgos.* file:///C:/Users/MI%20PC/Downloads/Dialnet-MapaDeRiesgos-4744304%20(1).pdf.

Lutsak, N., Maldonado, J., & Bogoya, D. (2022). *EVALUACIÓN TEÓRICOMETODOLÓGICA Y PROCEDIMIENTO DE RESULTADOS DE APRENDIZAJE EN PROGRAMAS DE POSGRADO.* Quito: Galina Segarra.

Matteis, L. (2019). *Seguridad Informática.* Atlántico Sur : IDEI.

Mina, M. A. (15 de Diciembre de 2019). Proceso de conformación del comité de la tecnología de la información (TI). *Procesos de formación de la información tecnológica del comité* , págs. 1-6.

Ministerio de telecomunicaciones y de la sociedad de la información. (6 de 12 de 2018). *Plan de la Sociedad de la Informacion PSIC*. Obtenido de Plan de la Sociedad de la Informacion PSIC: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2018/11/Plan-de-la-Sociedad-de-la-Informacion-PSIC-20181026.pdf

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (2019). Libro blanco de territorios digitales en Ecuador . En M. d. Información, *Libro blanco de territorios digitales en Ecuador* (pág. 29). Quito: Ecuador Digital.

Molina, Á. D. (16 de Septiembre de 2021). *ANÁLISIS DE LA IMPLEMENTACION DE DATOS ABIERTOS Y SU INCIDENCIA EN EL FORTALECIMIENTO DE LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA EN EL ECUADOR AL AÑO 2021*. Obtenido de ANÁLISIS DE LA IMPLEMENTACION DE DATOS ABIERTOS Y SU INCIDENCIA EN EL FORTALECIMIENTO DE LA TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA EN EL ECUADOR AL AÑO 2021: http://repositorio.uisrael.edu.ec/handle/47000/2954

Moron Peredo, K., & Atalaya Urrutia, C. (2023). *Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C.* Pimentel: USS.

Muñoz, J. D. (2019). *Diseño de políticas de Seguridad Informática.* España: Editorial Académica Española.

Namakforoosh, M. (2000). *Metodología de la Investigación.* Editorial Limusa.

Ortecho, M. E. (12 de Marzo de 2020). *Evaluación de riesgo de seguridad de información según ISO 27005, OGITT–Instituto Nacional de Salud.* Obtenido de Evaluación de riesgo de seguridad de información según ISO 27005, OGITT–Instituto Nacional de Salud: https://repositorio.ucv.edu.pe/handle/20.500.12692/42553

Ortega, A. O. (2010). *Enfoques de investigación* . Chicago: Club Universitario.

Ramos, M. A. (2019). *La Seguridad y la Confidencialidad de la Información y la LORTAD.* Puerto Rico : Informática y Derecho .

Rendón, M., Villacís, M., & Miranda, M. (2016). Estadística descriptiva. *Revista Alergia México, 63*(4), 397-407. https://www.revistaalergia.mx/ojs/index.php/ram/article/view/230.

Restrepo, L. (2020). *Plan de mejoramiento de los procesos logísticos de la empresa de Servicios Postales Nacionales S.A 4-72 de Pereira Risalda.* [Tesis de Administración de Empresas]. Universidad del Valle. Biblioteca digital de Universidad del Valle. https://bibliotecadigital.univalle.edu.co/handle/10893/19686. Obtenido de [Tesis de administración de empresas. .

Rivoir , A., & Morales, M. (2019). *Tecnnologías digitales en la auditoría.* Buenos Aires: CLACSO.

Robles, N. G. (14 de Marzo de 2022). *APLICACIÓN INFORMÁTICA PARA LA GESTIÓN DE PROCESOS DE RECAUDACIÓN E INVENTARIO DE LA CÁMARA DE COMERCIO DE JIPIJAPA*. Obtenido de APLICACIÓN INFORMÁTICA PARA LA GESTIÓN DE PROCESOS DE RECAUDACIÓN E INVENTARIO DE LA CÁMARA DE COMERCIO DE JIPIJAPA: http://repositorio.unesum.edu.ec/handle/53000/3558

Salgado , S., Osuna, M., Sevilla, C., & Morales, G. (2018). Auditoría informática. *La Auditoría Informática en las organizaciones*, 8-14.

Sunkel, G., Trucco, D., & Espejo, A. (2019). La integración de las tecnologías digitales en las escuelas de américa latina y el Caribe. En D. T. Guillermo Sunkel, *La integración de las tecnologías digitales en las escuelas de américa latina y el Caribe* (pág. 60). Caribe: CEPAL.

Vieites, Á. G. (2019). Auditoría de seguridad informática. En Á. G. Vieites, *Auditoría de seguridad informática* (pág. 42). Madrid: Ediciones de la U.

