UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES

CARRERA DE INGENIERÍA EN INFORMÁTICA

Tema: "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán"

Trabajo de titulación previa la obtención del
título de Ingeniera en Informática

AUTOR(A): Joselin Pamela Igua Alvarez

TUTOR(A): Msc. Jairo Vladimir Hidalgo Guijarro

Tulcán, 2022

CERTIFICADO JURADO EXAMINADOR

Certificamos que la estudiante Igua Alvarez Joselin Pamela con el número de cédula 0402036032 ha elaborado el trabajo de titulación: "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán"

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

f.....	**f.....**
Hidalgo Guijarro Jairo Vladimir, Msc.	Yandún Velasteguí Marco Antonio, Msc.
TUTOR	**LECTOR**

Tulcán, marzo de 2022

AUTORÍA DE TRABAJO

El presente trabajo de titulación constituye requisito previo para la obtención del título de **Ingeniera** en la Carrera de ingeniería en informática de la Facultad de Industrias Agropecuarias y Ciencias Ambientales

Yo, Igua Alvarez Joselin Pamela con cédula de identidad número 0402036032 declaro: que la investigación es absolutamente original, auténtica, personal y los resultados y conclusiones a los que he llegado son de mi absoluta responsabilidad.

f.....
Igua Alvarez Joselin Pamela
AUTORA

Tulcán, marzo de 2022

ACTA DE CESIÓN DE DERECHOS DEL TRABAJO DE TITULACIÓN

Yo, Igua Alvarez Joselin Pamela declaro ser autor/a de los criterios emitidos en el trabajo de investigación: “Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán” y eximo expresamente a la Universidad Politécnica Estatal del Carchi y a sus representantes legales de posibles reclamos o acciones legales.

f.....
Igua Alvarez Joselin Pamela
AUTORA

Tulcán, marzo de 2022

AGRADECIMIENTO

A la Universidad Politécnica Estatal del Carchi por su calidad académica aportada en la formación profesional, brindando la oportunidad de cumplir los objetivos inicialmente planteados.

A la Carrera de Ingeniería en Informática, por permitir formar parte del proceso estudiantil mediante su personal académico y administrativo, quienes brindaron su apoyo durante todo el transcurso.

Al Departamento de Sistemas del GAD – TULCÁN a cargo del Ing. Freed Carrera y funcionarios dentro del área, por su colaboración indispensable para la culminación del proyecto de investigación.

Expreso mi gratitud a los docentes: Msc Jairo Hidalgo, tutor y Msc. Marco Yandún, lector; por su paciencia, dedicación y por compartir sus conocimientos aportados para finalizar la investigación mediante su orientación.

DEDICATORIA

A Dios por darme la tranquilidad necesaria para enfrentar todas las dificultades durante este proceso y así culminar mis metas.

A mis padres Carlos y Carmen por ser el ejemplo perfecto de esfuerzo y sacrificio, por la protección y compañía que siempre me han brindado y jamás dejarme sola demostrando su confianza en mí.

A mi familia y amigos, a todas las personas que hicieron parte del transcurso que permitieron fortalecer de cierta manera cada una de las etapas durante el periodo universitario.

ÍNDICE

RESUMEN 13
ABSTRACT 14
INTRODUCCIÓN 15
I. PROBLEMA 16
1.1. PLANTEAMIENTO DEL PROBLEMA 16
1.2. FORMULACIÓN DEL PROBLEMA 17
1.3. JUSTIFICACIÓN 17
1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN 19
1.4.1. Objetivo General 19
1.4.2. Objetivos Específicos 19
1.4.3. Preguntas de Investigación 19
II. FUNDAMENTACIÓN TEÓRICA 20
2.1. ANTECEDENTES INVESTIGATIVOS 20
2.2. MARCO TEÓRICO 21
2.2.1 Sistema de gestión de seguridad de la información (SGSI) 21
2.2.2 Beneficios de un SGSI 22
2.2.3 Políticas de seguridad 22
2.2.4 ISO/IEC 27002 22
2.2.5 Dominios de la seguridad, objetivos de control y controles 23
2.2.6 Seguridad de la información 26
2.2.7 Seguridad informática 26
2.2.8 Importancia de la seguridad de la información 26
2.2.10 Confidencialidad de información 26
2.2.11 Integridad de información 27
2.2.12. Disponibilidad de la información 27

2.2.13 Delitos informáticos 27
2.2.14 Vulnerabilidad, amenaza y riesgo 27
2.2.15 Vulnerabilidad informática 27
2.2.16 Amenazas informáticas 28
2.2.17 Riesgos informáticos 28
2.2.18 Auditoria Informática 28
2.2.19 Auditoría interna 28
2.2.20 Verificación 29
2.2.21 Metodología de una Auditoria Informática 29
2.2.22 Informe 30
2.2.23 Plan de auditoría 31
2.2.24 Gestión de la información 31
2.2.25 Gestión de riesgos tecnológicos 31
2.2.26 Análisis de riesgos 31
2.2.27 Matrices de riesgos 31
2.2.28 Probabilidades de impacto 32
2.2.29 Plan de mitigación 32
III. METODOLOGÍA 34
3.1. ENFOQUE METODOLÓGICO 34
3.1.1. Enfoque 34
3.1.2. Tipo de Investigación 35
3.2. IDEA A DEFENDER 35
3.3 DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES 36
3.4. MÉTODOS UTILIZADOS 37
3.4.3 Población y tipo de muestreo 37
3.4.4 Técnicas e instrumentos 38
IV. RESULTADOS Y DISCUSIÓN 39

4.1. RESULTADOS 39
4.1.1 Datos informativos 39
4.1.2 Auditoría informática 43
4.1.3 Estudio inicial 43
4.1.4 Propuesta 52
4.1.5 Plan de auditoría 52
4.1.6 Informe de Resultados 63
V. CONCLUSIONES Y RECOMENDACIONES 98
5.1. CONCLUSIONES 98
5.2. RECOMENDACIONES 99

ÍNDICE DE FIGURAS

Figura 1 Dominios, objetivos de control y controles 25
Figura 2 PDCA 30
Figura 3 Matriz de probabilidad e impacto 32
Figura 4 Logotipo GAD Municipal de Tulcán 39
Figura 5 Ubicación GAD Municipal de Tulcán 39
Figura 6 Estructura Organizacional Funcional 42
Figura 7 Proceso de desarrollo de sistemas 53
Figura 8 Proceso de administración de base de datos 54
Figura 9 Proceso de administración web 55
Figura 10 Proceso de administración de red 56
Figura 11 Proceso de licenciamiento de software 57
Figura 12 Cumplimiento de controles 61
Figura 13 Porcentaje de cumplimiento actual 64
Figura 14 Porcentaje total del cumplimiento actual 64
Figura 15 Porcentaje de cumplimiento en una posible implementación 66
Figura 16 Porcentaje total del incremento de cumplimiento implementado 66

ÍNDICE DE TABLAS

Tabla 1. Familia ISO/IEC 27000 23
Tabla 2. Definición de variables 36
Tabla 3. Técnicas de levantamiento de información. 44
Tabla 4. Desarrollo de sistemas informáticos 53
Tabla 5. Administración de base de datos 54
Tabla 6. Administración Web 55
Tabla 7. Administración de redes 56
Tabla 8. Soporte técnico 57
Tabla 9. 14 Dominios, 35 Objetivos de control 114 controles 58
Tabla 10. Porcentaje de cumplimiento 63
Tabla 11. Incremento de cumplimiento en implementación de controles 65
Tabla 12. Estrategias de mitigación ISO/IEC 27002 67
Tabla 13. Riesgos externos 93
Tabla 14. Riesgos Internos 93
Tabla 15 Probabilidad - Impacto 95

ÍNDICE DE ANEXOS

Anexo 1: Certificado o Acta del Perfil de Investigación 107
Anexo 2: Certificado del Abstract por parte de idiomas 108
Anexo 3: Informe emitido por Turnitin 110
Anexo 4 Certificado de Culminación 111
Anexo 5 Aprobación para realizar la investigación en la Institución 112
Anexo 6 Solicitud de entrevista 113
Anexo 7 Entrevistas 114
Anexo 8 Solicitud de Verificación de Cumplimiento 116
Anexo 9 Oficio Entrega del Informe Ejecutivo 117
Anexo 10 Informe ejecutivo 117

RESUMEN

La presente investigación analiza los procesos realizados dentro del Departamento de Sistemas del municipio de Tulcán basados en la norma ISO/IEC 27002, debido a las limitaciones en temas de seguridad de la información se han implementado escasos controles de seguridad que puede afectar a la confidencialidad, disponibilidad e integridad de la información, al no garantizar la protección necesaria se realiza un análisis por medio de instrumentos de investigación, aplicados directamente a funcionarios del área, al jefe del departamento y a dos funcionarios para corroborar la información, y la observación en base a una matriz de controles del esquema gubernamental de seguridad de la información, este proceso permitió conocer de manera detallada las deficiencias que se contemplan dentro de los 14 dominios, 35 objetivos de control y 114 controles existentes en la normativa. Además, dentro de la metodología el enfoque mixto facultó el análisis de la documentación y fundamentación teórica para la aplicación de un plan de mitigación de riesgos tecnológicos tomando como referencia los hallazgos obtenidos por medio de la metodología de implementación del sistema de gestión de la seguridad de la información, PHVA, planear, hacer, verificar y actuar; se emitió un informe de resultados con el porcentaje cumplimiento que el área tiene actualmente, el que permite desarrollar posteriormente la matriz de riegos tomando en cuenta el porcentaje de probabilidad e impacto. Finalmente, se estableció estrategias de mitigación de riesgos internos y externos con potenciales amenazas que pueden efectuarse, determinando controles que se pueden poner en práctica a determinados sucesos.

Palabras clave: Seguridad de la Información, matriz de riesgos, auditoría informática, ISO/IEC 27002.

ABSTRACT

The current research analyzes the processes fulfilled by the Systems Department of the ¨GAD-TULCAN¨ grounded on the ISO/IEC 27002 standard, due to the restrictions in information about security issues; in fact, limited security controls have been implemented which can affect confidentiality, availability, and integrity of the information; subsequently, as the necessary protection is not guaranteed, an analysis is carried out through research instruments, applied directly to officials from the ICT Area, the director of the department and two officials to validate the information, besides; through observation based on a matrix of controls of the government information security scheme; therefore, this process allowed to recognize in detail the deficiencies that are contemplated within the 14 domains, 35 control objectives and 114 existing controls in the regulations. In addition, by implementing this methodology, the mixed approach enabled the analysis of the documents and theoretical foundation for the application of a technological risk mitigation plan, taking into apart as orientation the conclusions obtained through the methodology of implementation of the security management system of the information, PHVA, planning, doing, checking and acting. Although, a results report was issued with the percentage of compliance that the area currently develops, allowing to the risk matrix to be subsequently settled, by considering the percentage of probability and impact. Finally, internal and external risk mitigation strategies were established with potential threats that can be carried out by determining controls that can be placed into practice in certain events.

Keywords: Information Security, risk matrix, computer audit, ISO/IEC 27002.

INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Municipal de Tulcán es una institución que tiene como finalidad solventar inquietudes de los ciudadanos del cantón Tulcán, brindando procesos de gestión vinculando vocación de servicio a la sociedad.

En la estructura orgánica funcional cuenta con el área de Dirección Administrativa que enlaza directamente al Departamento de Sistemas que se encarga de realizar procesos de gestión y administración de tecnología, servicios en línea, intranet, teniendo como objetivo contribuir el cumplimiento correcto de procesos institucionales, tomando en cuenta que es un área de priorización encargada de proveer información confidencial, además se ocupa de proporcionar herramientas necesarias para la protección de recursos creando estrategias de servicios, planificaciones de control y gestiones referentes a uso de datos.