VII. ANEXOS

Anexo 1. Acta de sustentación de Pre defensa del TIC

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE COMPUTACIÓN

ACTA

DE LA SUSTENTACIÓN ORAL DE LA PREDEFENSA DEL TRABAJO DE INTEGRACIÓN CURRICULAR

ESTUDIANTE:	MURILLO RUANO LEIDY TAMARA	**CÉDULA DE IDENTIDAD:**	=RUBRICAIL6
PERIODO ACADÉMICO:	2022 A		
PRESIDENTE TRIBUNAL	MSC. JAIRO VLADIMIR HIDALGO GUIJARRO	**DOCENTE TUTOR:**	MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE:	MSC. GUANO CARDENAS CARLITOS ALBERTO		
TEMA DEL TIC:	"Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo"		

No.	CATEGORÍA	Evaluación cuantitativa	OBSERVACIONES Y RECOMENDACIONES
1	PROBLEMA - OBJETIVOS	7,00	Establecer de manera clara el problema a resolver, revisar los objetivos generales y específicos
	FUNDAMENTACIÓN TEÓRICA	7,00	ampliar la fundamentación teórica referente a procesos de auditoría.
3	METODOLOGÍA	7,00	relacionar las variables de estudio con la formulación del problema.
4	RESULTADOS	7,00	establecer de forma clara el proceso de auditoría realizado.
5	DISCUSIÓN	7,00	utilizar lenguaje técnico
6	CONCLUSIONES Y RECOMENDACIONES	7,00	aplicarlas a los resultados obtenidos, utilizando aspectos técnicos
7	DEFENSA, ARGUMENTACIÓN Y VOCABULARIO PROFESIONAL	7,00	argumentar las preguntas formuladas por el jurado
8	FORMATO, ORGANIZACIÓN Y CALIDAD DE LA INFORMACIÓN	7,00	presentar de manera organizada el informe

eniendo una nota de: 7,00 Por lo tanto, **APRUEBA** ; debiendo el o los investigadores acatar el siguiente artículo:

Art. 36.- De los estudiantes que aprueban el informe final del TIC con observaciones.- Los estudiantes tendrán el plazo de 10 días para proceder a corregir su informe final del TIC de conformidad a las observaciones y recomendaciones realizadas por los miembros del Tribunal de sustentación de la pre-defensa.

Para constancia del presente, firman en la ciudad de Tulcán el viernes, 28 de julio de 2023

MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
PRESIDENTE TRIBUNAL

MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE TUTOR

MSC. GUANO CARDENAS CARLITOS ALBERTO
DOCENTE

Anexo 2. Certificado de Abstract por el Centro de Idiomas UPEC.

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Murillo Ruano Leidy Tamara
DATE: 26 de julio de 2023

TOPIC: *"Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo"*

MARKS AWARDED **QUANTITATIVE AND QUALITATIVE**

VOCABULARY AND WORD USE	Use new learnt vocabulary and precise words related to the topic	Use a little new vocabulary and some appropriate words related to the topic	Use basic vocabulary and simplistic words related to the topic	Limited vocabulary and inadequate words related to the topic
	EXCELLENT: 2 ☐	GOOD: 1Vera Játiva, Edwin Andrés,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
WRITING COHESION	Clear and logical progression of ideas and supporting paragraphs.	Adequate progression of ideas and supporting paragraphs.	Some progression of ideas and supporting paragraphs.	Inadequate ideas and supporting paragraphs.
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
ARGUMENT	The message has been communicated very well and identify the type of text	The message has been communicated appropriately and identify the type of text	Some of the message has been communicated and the type of text is little confusing	The message hasn't been communicated and the type of text is inadequate
	EXCELLENT: 2 ☐	GOOD: 1,5 ☐	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
CREATIVITY	Outstanding flow of ideas and events	Good flow of ideas and events	Average flow of ideas and events	Poor flow of ideas and events
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
SCIENTIFIC SUSTAINABILITY	Reasonable, specific and supportable opinion or thesis statement	Minor errors when supporting the thesis statement	Some errors when supporting the thesis statement	Lots of errors when supporting the thesis statement
	EXCELLENT: 2 ☐	GOOD: 1,5 ■	AVERAGE: 1 ☐	LIMITED: 0,5 ☐
TOTAL/AVERAGE	9 - 10: EXCELLENT 7 - 8,9: GOOD 5 - 6,9: AVERAGE 0 - 4,9: LIMITED	TOTAL 9,5		

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Murillo Ruano Leidy Tamara
Fecha de recepción del abstract: 26 de julio de 2023
Fecha de entrega del informe: 26 de julio de 2023

El presente informe validará la traducción del idioma español al inglés si alcanza un porcentaje de: 9 – 10 Excelente.

Si la traducción no está dentro de los parámetros de 9 – 10, el autor deberá realizar las observaciones presentadas en el ABSTRACT, para su posterior presentación y aprobación.

Observaciones:

Después de realizar la revisión del presente abstract, éste presenta una apropiada traducción sobre el tema planteado en el idioma Inglés. Según los rubrics de evaluación de la traducción en Inglés, ésta alcanza un valor de 9,5 por lo cual se validad dicho trabajo.

Atentamente

EDISON ROMMEL PEÑAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3. Entrevista realizada al departamento de Sistemas.

El Ángel, junio 27 del 2022

Ingeniero
Arnaldo Cuases
ALCALDE DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTON ESPEJO.
Presente.-

De mis consideraciones:

Por medio del presente le hago llegar un cordial y atento saludo y a la vez augurarle toda clase de éxitos en sus funciones que tan acertadamente las dirige en beneficio de nuestro cantón.

Yo, **LEIDY TAMARA MURILLO RUANO**, con cédula de ciudadanía N° 04096899-5, alumna del octavo semestre de la Carrera de Computación, facultad Industrias Agropecuarias y Ciencias Ambientales de la Universidad Politécnica Estatal del Carchi; me dirijo a usted para solicitarle de la manera más comedida se digne ayudarme con la autorización respectiva para poder realizar mi tesis de grado que tiene como título "Plan de Auditoría Informática para Gestión de Riesgos Tegnológicos en el GADM -E", por lo que necesito que me ayuden facilitándome la documentación respectiva para la elaboración de mi tesis.

Segura que mi pedido será atendido favorablemente desde ya anticipo mis debidos agradecimientos.