El propósito de esta investigación fue generar un informe de estrategias de mitigación de riesgos tecnológicos por medio del análisis aplicado basado en la normativa internacional ISO/IEC 27002:2013, así se realizaron hallazgos mediante la estructura de auditoría informática con la finalidad de reducir el impacto de riesgos tecnológicos y prevenir riesgos que puedan ocasionarse en procesos institucionales, desarrollando mejoras continuas a corto, mediano y largo plazo. La importancia que brinda una auditoría informática es muy relevante ya que está encargada de verificar el cumplimiento de acciones o procedimientos realizados en un área específica, pero de manera objetiva planificando procesos protección de información que constituye como prioridad a la confidencialidad, disponibilidad e integridad, de manera que su eficacia sea vea reflejado en los sistemas informáticos y en actividades de gestión del Departamento de Sistemas.

I. PROBLEMA

1.1. PLANTEAMIENTO DEL PROBLEMA

Según Rodríguez, D (2017) menciona que:

Los sistemas virtuales han tomado un rol indispensable para una institución, organización o empresa. Por lo tanto, implica conocer sus falencias y estar actualizados debido a las nuevas amenazas informáticas teniendo un apropiado control sobre todo lo que posee la entidad. Por esto, resulta importante poseer un sistema de gestión de seguridad de la información (SGSI).

El crecimiento en las entidades que se desarrollan a nivel internacional es exponencial, muchas de ellas no cuentan con los pilares fundamentales de control de seguridad debido a que no se aplican de manera integral métricas o estrategias que permitan tener claridad sobre los requerimientos de la organización, generando grietas de recurso de un buen cumplimiento de procesos, dinámicas y controles que aportan a las buenas prácticas. (Ibarbo, L y Giraldo, V. 2019)

En el Ecuador debido a las limitaciones tecnológicas no se ha implementado SGSI y controles de seguridad generando innumerables inconvenientes por parte de funcionarios de las Instituciones como de usuarios, por ende, la escasa información que posee el personal que trabaja dentro de la institución no es bien ejecutada, es por eso que se debe aplicar la normativa establecida actualmente que abarca temas de seguridad de la información y políticas existentes sobre protección, definiendo que las instituciones obtienen un manejo masivo de datos e información privilegiada convirtiéndose así en un riesgo eminente. (Rocha, C. y Recalde, P., 2019).

El impacto que genera el no establecer estándares estratégicos para la seguridad de la información en procesos administrativos municipales afectan notablemente creando nuevas amenazas y sensibilizando las fases o actividades en temas organizativos, los municipios se encargan brindar seguridad dentro de los servicios correspondientes a su cargo, por lo tanto la información se caracteriza su prioridad por la sensibilidad que puede poseer y lo que puede generar si no existe planificaciones previas sobre estrategias de mitigación con un diagnóstico previo a la situación actual de la institución. (Bolaños. F, y Chica. I 2017)

Las instituciones públicas y privadas en la provincia del Carchi que respaldan sus actividades y toma de decisiones deben incluir todos los criterios en los pasos necesarios para garantizar la calidad y seguridad de su efectividad y transparencia. La falta de lineamientos de seguridad en la información no admite una inspección adecuada del manejo de los datos, por lo tanto, existe la posibilidad que la información pueda ser mal utilizada enfocándose en perjudicar directamente a la empresa.

La gestión y planeación sobre la seguridad de la información involucran recursos que requieren de tiempo y esfuerzo entre otros que normalmente no se ejecutarían en las organizaciones, estas son algunas de las razones por las que las no priorizan las acciones de gestión de riesgos, las instituciones que comprenden el valor de los activos conocen la responsabilidad que abarca la inversión de su protección, por lo tanto, tiende a seguir el estándar familiar ISO 27002

Según (Ley Orgánica de Telecomunicaciones) menciona qué: "El ministerio encargado del sector de las Telecomunicaciones y de la Sociedad de la Información es el órgano rector de las telecomunicaciones, la informática y tecnologías de la información"

La comunicación e información, la prestación de servicios, los procesos y el uso de herramientas técnicas tienden a ser una demanda al utilizarlos, siendo requeridos por las autoridades públicas y su personal. El alto potencial de estas herramientas y su uso inadecuado se forjan como armas para instigar fraudes e información ilegal y distribución de la misma o poner en vulnerabilidad a su infraestructura dejando en riesgo a su organización.

1.2. FORMULACIÓN DEL PROBLEMA

Debido a las limitaciones en temas de seguridad de la información se han implementado escasos controles de seguridad que puede afectar a la confidencialidad, disponibilidad e integridad de la información en el Municipio de Tulcán.

1.3. JUSTIFICACIÓN

Rodríguez D (2017) manifiesta que:

Las personas que gestionan los datos sensibles, estrategias de negocio y otro tipo de información, en su mayoría son personas anónimas. Dejando a los demás empleados y clientes alejados de sistema de seguridad. Ahí es cuando, un caso de espionaje causaría un daño fatal, dado que uno de los mayores vectores de ataque es la misma red. Fundamentalmente porque la gente se siente "protegida" por estas personas anónimas, por lo tanto, tienden a bajar la guardia en la red interna, desconociendo lo que pasa y dando por sentado sus propias especulaciones de la seguridad.

Por estas amenazas se ha desarrollado documentos o regulaciones que brindan orientación sobre cómo combatir con situaciones que pueden presentar ciertos tipos de amenaza, posible riesgo o vulnerabilidad, causando serios problemas dependiendo de la protección de las instituciones y especialmente al departamento de sistemas que es el encargado de su máximo resguardo.

Dentro de las organizaciones frecuentan fallas en el sistema de gestión de la seguridad de la información, por ende, establecen documentación fundamental que brindan soporte a la planeación interna, realizando ajustes a una proposición de mejora global en distintas áreas, con

la finalidad obtener protección a la información, además, su certificación garantiza un verdadero soporte que necesitan las entidades actualmente.

No existe limite de datos, toda la información almacanada en los sistemas es valiosa dependiendo de su categorización, como se registres y se almacenen depende de la sensibilidad o privacidad, con la finalidad de avalar estrategias de protección contra la extensa escala que existe de amenazas minimizando risgos y maximizando rendimiento, se puede lograr mediante la implementación de controles y procesos apropiados que deben establecer mejora cuando sea necesario cumpliendo los objetivos establecidos en la organización. (Kurniawan, E. y Riadi, I., 2018)

En la ciudad de Tulcán es indispensable mantener políticas o normativas que respalden la seguridad de la información ya sea en organizaciones públicas o privadas que posteriormente puedan efectuar su implementación y análisis de forma continua, logrando con ello proteger de manera adecuada los activos es decir toda aquella información indispensable, de esta forma se verifica el cumplimiento de las premisas que corresponden de la a la protección de información, en base a los distintos dominios y controles de seguridad, así se realizaría una mejora continua en las organizaciones.

La institución brinda la autorización necesaria para realizar la investigación, debido a que se efectuó una revisión previa del estado actual del departamento de sistemas ya que se encontraron diversas falencias y muestran interés de optimizar lo acontecido, por lo tanto, es oportuno proponer estrategias que logren salvaguardar las acciones que dependen del área de sistemas.

Considerando el acuerdo ministerial N° 025-2019

El Ministerio de Telecomunicaciones y de la sociedad de la información acuerda:

Art 1. Expedir el Esquema Gubernamental de Seguridad de la Información – ESGSI-, el cual es de implementación obligatoria en las Instituciones de Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Art 2. Recomendar a las Instituciones de Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, realizaran la Evaluación de Riesgos sobre sus activos de información críticos y diseñaran el plan para el tratamiento de riesgos de su Institución.

Art 3. Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía la norma técnica ISO/IEC 27000 para la Gestión de Seguridad de la Información.

1.4. OBJETIVOS Y PREGUNTAS DE INVESTIGACIÓN

1.4.1. Objetivo General

Proponer el sistema de gestión de seguridad de la información para garantizar la confidencialidad disponibilidad e integridad de la información en el Municipio de Tulcán.

1.4.2. Objetivos Específicos

- Fundamentar bibliográficamente el uso de la norma ISO/IEC 27002:2013 para no afectar la confidencialidad, disponibilidad e integridad de la información.
- Examinar los controles de seguridad informática implementados en el Municipio de Tulcán.
- Establecer criterios para la mitigación y/o cumplimiento normativo con las recomendaciones y actividades a llevarse a corto, mediano y largo plazo.
- Generar el informe ejecutivo basado en hallazgos generados de la matriz de riesgos y criterios de mitigación a través de análisis de resultados y cumplimiento de controles.

1.4.3. Preguntas de Investigación

- ¿Qué es un Sistema de Gestión de Seguridad de la Información?
- ¿Qué es seguridad informática?
- ¿Cuáles son los controles de seguridad informática?
- ¿Cuáles son las características de la seguridad de la información?
- ¿Cómo se implementan las buenas prácticas y controles de seguridad?
- ¿Cómo se analiza la implementación de las buenas prácticas y controles de seguridad?
- ¿Cómo perjudica el mal rendimiento en la gestión de las actividades en la empresa?

II. FUNDAMENTACIÓN TEÓRICA

2.1. ANTECEDENTES INVESTIGATIVOS

Según el estudio que se realizó en la Universidad Técnica de Ambato "Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo" facultad de ingeniería de sistemas, ciudad de Ambato - Ecuador. Criollo, S. (2017)

El análisis de la investigación recopila información sobre la situación actual, buscando mitigar riesgos a la diversidad de amenazas se sometió a ser evaluada en base a la normativa ISO 27002 en su versión 2013, planificando y ejecutando estrategias de implementación con el objetivo de brindar la seguridad necesaria para la información que se recauda diariamente en la institución manteniendo procesos adecuados garantizando la confidencialidad, disponibilidad e integridad. Como resultado al incorporar estándares internacionales contribuye al desarrollo del análisis que permite detectar vulnerabilidades posibles en la red del GAD municipal de Salcedo, resolviendo así problemas de manera interna o externa definiendo políticas para la seguridad de la información designando personal correspondiente al control de las mismas, con el fin de proporcionar beneficios de protección que adopta la institución.

Se realiza la investigación "Aauditoría de la seguridad informática basado en la ISO 27001 sistema de gestión de seguridad de la información para el GAD municipal de Milagro" (Paguay, C., y Zamora, G. 2017)

Se analiza las políticas definidas en la empresa sobre la protección de la información, como se lleva a cabo la gestión ante desastres naturales y el manejo de las condiciones básicas dentro de la confidencialidad, disponibilidad e integridad que se expone a distintos tipos de amenazas, destacando el incorrecto uso de los activos que tienen bajo su responsabilidad los funcionarios de la entidad.

Mediante el análisis se logró conocer el nivel de vulnerabilidad y detallar los procedimientos de manera apropiada que permite evitar la exposición de la información mejorando sus políticas de calidad disminuyendo los peligros posibles a existir basados en el diseño del SGSI y las estrategias de progreso continuo en procedimientos operativos.

El estudio realizado en la institución Universitaria Politécnico Grancolombiano "Diseño del sistema de gestión de la seguridad de la información (SGSI) para la administración municipal del municipio de la ceja Antioquia, bajo los lineamientos emitidos por el programa G.E.L" de la facultad de ingeniería y ciencias básicas. (Tobón, A. 2018)

Esta investigación logra la identificar las necesidades de la institución, los recursos sobre temas de seguridad de la información retrasan la prevención de escenarios dañinos, por ello se

desarrollarán estrategias para Gobierno Digital solucionando la problemática existente alineados al estándar de seguridad de la información y la metodología Magerit para realizar el análisis de riesgos, ejerciendo su cumplimiento de carácter obligatorio.

El resultado del estudio posterior a su implementación se proyecta mayor eficiencia, transparencia en las actividades participativas de los funcionarios aprovechando el fortalecimiento en la seguridad de la información garantizando protección y confidencialidad a los datos de la ciudadanía y funcionarios de la institución.

Según la investigación realizada en la Universidad Nacional y a Distancia, en Tecnología e Ingeniería, "Diseño de un sistema de gestión de seguridad de información bajo la norma ISO27001:2013 en la E.P.S ASMET SALUD" en Especialización en seguridad Informática, Colombia. Reyes, J. (2019)

Realiza un análisis sobre peligros y amenazas dentro de la empresa, mediante la implementación de un (SGSI) Sistema de Gestión de la Seguridad de la Información, con la finalidad de estandarizar estrategias que garanticen seguridad en los procesos del establecimiento, se fundamenta en modelos y estándares de la norma ISO/IEC 27002, formalizando estrategias técnicas apropiadas para la mejora continua.

Se logra comprobar el desempeño que se efectúa al implementar un SGSI y mediante los controles de la ISO 27002 esta norma vigente proporciona seguridad generando protección frente a amenazas y mitigando los riesgos existentes.

En la universidad Oberta de Catalunya con "Plan de implementación de un SGSI basado en la norma ISO 27001:2013 en el ámbito de la Administración Pública Argentina" en base al análisis realizado, la organización tiene implementado un SGSI que no fue actualizado en varios años, lo que causó la aparición de riesgos de alto impacto, por ende, el objetivo es adecuar los controles necesarios para verificar su cumplimiento. Roberti, B (2020).

A través del análisis se identificó riesgos críticos que en la normativa se disminuye potencialmente la brecha que generó inconvenientes hace años atrás al no verificar de manera periódica su cumplimiento.

2.2. MARCO TEÓRICO

2.2.1 Sistema de gestión de seguridad de la información (SGSI)

Según Nieves, A., (2017)

La información es una colección organizada de datos de gran valor para las instituciones, sin importar como se almacene o se envíe, su propósito es establecer distintos mecanismos para gestionar el correcto funcionamiento de procesos sin afectar el esquema de seguridad, ejecutado

por estándares previamente definidos y evaluados. La finalidad del SGSI es identificar los activos y al personal que a través de procesos de gestión de riesgos brindan apoyo hacia los sistemas informáticos, se puede mitigar riegos mediante controles, integrando las políticas y procedimientos establecidos.

2.2.2 Beneficios de un SGSI

La implementación de un SGSI demuestra la importancia que brinda el utilizar metodologías con el fin de mitigar riesgos, analizando distintos controles que preservan la confidencialidad, disponibilidad e integridad de la información, verificando particularidades del objeto aplican beneficios al modelo organizacional. (Sarmiento, W. 2020)

- Organizar procesos internos.
- Mitigar riesgos.
- Disponer de información integra.
- Contar con herramientas para mejorar el desarrollo de las labores.
- Mejorar tiempo evitando repetición de procesos.
- Mejora de comunicación interna y externa.
- Incrementar la posición de la empresa.

2.2.3 Políticas de seguridad

Estas normas de seguridad regulan maneras de proteger y dirigir objetivos implementados en organizaciones, garantizando convicción en activos informáticos, a su vez en infraestructura, al ser implementada disminuye el riesgo mediante buenas prácticas, el personal autorizado ayuda a monitorear el desempeño en los controles que se establece a fin de evitar posibles amenazas y violaciones de seguridad. (Rojas, D., Padilla, N., y Peña, Y., 2018)

2.2.4 ISO/IEC 27002

Se especifican dominios, objetivos y controles aplicados directamente a la solidez de los activos dentro de las entidades. La norma ISO/IEC 27002:2013 proporciona directrices que brindan una protección de sus datos e información más sólida en cualquier entidad u organización, gracias a la evaluación y la ejecución de controles. El SGSI establece fases de ejecución, dividiendo normas adecuadas dentro de la seguridad evitando riesgos en la información.
(Ramos, Y., Urrutia, O., Ordoñez, D., y Bravo, A., 2017)

- Norma certificable, se evidencia el compromiso prioritario a la seguridad de carácter estratégico y excelencia.
- Objetivos de seguridad medibles y mejora continua.
- Facilita el cumplimiento de requisitos legales y mitigar errores, desastres o sabotaje.

Tabla 1.
Familia ISO/IEC 27000

ISO 27000	Vocabulario estándar para el SGSI.
ISO 27001	Especifica los requisitos para la implantación del SGSI.
ISO 27002	Código de buenas prácticas para la gestión de seguridad de la información.
ISO 27003	Directrices para la implementación del SGSI.

2.2.5 Dominios de la seguridad, objetivos de control y controles

La organización Internacional de Estandarización ISO permite, planificar, ejecutar, verificar y proceder, interviniendo procesos guías de buenas prácticas aplicables con medidas de seguridad de la información su diseño hace referencia a 14 dominios que confortan controles propuestos por la norma ISO 27002 adoptados por organizaciones, verificando su cumplimiento y eficacia. (Huayamave, R. 2017)

- Políticas de seguridad: El objetivo velar por la seguridad afrontando riesgos de alto nivel y brindando protección que se necesita para proteger su información en determinados aspectos.
- Aspectos organizativos de la seguridad de la información: Su propósito es administrar la seguridad en las actividades de la organización ofreciendo apoyo y compromiso con la seguridad en procesos relevantes.
- Seguridad de los recursos humanos: Su finalidad no incrementar los riesgos protegiendo la información por medio de las responsabilidades establecidas adecuadamente en su contratación laboral, reduciendo riesgos de error humano en la autorización de información y manejo de instalaciones.
- Gestión de activos: Su objetivo es tener conocimiento sobre los activos informáticos de la empresa, su clasificación se debe establecer según la sensibilidad o la funcionalidad que cumplen para proteger la información.
- Control de acceso: Es la verificación directa que tiene una organización solicitando acceso a zonas restringidas controlando los procesos de la información.
- Cifrado: Se hace uso para salvaguardar la información mediante algoritmos que ayudan a aumentar la seguridad y así establecer confidencialidad e integridad.
- Seguridad física y ambiental: Protege de amenazas a los sistemas informáticos mediante barreras y ubicándose en áreas seguras, aplicando procedimientos de control minimizando daños e interferencias en las operaciones de la organización.

- Seguridad en la operativa: Esto permite determinar los procedimientos, desarrollo y mantenimiento de la documentación, los empleados deben tener conocimiento en su responsabilidad de la infraestructura de la organización.
- Seguridad de las telecomunicaciones: Asegura el control de las transmisiones de datos internas o externas, manteniendo la privacidad e integridad de la información.
- Adquisición, desarrollo y mantenimiento de los sistemas de información:
  Se dirige hacia el desarrollo de técnicas que garanticen seguridad en procesos dentro de su ciclo de vida, verificando sus actualizaciones y el soporte que se brinda.
- Relaciones suministrables: Se implementa y mantiene un nivel apropiado en la información comprobando la implementación de acuerdos y entrega de servicios contratados en línea.
- Gestión de incidentes en la seguridad de la información:
  Certifica las correcciones preventivas en un lapso adecuado, brindando procesos de mejora continua para evitar incidentes de seguridad gestionando su cumplimiento en su totalidad.
- Aspectos de seguridad de la información en la gestión de la continuidad del negocio: Su finalidad es resguardar la información de riegos inevitables durante períodos de reactivación de planes y procedimientos cotidianos, analizando consecuencias o fallas para implantar planes de contingencia.
- Cumplimiento: Busca evitar incumplimientos de reglamentos que tengan correlación con el resguardo de información, garantizando que realicen operaciones de acuerdo a las normativas determinadas.

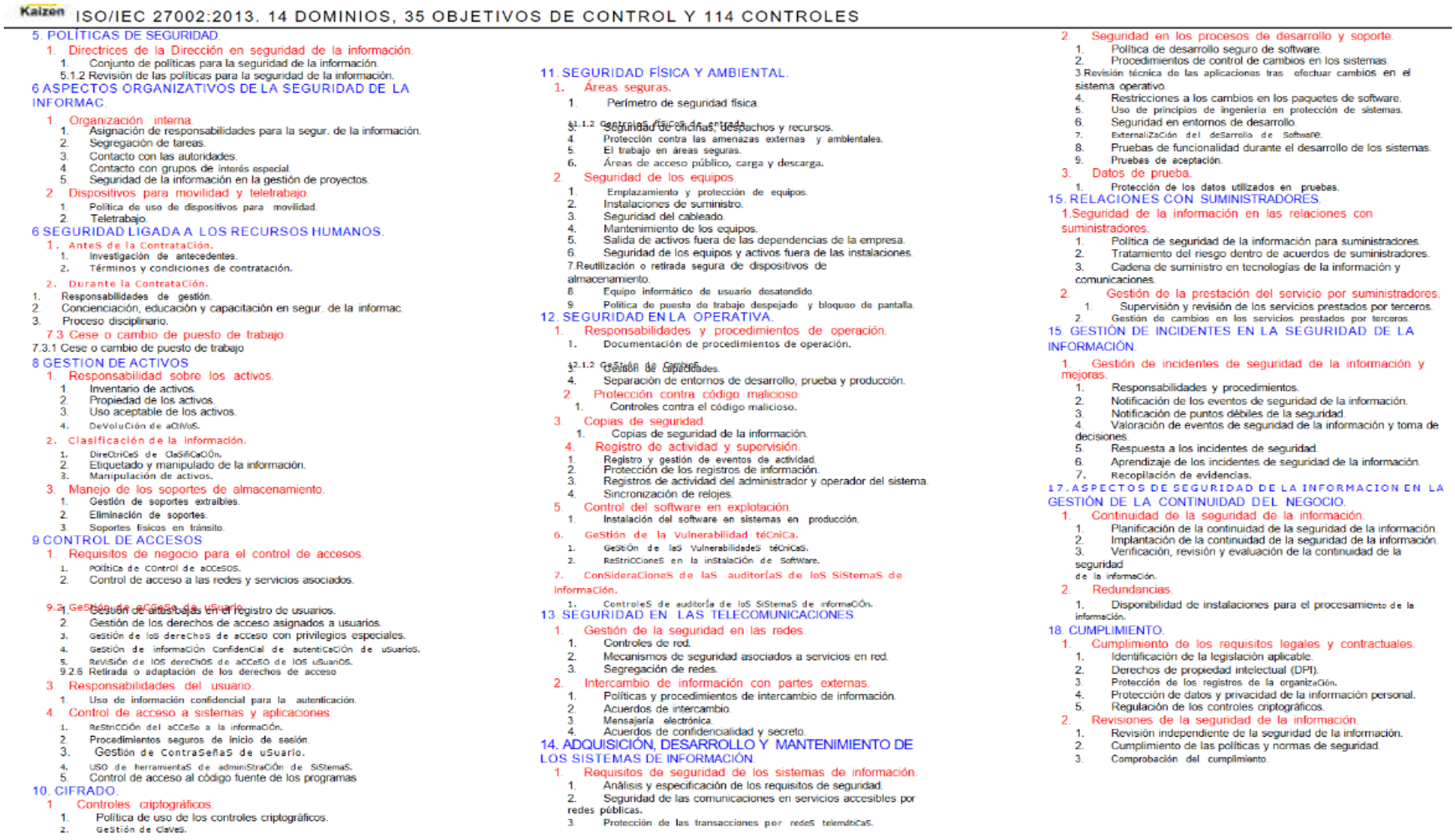


Figura 1 Dominios, objetivos de control y controles
Fuente: https://es.scribd.com/document/283710204/Estructura-ISOIEC-27002-2013-pdf

2.2.6 Seguridad de la información

Establecen medidas de prevención que resguardan y protegen la información para disminuir la probabilidad de amenazas que causan deterioro en las entidades para así mejorar la seguridad de los activos.

De manera detallada podemos encontrar los requerimientos en la norma ISO/IEC 27002 para lograr conservar beneficios específicos que se asocia a su implementación mediante los de controles de seguridad basados en las necesidades que proyecta la institución, brindando un servicio o una acción en específico, dependiendo de los objetivos y los alcances del SGSI que se definan. (Valencia, F., y Orozco, M., 2017)

2.2.7 Seguridad informática

"Se entiende por seguridad informática como la ciencia que se encarga plantear normas o técnicas con la finalidad de adecuar un sistema de información óptimo, confiable y seguro, minimizando riesgos eventuales ante amenazas que pueden acontecer". (Tellez, E. 2018)

2.2.8 Importancia de la seguridad de la información

Gómez, R. (2017) menciona que:

La información es esencial para el funcionamiento de una empresa y para la operación segura de sus actividades, lo que significa que la información debe protegerse como el activo más importante. Con el uso creciente de Internet, la evolución tecnológica y la falta de conocimiento para reducir el riesgo de ataques, las vulnerabilidades organizacionales ahora pueden usarse para amenazar a las empresas y causar daños. Todas las características necesarias para preservar la información: disponibilidad, integridad, confidencialidad.