Atentamente,

Srta. Leidy Murillo
SOLICITANTE
Cel. 096129151-1

G.A.D. MUNICIPAL DE ESPEJO
RECEPCIÓN
27 06 2022 12:54
2223

Anexo 4. Entrevista realizada al departamento de Sistemas.

Gobierno Autónomo Descentralizado Del Cantón Espejo

Entrevista

Objetivo. Determinar un nivel de cumplimiento en normativas de control interno 410 tecnológicas de la información de la Contraloría General del Estado en el GADM-E al departamento de Sistemas Informáticos y en referencia a estándar internacional de ISO/IEC 27002 que se encarga de la seguridad de la información.

1. Indique como se encuentran los siguientes documentos, mensuales que ayudan a cumplir políticas de seguridad.

PUBLICADO (P)	SOCIALIZADO (S)	EN DESARROLLO (D)	VERIFICADO (V)	NO DISPONIBLE (ND)	NO ALICA (NA)

Documentos/ Manuales	P	S	D	V	ND	NA
Politicas para la seguridad de la informacion						
Asignacion de roles y responsabilidades en el area						
Matriz sobre incidentes de seguridad de la informacion						
Contacto con grupo de interes especial						
Metodos de gestion de proyectos						
Politicas de dispositivos moviles						
Responsabilidades de gestion						
Proceso disciplinario						
Responsabilidades ante la finalizacion o cambio						
Inventario de activos						
Propiedad de los activos						
Uso aceptable de los activos						
Politicas de control de acceso						
Provision de acceso de usuario						
Retirado o reasignacion de derechos de acceso						
Uso de la informacion secreta de autentificacion						
Documentacion de procedimientos de las operaciones						
Copias de seguridad de la informacion						
Registro de administracion y operacion						
Restriccion en la instalacion de software						
Politicas y procedimientos de intercambio de informacion						
Acuerdo de intercambio de informacion						
Acuerdos de confidencialidad o no revelacion						
Politicas de desarrollo seguro						
Procedimientos de control de cambios en el sistema						
Notificacion de puntos debiles de la seguridad						
Implementar la continuidad de la seguridad de la informacion						

2. ¿Se lleva a cabo la elaboración de proyectos informáticos tanto como sistemas o aplicaciones por medio de teletrabajo? Si ( ) No ( )

3. Cuando alguien ingresa a el área de desarrollo, ¿Usted revisa el currículum o antecedentes de quien va a ingresar? Si ( ) No ( )

4. ¿Las personas que intervienen en el desarrollo firman un compromiso de confidencialidad para no revelar información sensible? Si ( ) No ( )

5. ¿Cuál es el mecanismo que le motiva a mantener la información segura?

6. ¿Cuántas veces en un año les capacitan a el personal sobre seguridad de la información?

( ) Mensual ( ) Semestral ( ) Anual ( ) Nunca

7. ¿Cuándo fue la última capacitación? ¿La capacitación es para todos o cierto sector de la empresa?

8. ¿En el caso de alguna falta grave de pérdida de datos dentro del departamento existe un proceso disciplinario para los empleados? ¿Cuál?

9. Si la persona que se contrata para el desarrollo finaliza su contratación laboral y expone información privada, ¿Cuáles son los procedimientos que toma el departamento de sistemas?

Anexo 5. Entrevista realizada al departamento de Sistemas.

10. ¿Se cuenta con horas de resguardo de equipos informáticos?

11. ¿Se tiene implementado reglas de uso aceptable de información?

12. ¿Se tiene formalizado un proceso de desvinculación que incluya la devolución de todo activo físico y electrónico que sean del departamento estén bajo su custodia?

13. Con la finalidad de asegurar que la información reciba un nivel adecuado de protección, clasifique la información de acuerdo con los siguientes parámetros.

Tipos de informacion	Publico	Privado	Confidencial	Restringido
Plan estrategico, metas y objetivos institucionales.				
Planes operativos anuales				
Proyectos institucionales, normativa interna y su documentacion.				
Plan de inversion anual				
Documentacion de soporte al Sistema de Informacion General				
Informe sobre escalas salariales				
Norma tecnica para la aplicacion de remuneracion				
Criterios informes juridicos y absoluciones de consultas juridicas cuyo objeto es el analisis de temas de diversa indole legal como temas comerciales, financieros, tributarios, laborales.				
Base de datos de los usuarios de la institucion.				
Descripcion de los procesos, politicas y procedimientos del area				
Planes y proyectos de inversion				
Plan operativo				
Infraestructura de red y de equipos				
Configuracion de la red y equipos				
Manuales tecnicos de las plataformas tecnologicas				
Indices, reportes, registros, estadisticas, propios del area				
Programas fuentes de los sistemas adquiridos desarrollados				
Codigo fuente de procedimientos, paquetes y scripts de base de datos e interfaces de sistemas				
Scripts de seguridad a nivel de aplicativos y bases de datos para encriptación de la informacion				
Manuales tecnicos/ Usuario/ Instalacion y configuracion tanto de HW como de SW, incluye sistemas de información.				
Documentacion de procesos criticos relacionados con los servicios de comunicación en la institución				
Diagrama de diseño de infraestructura y tecnologia de red, Data Center y en general de la arquitectura tecnológica de la institución				
Inventarios de HW y SW incluye aplicaciones				
Inventario de Usuarios, nombres de cuentas, contraseñas para las plataformas tecnológicas y sistemas de información.				
Proyecto y presupuestos de inversion para TI				
Planes de tratamiento de riesgo				

Anexo 6. Entrevista realizada al departamento de Sistemas.