2.2.9 Activos de la información

Es lo que la empresa u organización tiene con mayor validez, estos pueden distinguirse en distintas áreas dentro de soportes como papel o medios digitales, todo activo de información tiene un propietario generalmente es el dueño del proceso quien se encarga de establecer las medidas que sean necesarias para salvaguardar estos activos a su cargo. (Borrero, P. 2019)

2.2.10 Confidencialidad de información

Información que no debe ser divulgada sin consentimiento del usuario garantizando que es accesible por cierta autoridad determinada, la seguridad reciproca que se genera en hacia el usuario en cualquier tipo de operación, la organización queda comprometida a cualquier mecanismo. (Niño, N. 2018)

2.2.11 Integridad de información

La integridad de la información es la convicción de no alterar o modificar la información manteniendo los datos exactos sin ninguna manipulación, normalmente la integridad hace referencia a la fidelidad de la información previniendo cambios impropios, el objetivo es mantener su autenticidad. (Ferruzola, E., Duchimaza, S., Ramos, J., y Alejandro, M. 2019)

2.2.12. Disponibilidad de la información

Certeza de la información inmediata al ser requerida por usuarios autorizados, su finalidad es evitar interrupciones sin autorización previa del área de sistemas, manteniendo el equilibrio en diversos factores adecuados para la funcionalidad de la gestión de servicios que brindan las organizaciones. (Torres, C. 2020)

2.2.13 Delitos informáticos

Acción antijurídica cometida en espacios digitales o medios informáticos con el objetivo de robar, estafar, modificar información, entre otros; afectado directamente a la empresa y usuarios, atentando a la seguridad perjudicando a los usuarios, funcionarios y a la institución, son hechos ilícitos comprendidos por un conjunto de comportamientos que pueden ejecutarse de manera indefinida e intangible. (Carrillo, C., y Montenegro, A. 2018)

2.2.14 Vulnerabilidad, amenaza y riesgo

Rodriguez D., (2017) afirma que:

Los conceptos de debilidad o vulnerabilidad, que forman parte de diversas áreas de los conceptos de seguridad, y las amenazas y riesgos asociados también se aplican en relación con el resguardo de datos informáticos. Las vulnerabilidades de seguridad se consideran debilidades en los sistemas informáticos. Una amenaza es el contenido, riesgo y ataque potencial que una persona (interna o externa) puede llevar a cabo para explotar los diferentes métodos de esa amenaza y ataque. Puede unirse a una organización específica.

2.2.15 Vulnerabilidad informática

La vulnerabilidad informática es una entrada directa a posibles ataques volviéndose una latente amenaza, siendo una debilidad causada por procesos incorrectos poniendo en riesgo la información y a la entidad responsable permitiendo fácil acceso a un ataque.

La eficacia en planes de contingencia y estrategias de seguridad disminuye la vulnerabilidad informática en cualquier evento, evitando afectar la información ante la presencia de atacantes sin importar la condición. (Quiroz, S,. y Macías, D,. 2017)

2.2.16 Amenazas informáticas

Las amenazas informáticas se pueden presentar en cualquier momento ocasionando algún incidente causando potenciales daños a la información o medios informáticos, tomando en cuenta que los ataques pueden ser ejecutados por terceros causando daños directos a la información, infraestructura o generando grandes inconvenientes en la organización.

"Analizando esta situación y entrando en la actualidad, a partir de los años 90's y hasta la fecha la comisión de delitos informáticos ha ido en aumento, por lo que puede provocar acceso abusivo a la información, daño, uso de software malicioso, entre otros." (Sanchez, Z. 2017)

- Ataques pasivos

  Los ataques activos se basan en no alterar la infraestructura con el objetivo de interceptar claves cuentas o algunos datos que permitan causar alteración o daños.

- Ataques activos

  Dentro de los ataques activos involucra el modificar o alterar la información, robo o sabotaje de la misma, muchas veces es causado por personas con un alto conocimiento informático.

2.2.17 Riesgos informáticos

Los riesgos informáticos son acontecimientos que se convierten sucesos reales provocando fugas de información, robos, fraude, y otros riesgos, afectando a activos informáticos y a la entidad, más aún al no tener los planes de contingencia para mitigar la vulnerabilidad es posible que la magnitud del impacto genere mayor peligro para los activos informáticos.

Esto se puede deducir que al estar en presencia de una amenaza y surge una vulnerabilidad asociada ante la misma entonces existe un riesgo. (Rodriguez, J,. y Sámchez, D,. 2019)

2.2.18 Auditoria Informática

Dentro de una auditoría informática se establecen normas y procedimientos con personal capacitado para el efecto, basándose en que la auditoría informática ocupa un campo más amplio que la detección de errores sino para evaluar y mejorar lo existente proponiendo alternativas de solución. Este proceso implica obtener requerimientos, y un análisis exhaustivo de las evidencias recolectadas para comprobar que mediante las normativas correspondientes se puede salvaguardar la información. García, C., (2016)

2.2.19 Auditoría interna

Soy una herramienta que la organización ayuda a determinar las posibles fallas del sistema, pero también por la posibilidad de mejorar los procesos internos, lo que permite: evaluar la efectividad de los controles internos. Compruebe el proceso de proceso y sistema en general.

Verifique y monitoree el cumplimiento de los estándares y procedimientos actuales. Analiza la aparición de nuevos riesgos, lo que permite la implementación de métodos para minimizar sus efectos al mínimo o neutralizar. Bailon, W. (2019)

2.2.20 Verificación

La verificación es un proceso que involucra diferentes fases y uso de herramientas con el objetivo de mejorar actividades exclusivas enfocado en la eficacia y lograr el cumplimiento de gestión y buenas prácticas creando estrategias para un valor agregado. (Caycedo, X. y Arcentales, D. 2017)

Se verifica mediante distintos aspectos:

- Física. La inspección por medio de la observación directa involucra la verificación de documentos, registros, disposición de equipos y usuarios involucrados.
- Documental. La verificación más común que obtiene el auditor en su investigación tanto internas como externas.
- Testimonial. Esta evidencia se obtiene por terceras personas en forma de declaraciones que ayudan en la investigación, por medio de entrevistas que efectúa el auditor.
- Analítica. Se obtiene mediante el análisis de datos y su verificación.

2.2.21 Metodología de una Auditoria Informática

- Estudio preliminar

  Se obtiene información a través de técnicas y herramientas establecidas previamente.
- Revisión y evaluación de controles y seguridades

  Realizar un análisis exhaustivo para dar soluciones y recomendaciones para la mejora continua.
- Examen detallado de áreas críticas

  Se profundiza en las áreas críticas para definir objetivos dentro de ella para determinar un alcance satisfactorio.
- Comunicación de resultados

Ciclo Deming (PDCA)

La implementación del sistema de gestión de la seguridad de la información solicita de una metodología con la finalidad de mejora continua, el PDCA se fragmenta en 4 procesos importantes: Planificación, ejecución, verificación y cumplimiento; una vez obtenido los resultados se efectuará la primera fase. Recalde, J (2019)

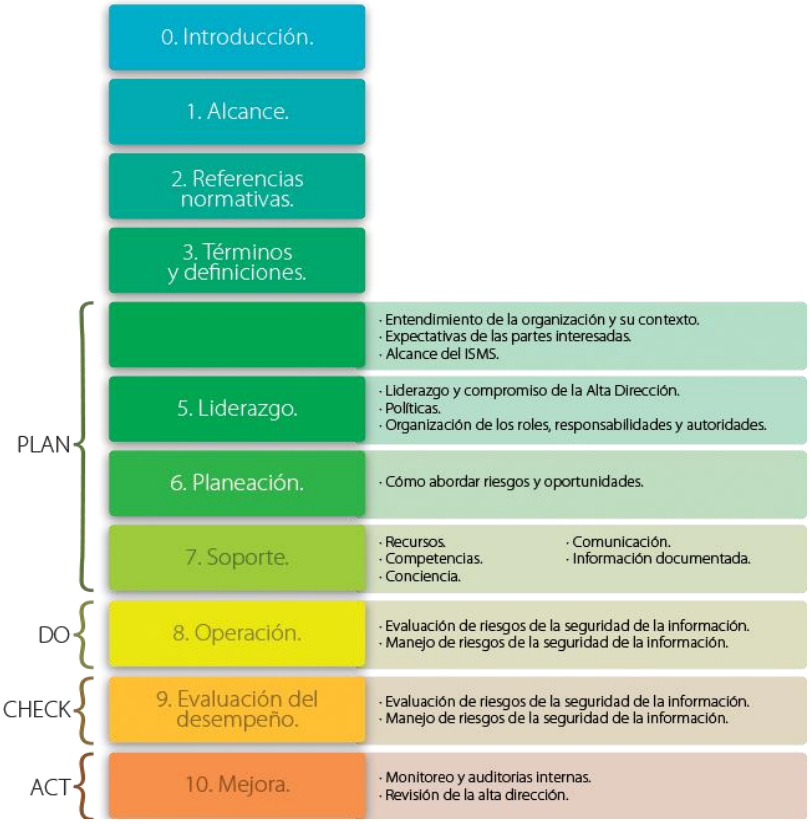


Figura 2 PDCA
Fuente: Proveda, F y Mollina, F. (2018) Recuperado de: https://www.researchgate.net/figure/Figura-2-Estructura-del-estandar-ISO-IEC-270012013-Gonzalez-Trejo-2013_fig2_333671914

2.2.22 Informe

El objetivo del informe es emitir opiniones sobre el estado de la empresa mediante la documentación poder brindar fiabilidad y cumplimientos de la normativa evitando vulnerabilidad frente a terceros.

Por medio de las normas establecidas se especifica que lo realizará personal calificado haciendo uso de técnicas aptas para su revisión y verificación.

Según Arcentales, D., y Caycedo, X., (2016) menciona que:

En ocasiones se establece realizar un análisis obligatorio cuando la empresa tiene una relevancia vital, la información que pueda ser utilizada por personas externas a la empresa es indispensable, por lo tanto, su fiabilidad deberá ser comprobada.

La mayor parte de las empresas no tienen la obligación legal de ser auditadas. Sin embargo, si los informes de auditoría son favorables, muchos de ellos son auditados porque el tercero confía en la empresa.

2.2.23 Plan de auditoría

"Se detalla de manera general el procedimiento con cada una de sus actividades o acciones correspondientes con el tiempos adecuado y sostenible determinando que se realice de manera eficiente las gestiones pertinentes, obteniendo resultados apropiados para establecer controles o normativas." (Albarrán, S., Perez, J., y Valero, L., 2017)

2.2.24 Gestión de la información

Es el uso apropiado de la información y un objetivo responsable de los recursos involucrados en el flujo de información, con el fin de mantener una alta eficiencia en el funcionamiento de los procesos estratégicos y productivos que conforman el sistema. La gestión de la información está coordinada, directamente y controla sistemáticamente el flujo de información en cada sistema, dado los segmentos típicos de los sistemas, como el medio ambiente, los procesos generados generan, entre otras cosas, las personas involucradas en personas y tecnologías; La de la reacción alternativa. Así como el conocimiento actualizado y preciso del ciclo de vida generado por el sistema. (Castellanos, J. 2020)

2.2.25 Gestión de riesgos tecnológicos

Se sustenta con el conocimiento técnico adaptando el contexto normativo y legal para el funcionamiento de gestión de riesgos tecnológicos, por ende, queda a libre elección del encargado de la seguridad utilizar métodos para riesgos laborales que se enfoquen en la prevención y corrección en eventos específicos. Montenegro, M. (2018)

2.2.26 Análisis de riesgos

El análisis de riesgos dentro de la seguridad de la información contiene diversos receptores en una institución, obteniendo información sobre la seguridad que ayuda a delimitar acciones necesarias para un cumplimiento óptimo, estableciendo medidas con un alcance adecuado, proporcionando su finalidad de resguardo de información. (Manzaba, G. 2017)

Se lleva a cabo las evaluaciones sobre el cumplimiento de normas o políticas para realizar un plan de acción con los requerimientos que proporcione la institución mejorando de manera global todos los procedimientos o actividades de funcionarios, logrando mitigar riesgos internos o externos.