Informacion de procesos contractuales para la provision de soluciones tecnológicas				

14. ¿Cómo se encuentra etiquetada la información de la base de datos de los usuarios de la institución?

15. ¿Quiénes son responsables de manipular esa información?

16. ¿Cuáles de las directrices que se consideran en esta institución para la gestión de soportes extraibles?

Directrices para la gestión de soportes extraibles	Si	No
En caso de ya no ser necesarios, deberian borrarse definitivamente los contenidos de cualquier soporte reutilizable que vaya a ser retirado		
Cuando sea necesario y practico, deberia solicitarse autorizacion para extraer soportes de la organización, y deberia mantenerse un registro de tales retiradas para mantener la trazabilidad a efectos de auditoria		
Todos los soportes deberian almacenarse en un entorno seguro y protegido, conforme a las especificaciones de sus fabricantes		
Deberian emplearse tecnicas criptograficas para proteger datos en soportes extraibles en caso de que apliquen requisitos importantes de confidencialidad o integridad		
Los datos deberian transferirse a soportes de fabricacion reciente antes de que se conviertan en ilegibles, a fin de mitigar el riesgo de degradación del soporte durante el tiempo en que los datos almacenados aún son necesarios		
Deberian almacenarse copias multiples de datos valiosos en soportes separados para reducir aun mas el riesgo de daño o pérdida simultánea de los datos		
El inventariado de soportes extraibles deberia considerarse para limitar las posibilidades de perdida de datos		
Solo deberian permitirse reproductores de soportes extraibles cuando haya una razon de negocio para ello		
La transferencia de informacion a medios extraibles deberia ser monitorizada, cuando hay necesidad de usar dichos soportes.		

17. ¿Existen procedimientos para la eliminación de soportes?

18. ¿Envian información en soportes extraibles fuera de la organización? Si ( ) No ( )

19. ¿Existen procedimientos de autorización que determine quien tiene permitido el acceso a qué redes y a qué servicios?

20. ¿Existe un procedimiento donde se da de baja a los usuarios?

21. ¿Tienen una matriz de usuarios para verificar que accesos tiene y que privilegios goza?

22. ¿Cuál es el mecanismo para restablecer una contraseña?

23. Si se ha implementado un sistema para un área especifica, ¿Quién tendría derechos de acceso privilegiado?

24. ¿Cada qué tiempo usted renueva las claves de seguridad en su equipo?

( ) Mensual ( ) Semestral ( ) Anual ( ) Nunca

25. ¿Los sistemas que utilizan contemplan un menú de acceso para colocar el usuario o contraseña?

26. Al momento del desarrollo de un sistema o aplicación se toma en cuenta procedimientos seguros de inicio de sesión.

27. Cuando se realiza el proceso de cambio de contraseña es: ( ) Obligatorio ( ) Voluntario

28. ¿Cuáles son los procedimientos de ingreso a programas de utilidad?

29. ¿El acceso al código fuente de programas está estrictamente controlado?

30. Los desarrolladores emplean algún método criptográfico cuando se encuentran desarrollando sistemas?

31. ¿Se genera claves para distintos sistemas criptográficos y diferentes aplicaciones?

Anexo 7. Encuesta aplicada al personal administrativo del GADME.

32. ¿Si se encuentran desarrollando un sistema quien tiene acceso?

33. ¿Cuándo desarrollan un sistema o un software utilizan una base de datos independiente a la que están manejando en operación?

34. ¿Se tiene implementado controles de prevención y recuperación que sirvan como protección de código malicioso?

35. Para identificar si se realiza copias de seguridad seleccione:

Copias de seguridad	Si	No	
Realizan respaldo de las bases de datos			
¿Cada cuanto tiempo?			Explique
Se las realiza fuera del servidor			
Se protegen de manera fisica			
Se protegen de manera mental			
Los respaldos son comprobados			
La informacion esta cifrada			

36. ¿Se realiza un registro, protección y revisión periódica de actividades de usuario durante el proceso de desarrollo?

37. ¿Qué capacidad de almacenamiento tienen los ficheros de registro?

38. ¿Se encuentran sincronizados los relojes?

39. ¿Existe una plataforma de auditorías para si los sistemas de información funcionan adecuadamente?

40. ¿Se tienen establecido controles especiales para salvaguardar la confidencialidad e integridad de datos?

41. ¿Cuándo se modifica los sistemas operativos o aplicaciones se revisa y se prueba, para garantizar que no exista efectos adversos?

42. Indique el procedimiento de desarrollo de software y aplicativos

43. ¿Qué reglas se tiene en cuenta en el momento de iniciar un desarrollo de sistemas seguro? Seleccione

Reglas de desarrollo seguro	Si	No
La seguridad del entorno de desarrollo		
Directrices sobre la seguridad en el ciclo de vida de desarrollo de software		
Requisitos de seguridad en la fase de diseño		
Puntos de verificacion de seguridad incorporados a los hitos del proyecto		
Repositorios seguros		
Seguridad en el control de versiones		
Conocimiento necesario sobre seguridad de aplicaciones;		
Capacidad de los desarrolladores de evitar, encontrar y reparar vulnerabilidades.		

44. ¿Se realiza pruebas de aceptación del sistema?

45. ¿En el momento de desarrollo existe una fuga de información a quien se le notifica?

46. ¿Cuál es el proceso para la notificación?

47. ¿Evalúan el riesgo de las notificaciones de los incidentes que ocurren dentro de la organización?

48. ¿Cuál fue el aprendizaje de las fallas de seguridad de la información?

49. ¿Cuál será el proceso de recopilación de evidencias?

50. ¿Se tiene una planificación de continuidad de la organización?

Anexo 8. Encuesta aplicada al personal administrativo del GADME.

5. ¿El departamento de sistemas en que lapso soluciona los problemas de su computador o fallas que se presenten en sistemas informáticos?
(x) Una semana a dos
( ) Dos a tres semanas
( ) Un mes
( ) Un mes y más

6. En una escala del 1 al 5 califique la asesoría que brinda el personal de tecnología del municipio acerca de seguridad.

1	X 2	3	4	5

Cuestionario de Auditoría correspondiente al desarrollo de proyectos

7. ¿Los sistemas son desarrollados de manera?
(X) Externa
( ) Interna

8. ¿Considera de sistemas cubre las necesidades para el manejo de redes, sistemas operativos, aplicaciones?
( ) No lo cubre
(x) Parcialmente
( ) La mayor parte
( ) Todas

9. ¿Existen políticas para el manejo de redes, sistemas operativos, aplicaciones?
( ) Si
(x) No
¿Cuáles?.....

10. ¿Dentro del departamento existe la disponibilidad de desarrollo de sistemas y aplicaciones y que se realicen en un lapso establecido?
( ) Generalmente
( ) Regularmente
( ) Ocasionalmente
( ) Siempre

Cuestionario de Auditoría correspondiente a seguridad de la información

11. ¿Usted ha recibido capacitaciones sobre políticas de seguridad?
( ) Pocas veces
( ) A menudo
( ) Siempre
( ) Nunca
(x) No conozco

12. ¿Conoce si los sistemas del municipio cuentan con políticas de seguridad que se encarguen de supervisar la manera en la que se manipula la información?
( ) Si
(X) No, conozco
( ) No es necesario

13. ¿Se ha establecido procedimientos para la gestión de los medios de almacenamiento removibles de acuerdo con el valor de la información?
Si ( ) No ( )

14. ¿Cada qué tiempo realiza el respaldo de la información?
( ) Una vez por semana
( ) Dos veces a la semana
( ) Mensual
( ) Anual
( ) Siempre
(x) Nunca

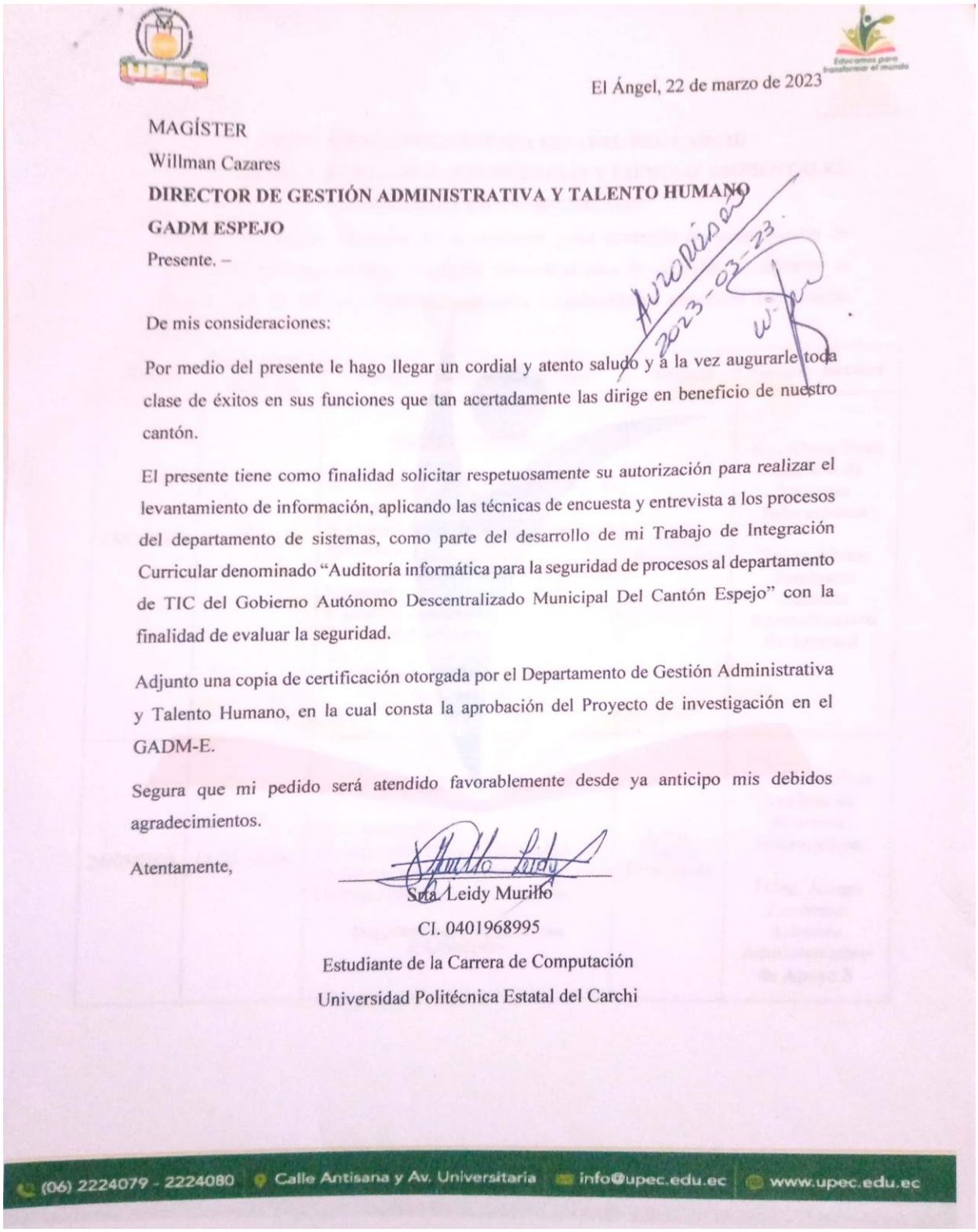
15. ¿En qué dispositivos usted respalda la información?
( ) Dispositivos USB
( ) Disco extremo

Anexo 9. Encuesta aplicada al personal administrativo del GADME.