2.2.27 Matrices de riesgos

La matriz de riesgo se utiliza para evaluar la gestión de riesgos de negocios a través de la ponderación de los efectos y la probabilidad del evento por diferentes parámetros, permite determinar un plan de acción para los procesos que tienen los procesos, efectos del riesgo corporativo y la frecuencia máxima de gestión administrativa de la organización afecta. Esto

permite el diseño de estrategias de mitigación de riesgos corporativos para permitir la mitigación del riesgo comercial. (Sulca, G. y Becerra, E. 2017)

2.2.28 Probabilidades de impacto

La estandarización de los riesgos informáticos identificados requiere la distribución de valores probabilísticos para definir la aparición del evento, y sus efectos deben ser una amenaza de este tipo y, por lo tanto, la organización debe tener una idea clara de la probabilidad de que la probabilidad de que ocurra en todo tipo de escenarios de riesgo.

Si existe una probabilidad de (100%), no es un riesgo, sino también una certeza que se llevará a cabo esta posibilidad. Si se ha producido un evento en este sentido en el pasado, se tiene en cuenta que se tomaron medidas adecuadas de prevención para reducir el riesgo de eventos. Por lo tanto, no se considera una ocurrencia segura ni los valores definidos por incidentes exitosos. En una amenaza para cualquier probabilidad cero (0%) no se considera un riesgo y, por lo tanto, no se tiene en cuenta. Sin embargo, es muy difícil (si no imposible) tener la seguridad total de que algunas posibilidades ocurren de alguna manera, con mayor razón para la información. (Peña, R y Lugani, C. 2018)

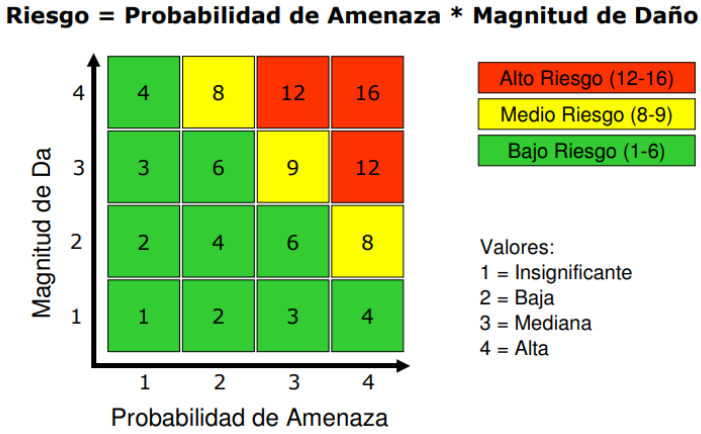


Figura 3 Matriz de probabilidad e impacto
Fuente: Análisis de riesgos. (2019) Recuperado de:
https://criminologainformatica1.blogspot.com/2019/03/analisis-de-riesgos.html?m=1

2.2.29 Plan de mitigación

La comprensión significativa de la mitigación del riesgo es reducir los riesgos con la intención de las listas emergentes para cada organización. Por lo tanto, es posible que el plan de emergencia deba decir que un plan toma los eventos o no puede ocurrir. A menudo observamos que algunos creen que estos dos planes de riesgo han excluido, y, sin embargo, este no es el caso. Benavides, C. (2017)

- Es necesario que se planifique la respuesta al riesgo de atenuación y reacción de emergencia. Las acciones se definen antes de que ocurra el riesgo o no se produzca.
- Los recursos se asignan de antemano debido a la situación de riesgo identificada.
- Los riesgos que por encima del umbral establecido se mitigan, aplicando los planes de respuesta para reducir la probabilidad y la influencia del trabajo como un plan proactivo.

III. METODOLOGÍA

3.1. ENFOQUE METODOLÓGICO

3.1.1. Enfoque

Mixto

El enfoque mixto logra ampliar la perspectiva de estudio dando un discernimiento más completo de lo que ocurre en el fenómeno estudiado, debido a que se lo realiza explorando y evaluando distintos niveles de fortalezas y debilidades, se logra obtener mayor magnitud como profundidad con claridad. Al incorporar enfoques optimiza su confiabilidad facilitando datos e interpretaciones de utilidad y brindando veracidad en la muestra y el uso de los instrumentos. Baena, G (2017)

En la presente investigación se toma prioridad a los elementos utilizados de los distintos enfoques que brindan facilidad para la obtención de requerimientos logrando un análisis de los resultados en cada proceso y etapa. Mediante este enfoque existe la reducción de incertidumbre consolidando argumentos que provienen de evaluaciones de datos, esta complementación se logra deducir que enfoque cualitativo representa un gran porcentaje en la investigación basando en la recolección de información en base a entrevistas semiestructuradas, observación y cuantitativo que en su minoría es un complemento de suma importancia, siendo este el que nos ayudará a verificar el objeto de estudio y a su vez a mitigar vulnerabilidades a través del análisis de escalas para solucionar problemas sobre la seguridad de la información.

Modalidad de investigación

Documental

La recopilación documental tiene la finalidad de obtener información susceptible a ser utilizadas en concreto, tomando en cuenta que puede llegar a ser una tarea ardua y laboriosa podemos obtener resultados conforme al problema establecido dependiendo también de las habilidades y la experiencia de quien realiza la investigación. (Metodología de la Investigación, 2018)

Esta investigación se la realiza a través de investigación bibliográfica la cual aporta con bases estratégicas para búsqueda y selección de documentos, en la recolección de información se obtiene un proceso sistemático bien definido según los objetivos propuestos, fundamentalmente la información es fuente o referencia en cualquier momento o lugar sin alterar el sentido del acontecimiento.

Investigación de campo

Según Cabezas, E., Andrade, D., y Torres, J. (2018) afirman que:

En la investigación de campo se somete al fenómeno de estudio en distintos parámetro o etapas, es decir, como se lleva a cabo los procesos y conque se realizó la investigación, con el objetivo de recoger datos exactos de cada proceso establecido y los impactos que genera en las variables. En la investigación de campo de esta investigación se usa distintos instrumentos de representaciones estadísticas combinadas con técnicas como la observación, entrevistas y encuestas permitiendo la recolección de información llevando a cabo que los datos recolectados son más confiables.

3.1.2. Tipo de Investigación

Investigación descriptiva

Con el estudio descriptivo el investigador busca interpretar situaciones o sucesos especificando las propiedades y características del fenómeno sometido a este análisis, es decir que su objetivo es medir o recoger información de manera conjunta o independiente pero no indicar como están relacionadas las variables.

"Se sustenta la toma de decisiones evidenciando de manera concreta la situación, delimitando el campo de estudio para investigar las perspectivas sin tener resultados subjetivos sino de manera precisa para lograr desarrollar la intención del investigador" Carhuancho, I., Nolazco, F., y Monteverde, L, (2019)

En esta investigación el método descriptivo permite mostrar precisión de los sucesos o situaciones, logrando medir los conceptos y variables, los grupos de quienes se recolectará datos, así como determinar las características o procesos de una población en específico.

Investigación explicativa

Según Sánchez, H., Reyes, C y Mejía, K (2018) mencionan que:

"Existe un propósito que además de establecer relación entre variables se enfoca en determinar las causas de los eventos de cualquier índole, conociendo el problema actual que señalan posibles antecedentes mínimos sobre un problema."

La investigación explicativa sobrepasa la descripción de conceptos o el estudio de variables, es decir, enlazados directamente dar soluciones a causas, sucesos o eventos relacionados con el estudio del fenómeno, es por eso que la utilizamos en este caso de estudio al establecer la causa de los sucesos por verificar.

3.2. IDEA A DEFENDER

Promover la implementación del sistema de gestión de la información y análisis de controles de seguridad en beneficio del GAD - Municipal del Tulcán.

3.3 DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES

Tabla 2.
Definición de variables

Variable	Definición conceptual de la variable	Dimensión	Indicadores	Técnica	Instrumento	Informante
Independiente: Seguridad de la Información	Sistema de gestión de la seguridad de la información salvaguardando la confidencialidad, integridad y disponibilidad.	Seguridad de los activos. Eficiencia en los resultados que se requiere. Infraestructura de la organización.	Vulnerabilidad en procesos. Amenazas de la Información.	-Observación -Entrevistas -Auditoría	*Preguntas establecidas, *matrices. *Checklist *Guión de entrevistas	Coordinador del centro de Tics del Municipio de Tulcán. Jefes de cada departamento.
Dependiente: Análisis de controles de seguridad	Consiente en proponer soluciones para mitigar riesgos y mejorar el rendimiento de los procesos de la información	Condiciones actuales. Recursos tecnológicos. Mejora continua. Buenas prácticas.	Mitigar riesgos Normativa o parámetros a cumplir.			

3.4. MÉTODOS UTILIZADOS

Método analítico

Ochoa, C (2019) menciona que:

La comparación de variables conlleva una elección de medidas de riesgo y validez con mayor precisión y se adecúa de acuerdo al tipo de estudio, considerando que es un método estadístico el tipo de escala es la medida de las variables analizadas.

Se utiliza el método analítico con el propósito de descomponer el todo en sus partes para observar con mayor determinación el objeto de estudio, mediante este podemos identificar de mejor manera los requerimientos necesarios para analizar los controles y procedimientos de la información, esta interpretación nos ayuda a reconocer aportes válidos y argumentaciones para dar solución a lo relacionado con la investigación.

Diseño no experimental

Según (Orozco, H. 2017) Afirma que:

Los estudios no experimentales Se realizan sin manipulación de variables, se designa control conductual de otros grupos sin recibir tratamiento ni persuasiones de prueba, las relaciones entre variables se manifiestan en su contexto natural y se indaga en incidencias en un momento determinado.

Se realiza una investigación no experimental debido a que no ejecutaremos acción – reacción para conseguir resultados claros dependiendo de experimentos, únicamente fundamentaremos con investigación documentada independientemente de lo solicitado, se utilizó para observar y analizar distintas perspectivas para llevar a cabo la muestra de estudio obteniendo razones y relaciones entre las variables.

3.4.3 Población y tipo de muestreo

El muestreo no probabilístico permite seleccionar la población de manera limitada y de acuerdo a la facilidad del personal, la accesibilidad y proximidad de la idea del investigador, utilizando escenarios donde la muestra es muy pequeña estando sujetos a tener individuos seleccionados con objetivos prácticos para determinar los requerimientos necesarios para la investigación. Otzen, T., Manterola, C. (2017)

La población en la que se adecuó en la investigación es muy pequeña y no se aplicó cálculo muestral, por ende, que se utilizó muestreo no probabilístico seleccionando así por conveniencia al grupo adecuado para proceder con la investigación que fue efectuada en el área de sistemas del “GAD municipal de Tulcán”.

3.4.4 Técnicas e instrumentos

Entrevista

Troncoso, C., Amaya, A., (2016) confirman que:

A través de la investigación la búsqueda de conocimiento se centra en la interpretación y complejidades de un fenómeno de estudio, obteniendo varias fuentes de información se puede fortalecer los resultados por medio de un análisis abierto para explicar y comprender de manera precisa sin necesidad de generalizar resultados. La entrevista es un intercambio de pensamientos o puntos de vista no solo un conversatorio, dependiendo también de la habilidad del entrevistador y sus capacidades comunicativas, para facilitar se puede contextualizar la información en la importancia de temas relevantes y las acciones que se interpretan.

La entrevista nos permite obtener información directamente de los sujetos de estudio con el fin de obtener respuestas verbales a las interrogantes que se ha planteado de manera eficaz logrando aclarar ciertas incertidumbres sobre el problema en una pregunta que radica de una guía previamente orientada al estudio de investigación por medio de formularios, siendo el método más utilizado.