( ) Unidad de DVD
(x) Almacenamiento en la nube
Otros.....

16.¿El cambio de contraseña es?
( ) Obligatorio
(X) Voluntario
17.¿Cada qué tiempo usted renueva las claves de seguridad en los equipos del municipio?
( ) Mensual
( ) Semestral
( ) Anual
(X) Nunca
18.¿Existe alguna exigencia o control para el acceso a sitos webs permitidos, para el cumplimiento de sus funciones?
( ) Si
(X) No
¿Cuáles?
( ) Manejo de permisos y privilegios
( ) Asignación incorrecta de privilegios
( ) Cacheo del resultado de una operación privilegiada
( ) Rutinas de autorización
(X) Manejo de permisos por defecto
( ) Cuentas de usuarios
( ) Acceso a base de datos
19.¿Qué medidas de seguridad se encuentran disponibles para evitar que otros usuarios accedan a su computador?
( ) Control de acceso a los datos más estrictos
( ) Realizar copias de seguridad
(x) Utilizar contraseñas seguras
(x) Proteger el correo electrónico
(x) Contratar un software integral de seguridad
( ) Utilizar software DLP
( ) Trabajar en la nube
( ) Lector de retina
( ) Active directory
20. ¿Cómo se da cuenta que otro usuario ha utilizado su equipo?
.....
21. ¿Qué medidas de seguridad aplica?
(x) Cambio de contraseña
( ) No hago nada
( ) Resguardo la información
Otros.....
22.¿Cuándo fue la última capacitación que recibió acerca del uso de dispositivos y sistemas informáticos?
( ) Último mes
( ) Último semestre
( ) Último año
(X) No he recibido
23.¿Qué temáticas de capacitación ha recibido últimamente??
( ) Seguridad informática
( ) Ataques de phishing (suplantación de identidad)
( ) Wi-Fi público
( ) Seguridad en la nube
( ) Ofimática
( ) Base de datos

Anexo 10. Autorización para obtener información.



El Ángel, 22 de marzo de 2023

MAGÍSTER
Willman Cazares
DIRECTOR DE GESTIÓN ADMINISTRATIVA Y TALENTO HUMANO
GADM ESPEJO
Presente. –

Autorizado 2023-03-23

De mis consideraciones:

Por medio del presente le hago llegar un cordial y atento saludo y a la vez augurarle toda clase de éxitos en sus funciones que tan acertadamente las dirige en beneficio de nuestro cantón.

El presente tiene como finalidad solicitar respetuosamente su autorización para realizar el levantamiento de información, aplicando las técnicas de encuesta y entrevista a los procesos del departamento de sistemas, como parte del desarrollo de mi Trabajo de Integración Curricular denominado "Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo" con la finalidad de evaluar la seguridad.

Adjunto una copia de certificación otorgada por el Departamento de Gestión Administrativa y Talento Humano, en la cual consta la aprobación del Proyecto de investigación en el GADM-E.

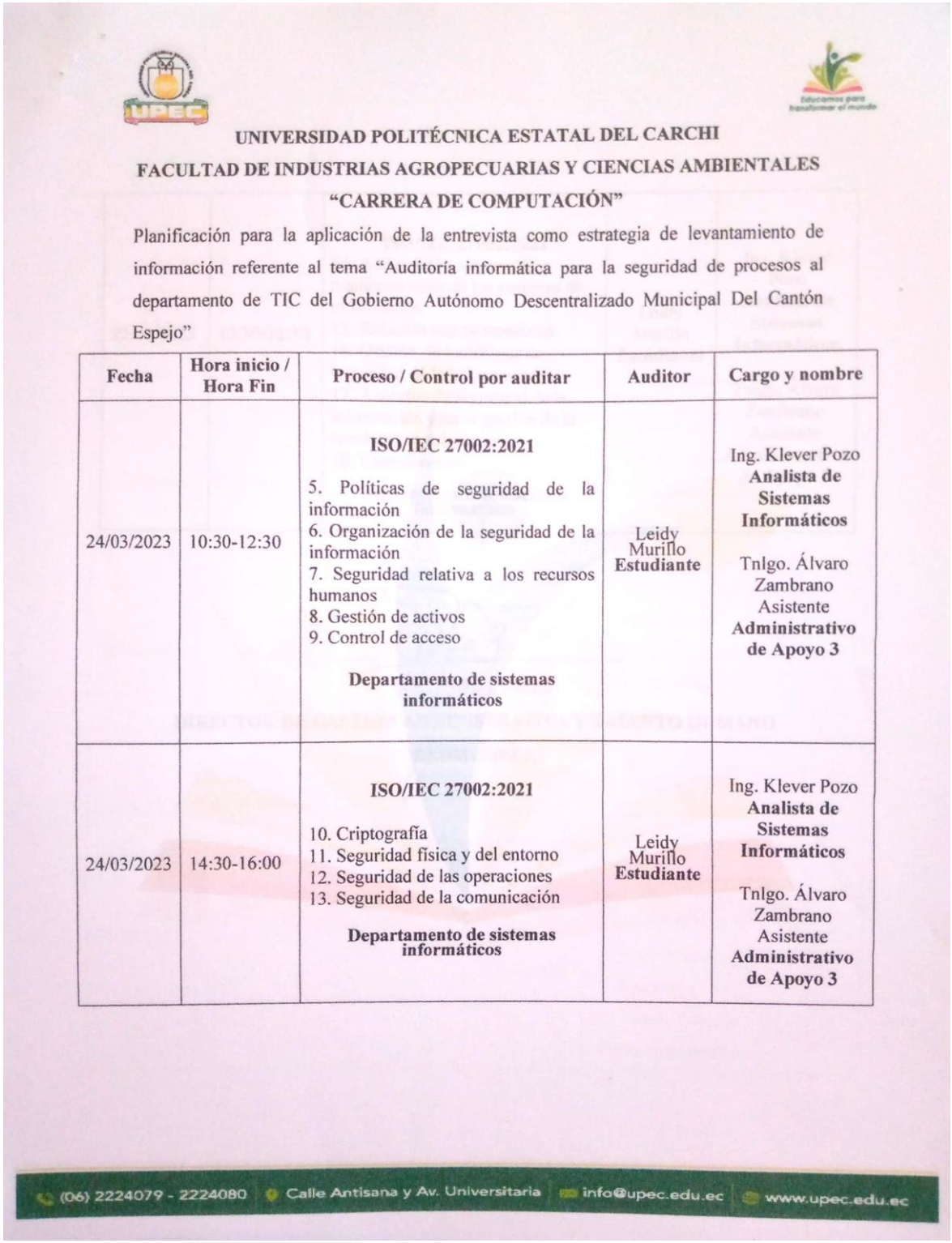
Segura que mi pedido será atendido favorablemente desde ya anticipo mis debidos agradecimientos.