Observación

Mediante la observación podemos interpretar minuciosamente y con detenimiento procesos, situaciones personas o contextos, se obtendrá conocimiento sobre características y comportamientos de las acciones necesarias para el objeto de estudio. Ávila, G. (2017)

Se planificó realizar la observación para dar validez y confiabilidad ya que se involucra directamente en la recolección de datos como objetivo, este método es útil al obtener información de manera detallada abordando el problema general y manteniendo la veracidad de la información requerida.

IV. RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

4.1.1 Datos informativos

Gobierno Autónomo Descentralizado Municipal de Tulcán

4.1.1.1 Logotipo

Figura 4 Logotipo GAD Municipal de Tulcán
Fuente: GADMT (2021) Recuperado de: http://www.gmtulcan.gob.ec/municipio/.

4.1.1.2 Ubicación

Municipio de Tulcán – Parque Principal

Olmedo – 10 de agosto

Figura 5 Ubicación GAD Municipal de Tulcán
Fuente: GADMT (2021) Recuperado de: http://www.gmtulcan.gob.ec/municipio/

4.1.1.3 Descripción

El GAD municipal de Tulcán es una institución encargada de gestionar procesos públicos utilizando herramientas que son indispensables para el desarrollo, permitiendo la accesibilidad de la información, compartiendo su disponibilidad y asegurando información de la ciudadanía.

4.1.1.4 Misión y visión

Misión

Somos una organización de gobierno y servicio público local que promueve el desarrollo y bienestar integral de la comunidad de manera eficiente, honesta y responsable, involucrando la participación ciudadana en pro del bienestar común. (GADMT, 2021)

Visión

Constituirse para el año 2023 en un Gobierno Autónomo Descentralizado con un modelo de gestión administrativa, técnica participativa y operativa que fundamente su accionar en el bienestar de la comunidad, a través de un proceso de mejoramiento continuo de calidad y eficacia de los servicios que potencie la productividad, constituyéndose en una población apta para invertir y vivir en armonía. (GADMT, 2021)

Objetivos estratégicos

- Efectivizar la ejecución presupuestaria con la finalidad de garantizar el cumplimiento de planes y programas establecidos por la administración municipal;
- Agilitar los procedimientos de pago para apoyar a la efectividad de la ejecución presupuestaria;
- Garantizar la recaudación oportuna de los tributos y obligaciones municipales que tienen los ciudadanos del cantón a través de una potenciada sistematización de cobranza y control de cartera;
- Garantizar la confiabilidad razonable de los registros financieros con el objeto de poder tomar decisiones oportunas es necesario que la información se obtenga en tiempo real;
- Impulsar el potencial turístico del Cantón Tulcán; para posicionarlo como una prioridad turística que mejore la economía del cantón;
- Desarrollar nuevas políticas a favor del desarrollo local, considerando la protección y garantía en materia de derechos humanos, priorizando los elementos insertos en las Agendas Nacionales de Igualdad;
- Mejorar la prestación de servicios públicos en las diferentes parroquias del cantón; de acuerdo a las necesidades de la ciudadanía para garantizar el Buen Vivir;

- Desarrollar programas de capacitación con enfoque social y dirigidos hacia la comunidad del cantón, con la finalidad de establecer directrices que permitan a los ciudadanos conocer la formativa Legal Vigente y la situación actual del cantón;
- Actualizar periódicamente el Plan Maestro de Gestión Ambiental Cantonal 2020 –2030, con el fin de garantizar su buen uso a favor de la ciudadanía;
- Incrementar el nivel de seguridad en el cantón en relación a los delitos de mayor connotación: robo a personas, robo a domicilio, robo de vehículos, venta de drogas;
- Gestionar la administración procesos por cada dependencia municipal;
- Mejorar los subsistemas de gestión y gestión del talento, posibilitar el desarrollo personal y profesional para mejorar los servicios urbanos.
- Mejorar la funcionalidad de la infraestructura municipal en base a los procesos de servicio al cliente;
- Efectivizar la comunicación institucional en base a buenas prácticas y medios adaptados a las necesidades;
- Lograr una cultura organizacional de clase mundial enfocada al servicio hacia el cliente interno y externo;
- Lograr un gobierno digital con servicios tecnológicos;
- Mejorar la gestión con mecanismos de control actuales para asegurar el desempeño de objetivos institucionales, a través de herramientas de apoyo tecnológico;
  (GADMT, 2021)

Estructura Organizacional Funcional

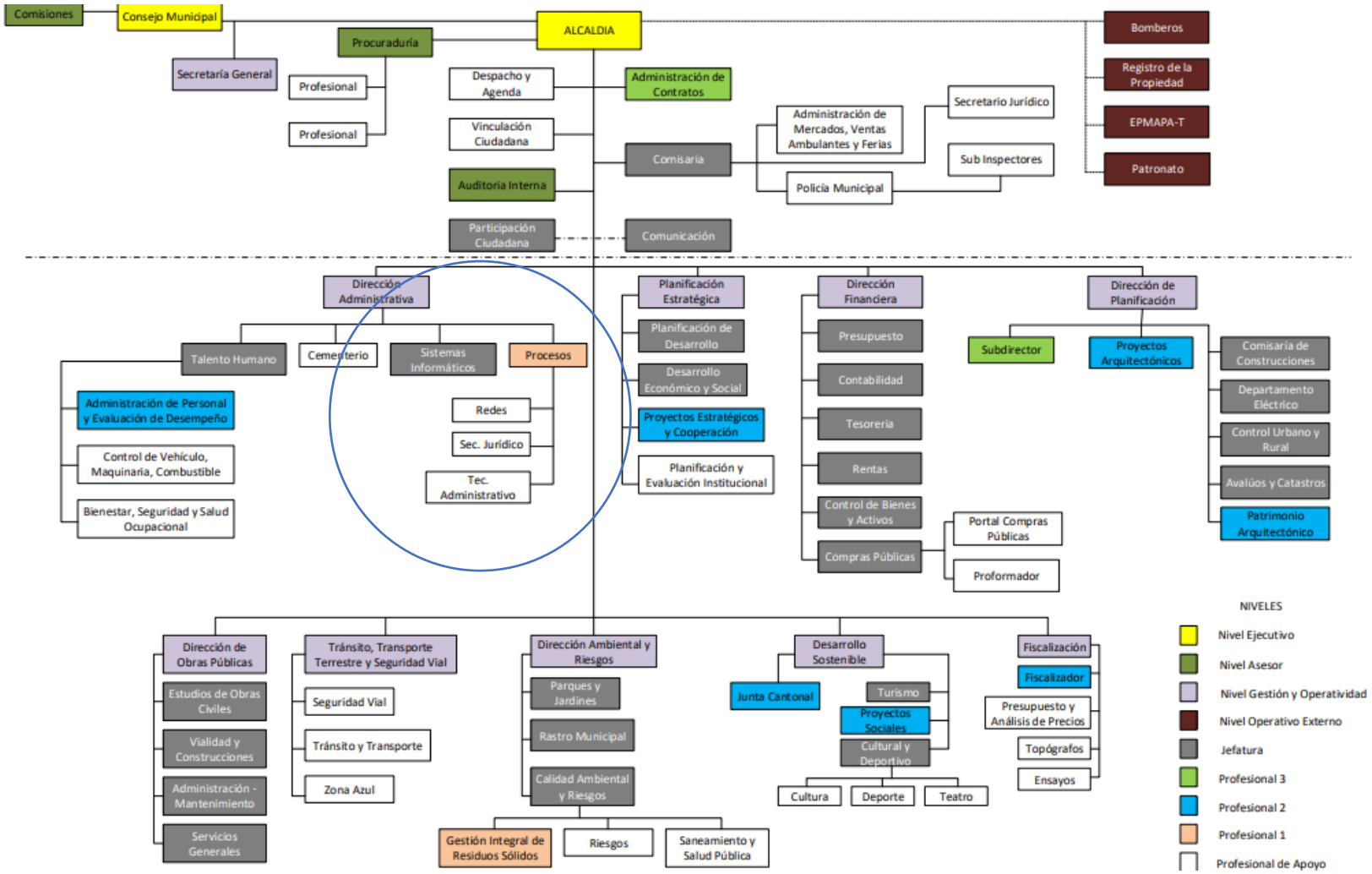


***Figura* 6** Estructura Organizacional Funcional
Fuente*:* Arévalo. L (2019) Recuperado de: www.dit.upm.es.

4.1.2 Auditoría informática

4.1.2.1 Objetivo de auditoría

Analizar los controles y procesos internos en el área de sistemas del GAD Municipal, con el fin de evaluar el cumplimiento de normativa e identificar riesgos y el impacto que puede provocar en la institución.

4.1.2.2 Alcance

El alcance de la investigación se enfoca inspeccionar los controles la norma internacional ISO/IEC 27002 un estándar de seguridad de la información, que permite controlar y evaluar procesos, para así proceder a ejecutar estrategias de mitigación para la mejora continua de procesos eficientes y seguros en un área específica.

4.1.2.3 Justificación

El análisis de controles se lo realiza en el área de sistemas que está sujeto a vulnerabilidades y amenazas poniendo en riesgo la pérdida de su disponibilidad, confidencialidad e integridad, detectando falencias que se pueden minimizar o riesgos que se puede evadir.

4.1.2.4 Equipo auditor

Auditor Joselin Igua

Asesor Msc. Jairo Hidalgo

4.1.3 Estudio inicial

4.1.3.1 Análisis de la situación actual del GAD Municipal de Tulcán.

El GAD Municipal de Tulcán, está dedicada a prestaciones de servicios brindando seguridad y eficiencia, procurando el bienestar de la colectividad en áreas urbanas y rurales, fomentando enfrentar problemas a su disposición, coordinando con otras entidades para mejorar el desarrollo del Cantón.

La estructura organizacional del Gobierno Autónomo Descentralizado Municipal de Tulcán se alinea a su misión y visión consagrada en la Constitución de la República y el Código Orgánico de Organización Territorial, Autonomía y Descentralización y se sustenta en la filosofía y enfoque de productos, servicios y procesos con el propósito de asegurar su ordenamiento orgánico interno. (GADMT, 2021)

El departamento de sistemas es el área a ser evaluada, formando parte del GAD Municipal cumple funciones diversas funciones que determinan una buena labor dentro de la institución, siendo dependiente de la Dirección de Gestión Administrativa garantiza procesos de gran impacto determinando seguridad de la información siendo activos prioritarios para la organización.

4.1.3.2 Estructura Organizacional

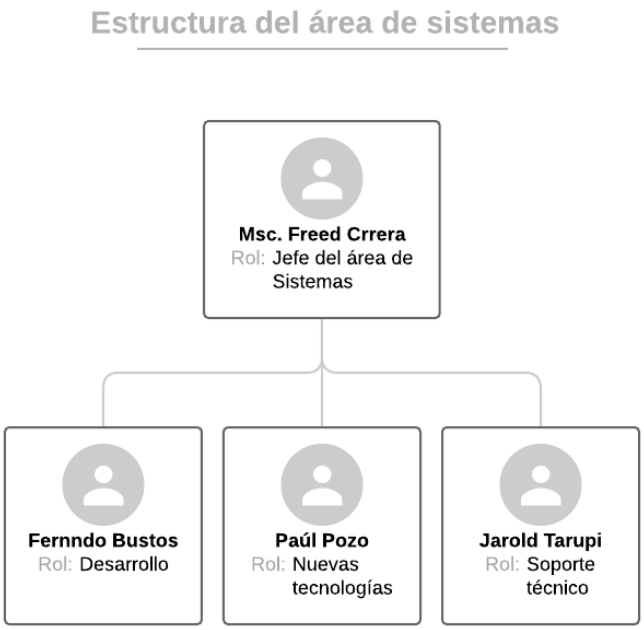


Figura 7 Estructura Organizacional Área de Sistemas

4.1.3.3 Técnicas para el levantamiento de información

Tabla 3.
Técnicas de levantamiento de información.