Atentamente,

Srta. Leidy Murillo
CI. 0401968995
Estudiante de la Carrera de Computación
Universidad Politécnica Estatal del Carchi

(06) 2224079 - 2224080 Calle Antisana y Av. Universitaria info@upec.edu.ec www.upec.edu.ec

Anexo 11. Autorización para obtener información.



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

"CARRERA DE COMPUTACIÓN"

Planificación para la aplicación de la entrevista como estrategia de levantamiento de información referente al tema "Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo"

Fecha	Hora inicio / Hora Fin	Proceso / Control por auditar	Auditor	Cargo y nombre
24/03/2023	10:30-12:30	**ISO/IEC 27002:2021** 5. Políticas de seguridad de la información 6. Organización de la seguridad de la información 7. Seguridad relativa a los recursos humanos 8. Gestión de activos 9. Control de acceso **Departamento de sistemas informáticos**	Leidy Murillo **Estudiante**	Ing. Klever Pozo **Analista de Sistemas Informáticos** Tnlgo. Álvaro Zambrano Asistente **Administrativo de Apoyo 3**
24/03/2023	14:30-16:00	**ISO/IEC 27002:2021** 10. Criptografía 11. Seguridad física y del entorno 12. Seguridad de las operaciones 13. Seguridad de la comunicación **Departamento de sistemas informáticos**	Leidy Murillo **Estudiante**	Ing. Klever Pozo **Analista de Sistemas Informáticos** Tnlgo. Álvaro Zambrano Asistente **Administrativo de Apoyo 3**

(06) 2224079 - 2224080 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Anexo 12. Autorización para obtener información.

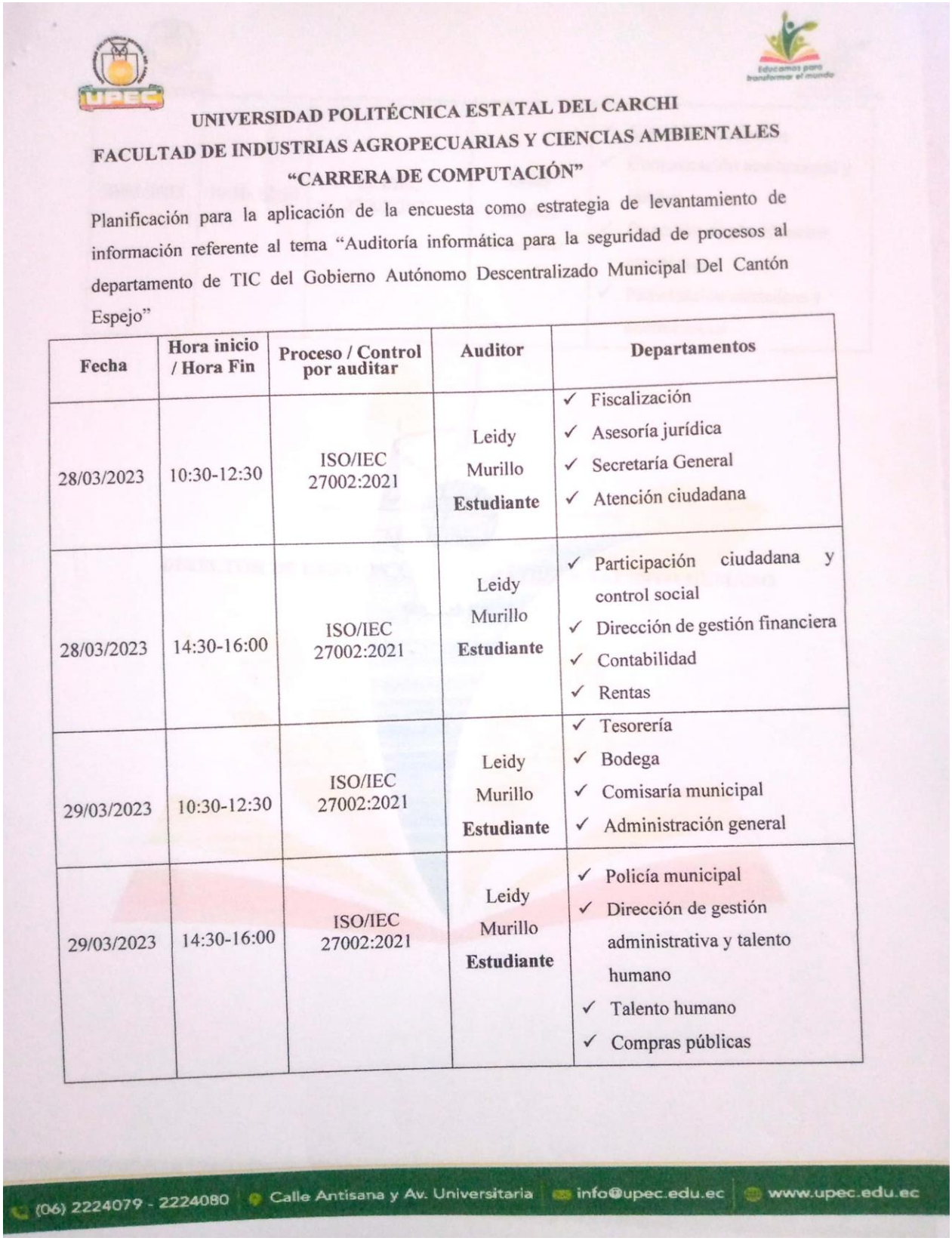
27/03/2023	10:30-12:30	**ISO/IEC 27002:2021** 14. Adquisición, desarrollo y mantenimiento de los sistemas de información 15. Relación con proveedores 16. Gestión de incidentes de seguridad de la información 17. Aspectos de seguridad de la información para la gestión de la continuidad del negocio 18. Cumplimiento **Departamento de sistemas informáticos**	Leidy Murillo **Estudiante**	Ing. Klever Pozo **Analista de Sistemas Informáticos** Tnlgo. Álvaro Zambrano Asistente **Administrativo de Apoyo 3**

Msc. Willman Cazares

DIRECTOR DE GESTIÓN ADMINISTRATIVA Y TALENTO HUMANO

GADM-ESPEJO

Anexo 13. Autorización para obtener información.



UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

"CARRERA DE COMPUTACIÓN"

Planificación para la aplicación de la encuesta como estrategia de levantamiento de información referente al tema "Auditoría informática para la seguridad de procesos al departamento de TIC del Gobierno Autónomo Descentralizado Municipal Del Cantón Espejo"

Fecha	Hora inicio / Hora Fin	Proceso / Control por auditar	Auditor	Departamentos
28/03/2023	10:30-12:30	ISO/IEC 27002:2021	Leidy Murillo **Estudiante**	✓ Fiscalización ✓ Asesoría jurídica ✓ Secretaría General ✓ Atención ciudadana
28/03/2023	14:30-16:00	ISO/IEC 27002:2021	Leidy Murillo **Estudiante**	✓ Participación ciudadana y control social ✓ Dirección de gestión financiera ✓ Contabilidad ✓ Rentas
29/03/2023	10:30-12:30	ISO/IEC 27002:2021	Leidy Murillo **Estudiante**	✓ Tesorería ✓ Bodega ✓ Comisaría municipal ✓ Administración general
29/03/2023	14:30-16:00	ISO/IEC 27002:2021	Leidy Murillo **Estudiante**	✓ Policía municipal ✓ Dirección de gestión administrativa y talento humano ✓ Talento humano ✓ Compras públicas

(06) 2224079 - 2224080 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Anexo 14. Autorización para obtener información.

30/03/2023	10:30-12:30	ISO/IEC 27002:2021	Leidy Murillo **Estudiante**	✓ Seguridad ciudadana ✓ Comunicación institucional y pública ✓ Dirección de planificación estratégica ✓ Participación ciudadana y control social

Msc. Willman Cazares

DIRECTOR DE GESTIÓN ADMINISTRATIVA Y TALENTO HUMANO

GADM-ESPEJO

(06) 2224079 - 2224080 | Calle Antisana y Av. Universitaria | info@upec.edu.ec | www.upec.edu.ec

Anexo 15. Certificado de finalización de auditoría informática.

Gobierno Autónomo
Descentralizado
Municipal de Espejo
Administración 2023 - 2027

Sistemas Informáticos

El Ángel 15 de Agosto de 2023.

CERTIFICADO

Por medio del presente y en mi calidad de Analista de Sistema Informáticos del Gobierno Autónomo Descentralizado Municipal de Espejo encargado de la Unidad de Sistemas Informáticos, me permito Certificar la culminación del proyecto "AUDITORIA INFORMÁTICA PARA LA SEGURIDAD DE PROCESOS AL DEPARTAMENTO DE TIC DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ESPEJO", mismo que se le permitió el levantamiento de información de normativas y políticas para la utilización de norma ISO/IEC 27002 en la Unidad; entregando a entera satisfacción el plan de contingencia que permitirá al GADME disminuir riegos de seguridad de información. En tal sentido me permito agradecer al estudiante de la carrera de computación de la Universidad Politécnica Estatal del Carchi; Leidy Tamara Murillo Ruano, con CI: 0401968995, por el trabajo realizado.

Particular que comunico para los fines pertinentes.

Atentamente,

Ing. Klever Pozo

Analista de Sistemas Informáticos