Técnica	Personal de trabajo	Objetivo
Entrevistas	Jefe del área de sistemas Desarrollador Administrador de base de datos	Conocer el cumplimiento de normativa y procedimientos basados en la normativa establecida
Observación	Área de Sistemas	Evidenciar el nivel de cumplimiento en las responsabilidades de los funcionarios.

4.1.3.4 Análisis de la entrevista

La presente entrevista se la realizó directamente con el Jefe del departamento de sistemas, encargado de todos los procesos necesarios para realizar el análisis y verificar su cumplimiento.

Jefe del área de sistemas

Msc. Freed Carrera

En referencia al estándar internacional ISO/IEC 27002 encargado de la seguridad de la información, siendo estos los activos más significativos dentro de las instituciones ya sea hardware, software e información confidencial.

Preguntas:

Pregunta 1. ¿Cuál es el estándar que se utiliza para la protección de activos informáticos?

Respuesta: No se establece controles o estándares de una normativa internacional, siendo una institución pública se adapta a las normativas de la Contraloría General del Estado basados en el Art. 410

Análisis: Si la institución no cuenta con normativa que se rige en la seguridad de la información es posible que se pueda generar un alto porcentaje de vulnerabilidad, ya que no existe revisión del cumplimiento de las actividades o respaldar las acciones mediante certificación, tomando en cuenta que el Art. 410 de la Contraloría General del Estado posee secciones de la seguridad de la información, no se da cumplimiento a la misma, por lo tanto, los parámetros establecidos por la normativa ISO/IEC 27002 se enfoca en la protección de la información y activos informáticos.

Pregunta 2. Independientemente de la normativa de la institución ¿Cuáles son los controles establecidos para la gestión de la seguridad de la información y quienes son los responsables de verificar el cumplimiento?

Respuesta: Se encargan de verificar el personal a disposición cuando sea necesario, se determina responsabilidades al personal dependiendo del proceso a realizar, los controles se determinan dependiendo de la actividad a realizar.

Análisis: realizar la verificación del cumplimiento de manera imparcial no puede generar un cumplimiento total y preciso de los controles establecidos, al no existir una persona encargada de la seguridad de la información de manera directa bajaría el cumplimiento de la normativa dentro de la organización interna que respalda la asignación de responsabilidades a un oficial de seguridad de la información según el control 6.1 Organización interna.

Pregunta 3. ¿Cómo es el procedimiento para resguardar la información mediante normativas de seguridad y dónde lo almacenan?

Respuesta: Se lo realiza brindando acceso a un usuario determinado, se verifica su registro y proceso para aseguramiento de eventos que pueden acontecer de tal manera que podemos indicando que es lo que se realizó dentro del servidor físico y virtual

Análisis: el procedimiento puede mantener un control de eficiencia con seguridad baja, pero puede funcionar si no es respaldo de información confidencial o modificaciones de las mismas, tomando en cuenta el control de responsabilidad de los activos dentro del objetivo de la gestión de activos primarios existe la operación de respaldos bajo ciertos parámetros bajo cargos aplicados a funcionarios del área de tecnología, lo óptimo es tomar referencia del dominio Seguridad en la operativa ya que establece los responsables de procedimientos de operación.

Pregunta 4. Describa las funciones que tiene el personal encargado de la seguridad de la información lógica y física dentro del departamento de tecnología de la información.

Respuesta: El departamento de sistemas está dividido por áreas: infraestructura, desarrollo y nuevas tecnologías, las funciones depende de las necesidades que se presenten.

Análisis: todos los funcionarios dentro del área de tecnología están encargados de distintas responsabilidades, se las realiza dependiendo de la situación o requerimiento que pueda acontecer, dentro de los aspectos organizativos de la seguridad de la información requiere del cumplimiento de diversas estrategias administración, evaluación, control, desarrollo gestiones de incidentes, entre otros.

Pregunta 5. ¿Cómo son controladas las normativas para la gestión de la información?

Respuesta: La seguridad proviene de las acciones de personal al brindar acceso o privilegios en procesos específicos, no hay normativa que mencione control de gestión, se lo resuelve realizando correctamente las funciones.

Análisis: no existe normativa establecida para la gestión de información lo cual puede delimitar funciones que sean necesarias para prevenir acciones dentro de los procesos, de acuerdo a la normativa analizada existen varios controles que respaldan las gestión de la información las actividades se documentan e independientemente ya que abarca distintos aspectos como: gestión de incidentes, prestación de servicios, seguridad de redes, vulnerabilidades técnicas, entre otros, es decir que la protección de la información cubre gran cantidad de procesos.

Pregunta 6 ¿Cuáles son las funciones del encargado de la seguridad de la información?

Respuesta: No existe un responsable directo para la seguridad de la información.

Análisis: los controles establecen varios parámetros que debe cumplir la persona encargada de estas funciones, de esta manera poder conseguir total o parcialmente el objetivo, al realizar ciertos aspectos de control por parte de los funcionarios no se podría mitigar riesgos, ya que tiene prioridad la protección de la información, establecer la asignación de responsabilidades a un oficial de seguridad de la información vulnera muchas actividades ya que en la segregación de tareas control 6.1.2 determina ciertos mecanismos ligados a los 114 controles de protección de la información .

Pregunta 7 ¿Se encuentra clasificada la información en privada, publica, confidencia y critica?

Respuesta: No, la información solo es almacenada con datos de autenticación, solo existe la categorización de información pública.

Análisis: el área de tecnología no realiza una categorización de información lo que conlleva a no dar prioridades a datos relevantes para la institución, es por eso que se puede generar riesgos frecuentes de fuga de información, el dominio de Gestión de activos especifica la importancia de establecer directrices de clasificación, manipulado y etiquetado de información, siendo los errores de funcionarios quienes pueden vulnerar este acontecimiento.

Pregunta 8. ¿Cómo se accede a los diferentes sistemas informáticos?

Respuesta: Realizando registro en la bitácora, y dando uso de usuarios y contraseñas

Análisis: este proceso se puede definir con una protección media de vulnerabilidad, ya que está cumpliendo cierta parte de los elementos de control que se establece en la normativa internacional dentro del control de accesos, y sus diversas políticas de gestión y revisión.

Pregunta 9. De acuerdo con la última auditoria ¿cuál fue el porcentaje de conformidad o inconformidad y cuáles son los aspectos más débiles dentro de la seguridad informática.?

Respuesta: No se ha realizado auditorías hasta la fecha.

Análisis: al no realizar una auditoría periódica no se puede saber con exactitud los riegos que los procedimientos actuales pueden causar a la empresa, tampoco se puede mitigar riesgos o prevenirlos como está establecido en el dominio de seguridad en la operativa, control 12.7.1 consideraciones de las auditorías periódicas.

Pregunta 10. ¿Qué medidas se toman en caso de fallas en la disponibilidad de la información?

Respuesta: Realizar un informe para determinar las fallas que produjeron este inconveniente para mejorarlo y no frecuentarlo.

Análisis: se puede solventar con este procedimiento de manera parcial, para evitar este tipo de inconvenientes es necesario realizar un plan de contingencia o estructurar estrategias que lo puedan establecer dentro de la seguridad de telecomunicaciones con políticas y controles y mecanismos asociados a la gestión de red.

Pregunta 11. ¿Cómo es el proceso para acceder la data center?

Respuesta: Solo el personal autorizado puede tener acceso directo con los dispositivos y sistemas que se encuentran dentro del área de datos restringida.

Análisis: este es un parámetro cumple con ciertos procesos hacia los activos prioritarios, pero siendo deficiente para el departamento de tecnologías por lo tanto se debe implementar normas de acceso físico como de gestión de usuarios, para verificar que solo el personal autorizado con sus respectivas credenciales pueda acceder a realizar cambio o modificaciones específicas por algún motivo que sea completamente necesario y autorizado.

Pregunta 12. ¿Cuál es el procedimiento para que los proveedores accedan a los sistemas informáticos?

Respuesta: Nos acoplamos a sus normativas de registro y damos acceso a lo que sea necesario dar disposición y realizando backups.

Análisis: el área de sistemas también debe establecer normativas para el acceso de servidores, de esta manera se puede prevenir distintos riesgos que pueden ser causados por terceros, por lo tanto, de debe realiza un acuerdo con las necesidades de la institución, la supervisión de manera periódica, y las notificaciones que deben generar si existe algún cambio dentro de los servicios prestados.

Pregunta 13. ¿Cómo se realiza la gestión de usuarios?

Respuesta: La gestión de usuarios está determinada por altas y bajas, también dando privilegios y restricciones.

Análisis: la gestión de usuarios cuenta con varias secciones y una de ellas que es indispensable y segura es dar privilegios y establecer restricciones, es un mecanismo seguro

para no ser una fuente de vulnerabilidad, en el área se cumple con la gestión de usuarios, aunque se puede encontrar ciertas falencias al no establecer la política asociada para estos procedimientos.

Pregunta 14. ¿Con qué frecuencia se realizan copias de seguridad, y se realiza una verificación posterior?

Respuesta: Las copias de seguridad se las realiza todos los días, las verificaciones depende el requerimiento.

Análisis: en caso de fallas en los sistemas la información debe estar respaldad diariamente así se evitaría inconvenientes graves, aunque se debe tomar en cuenta que los datos a respaldar deben estar cifrados.

Pregunta 15. ¿Se realizan reportes de cumplimiento de funciones?

Respuesta: Se las realiza, aunque no de manera periódica sino en base a las actividades que hayan realizado.

Análisis: el cumplimiento de actividades se lo debe realizar de forma periódica para mantener controlada la existencia de riesgos, y el registro de actividades se lo debe revisar posteriormente, de acuerdo con el dominio de gestión de incidentes de la información podemos definir notificaciones de todas las acciones realizada de manera documentada y socializada con el encargado de dicha responsabilidad tomando en cuenta que servida para procesos posteriores conociendo el inicio de la vulnerabilidad y evitando su aparición.

Pregunta 16. ¿Existen planes estratégicos en áreas específicas?

Respuesta: No, podemos determinar alguna falla y justificarla después de hacer un análisis de alguna vulnerabilidad.

Análisis: deben existir planes ya valorados para todas las secciones del área de sistemas por posibles amenazas, ayudan a reestablecer funciones de manera eficiente en algún posible incidente, por ende, se analiza el dominio de la gestión de continuidad de negocio que determina la planificación, verificación y evaluación de la información de caso de acontecimientos, realizando la valoración de impacto y probabilidad para dar prioridad a ciertas actividades.

Pregunta 17. ¿Los manuales de usuario son verificados por funcionarios públicos de altos cargos?

Respuesta: No necesariamente, estoy a cargo de esa responsabilidad y ese cumplimiento

Análisis: si existe una disposición de no ser necesaria la aprobación de otros funcionarios se pueden respaldar del Jefe de área, aunque se debe informar a superiores los procesos a realizar.

Pregunta 18. ¿El personal del área de sistemas cuenta con activos a su cargo o responsabilidad?

Respuesta: Si, existe un listado de los activos con codificación y los responsables correspondientes a cada equipo o activo no tangible.

Análisis: la responsabilidad de los activos se divide en todos los funcionarios del área de tecnología, brindando apoyo y soporte en caso de fallas, así se puede mantener certeza del cuidado de los equipos.

Pregunta 19. ¿Existe documentación que respalde la evidencia de las actividades y responsabilidades?

Respuesta: No documentación formal, pero si el registro y los avances de las actividades que realizan dentro del área.

Análisis: se debe documentar de manera formal las actividades realizadas o por realizarse para tener conocimiento al realizar análisis de riesgos o algún inconveniente y sea solicitada desde la institución, también para evidenciar las actividades manteniendo el control de las acciones y la supervisión necesaria.

Pregunta 20. ¿La información de alto riesgo cuenta con sistemas de cifrado?

Respuesta: No tenemos ese tipo de protección para la información.

Análisis: la información que la institución puede considerar como confidencial se necesita sistemas de codificación o encriptación para resguardar o realizar envío de datos a otras entidades, se debe realizar un estudio para la aplicación de política de cifrado, pero la gestión de claves de acceso debe estar asociada a los parámetros necesarios que menciona en el control 10.1.2 de la normativa.

Pregunta 21. ¿Se hace uso de firmas electrónicas como protección y verificación de información?

Respuesta: Si, en muchas ocasiones la única verificación existente es la firma electrónica.

Análisis: el uso de firmas digitales puede proteger la información necesaria bajo la autoría de manera más precisa

Pregunta22. ¿Cuentan con prestación de equipos para áreas distintas de la institución?

Respuesta: El departamento de sistemas no está encargado de ese procedimiento, quien lo realiza es el área de bienes o servicios.

Pregunta 23. ¿Cuentan con sistemas de detección de intrusos?

Respuesta: No, no son configuraciones que hemos realizado, solo las básicas de telecomunicaciones

Análisis: la detección de intrusos evitaría significantes amenazas en contra de la institución ya que se puede ver afectado mediante la intrusión generando diversos daños de alto impacto, el monitoreo de red y la aplicación de estrategias establecidas en el control de telecomunicaciones es indispensable para evitar actos fraudulentos de manera interna o externa.

Pregunta 24. ¿Cada qué tiempo se realiza monitoreo de red?

Respuesta: La red no es monitoreada a menos que sea requerida por algún inconveniente que sea especifico.

Análisis: al no ser monitoreada la red puede causar riesgos silenciosos que no se pueden identificar con facilidad, es por eso que se lo debe realizar de manera periódica, dentro del control 12.6.6 generación de vulnerabilidades técnicas determina como cubrir las vulnerabilidades para prevenir incidentes relacionados con el dominio de telecomunicaciones.

Pregunta 25. ¿Existen bloqueo de puertos para los funcionarios de todas las áreas?

Respuesta: Los bloqueos se los realiza dependiendo las necesidades de las áreas

Análisis: independientemente de las áreas se debe preestablecer los puertos seguros y necesarios para las funciones del personal, tomando en cuenta los que pueden ser vulnerados por desconocimiento de los mismos, de igual manera a la aplicación de acceso remoto y

teletrabajo se debe implementar controles para la seguridad de la información ya que es un mecanismo empleado recientemente.

4.1.4 Propuesta

La propuesta consiste en realizar el análisis del sistema de gestión de la seguridad de la información en el área de sistemas del municipio de Tulcán, basado en la evaluación del cumplimiento de los controles de la normativa ISO/IEC 27002, mediante métodos e instrumentos de investigación, realizando procesos de auditoría informática y análisis de riesgos que nos permite determinar las los riesgos actuales y los que podrían presentarse, con la finalidad de establecer estrategias de mitigación y buenas prácticas para minimizar o prevenir amenazas a corto, mediano y largo plazo.

4.1.5 Plan de auditoría

4.1.5.1 Selección de procesos de TI

Los procesos en el área de tecnología fueron seleccionados en base a las técnicas aplicadas, observación y entrevista, y las funciones que desempeñan en el área de trabajo.

- Desarrollo de sistemas informáticos
- Administración de base de datos
- Administración Web
- Administración de redes
- Soporte técnico

Fichas de procesos TI

Tabla 4.
Desarrollo de sistemas informáticos

	PROCESO TI

Proceso:	Desarrollo de sistemas informáticos
Descripción:	Realizar sistemas informáticos en base a los requerimientos de la institución o petición directa de áreas externas.
Responsable:	Jefe de Sistemas Desarrollador de sistemas
Hallazgos:	• Almacenar código fuente sin cifrado
Frecuencia:	Probable

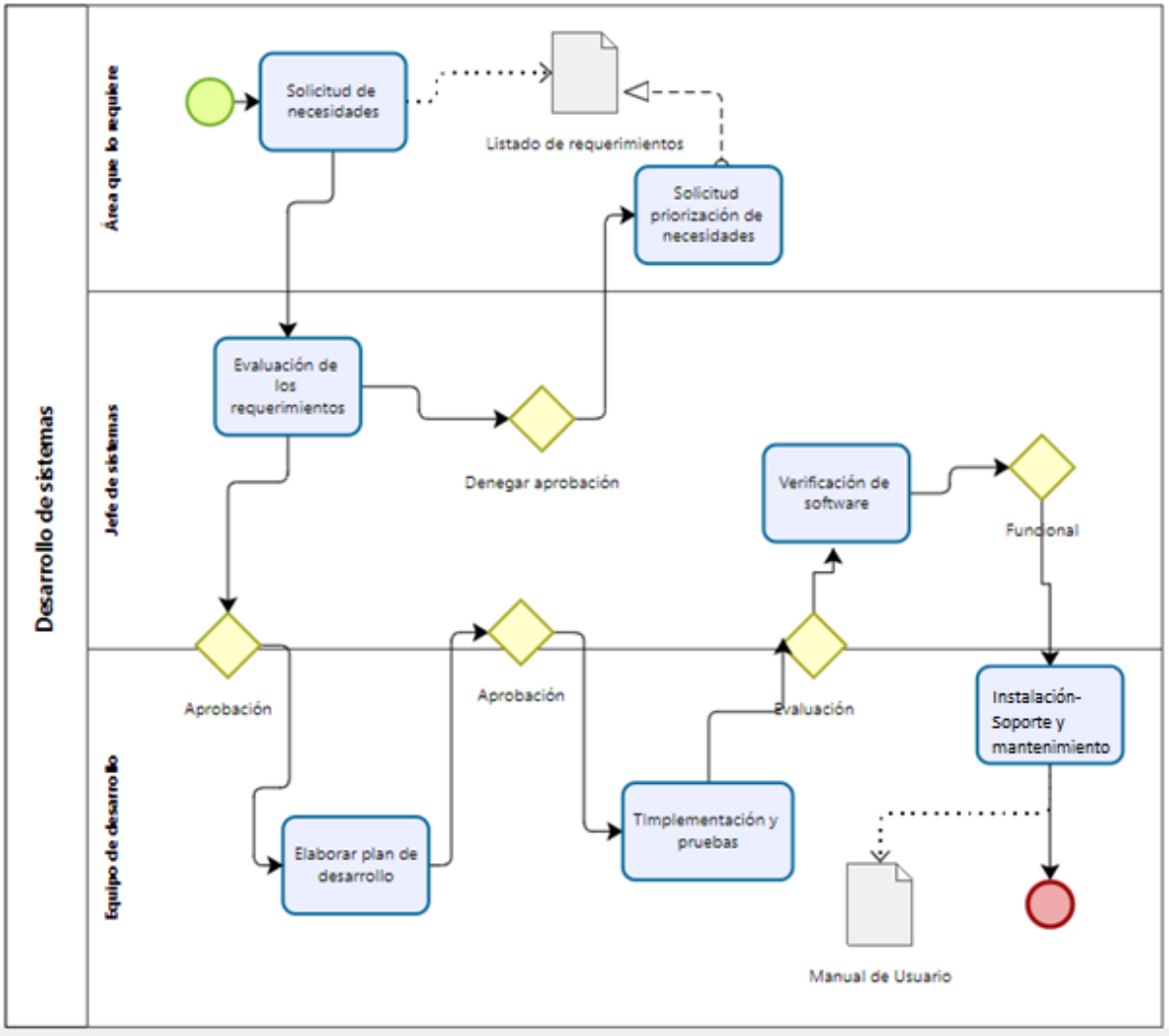


Figura 8 Proceso de desarrollo de sistemas
Fuente: Elaboración propia

Tabla 5.
Administración de base de datos

	PROCESO TI

Proceso:	Administración de base de datos
Descripción:	El administrador de base de datos con acceso directo a la información
Responsable:	Jefe de Sistemas Administrador de bases de datos
Hallazgos:	• Actualizaciones no periódicas • Almacenar código fuente sin cifrado
Frecuencia:	Probable

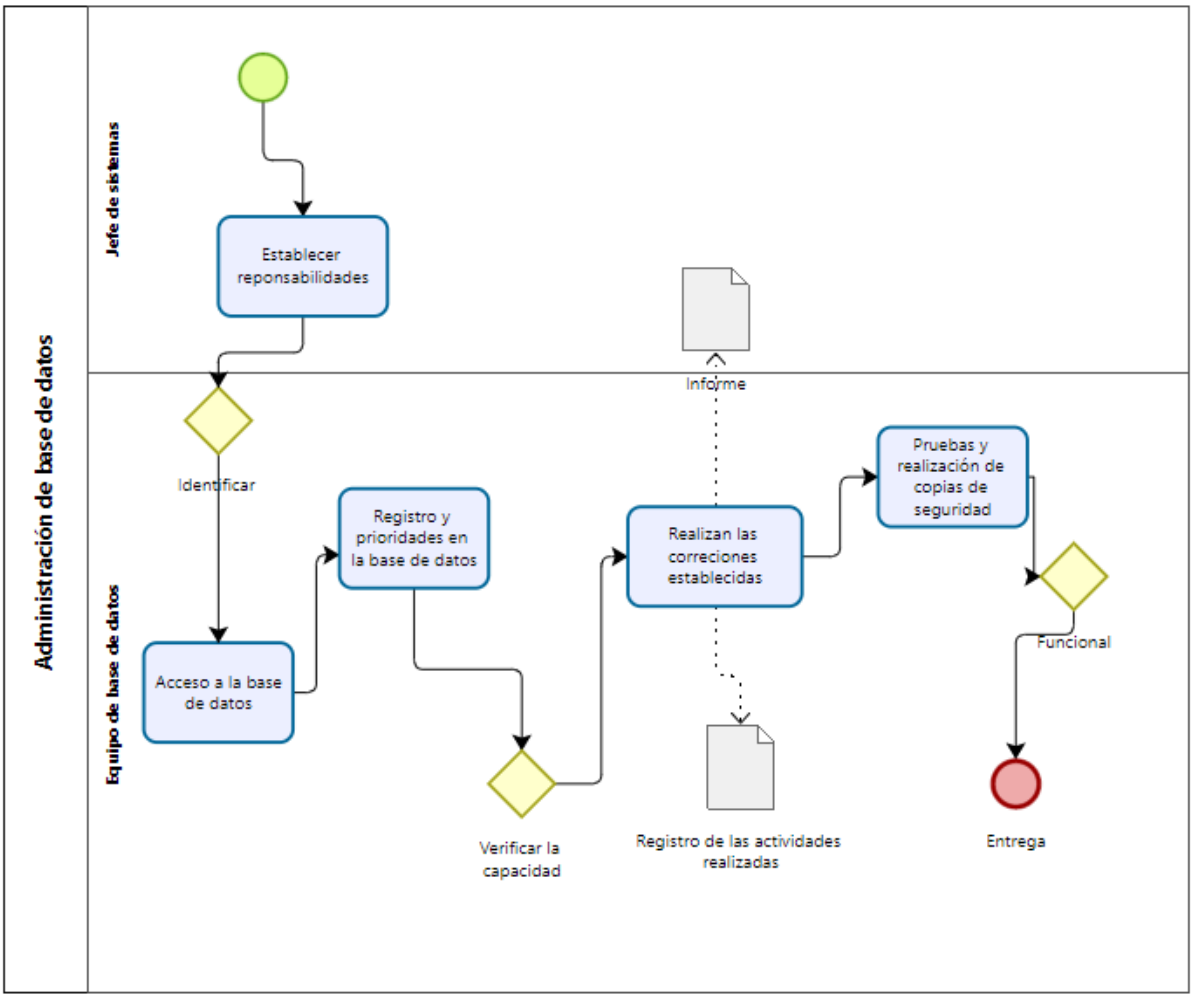


Figura 9 Proceso de administración de base de datos
Fuente: Elaboración propia

Tabla 6.
Administración Web

	PROCESO TI

Proceso:	Publicación de información
Descripción:	Peticiones de altos funcionarios para cambios o publicación de información relevante
Responsable:	Jefe de Sistemas Administrador web
Hallazgos:	• Sitios web no rigurosos
Frecuencia:	Media

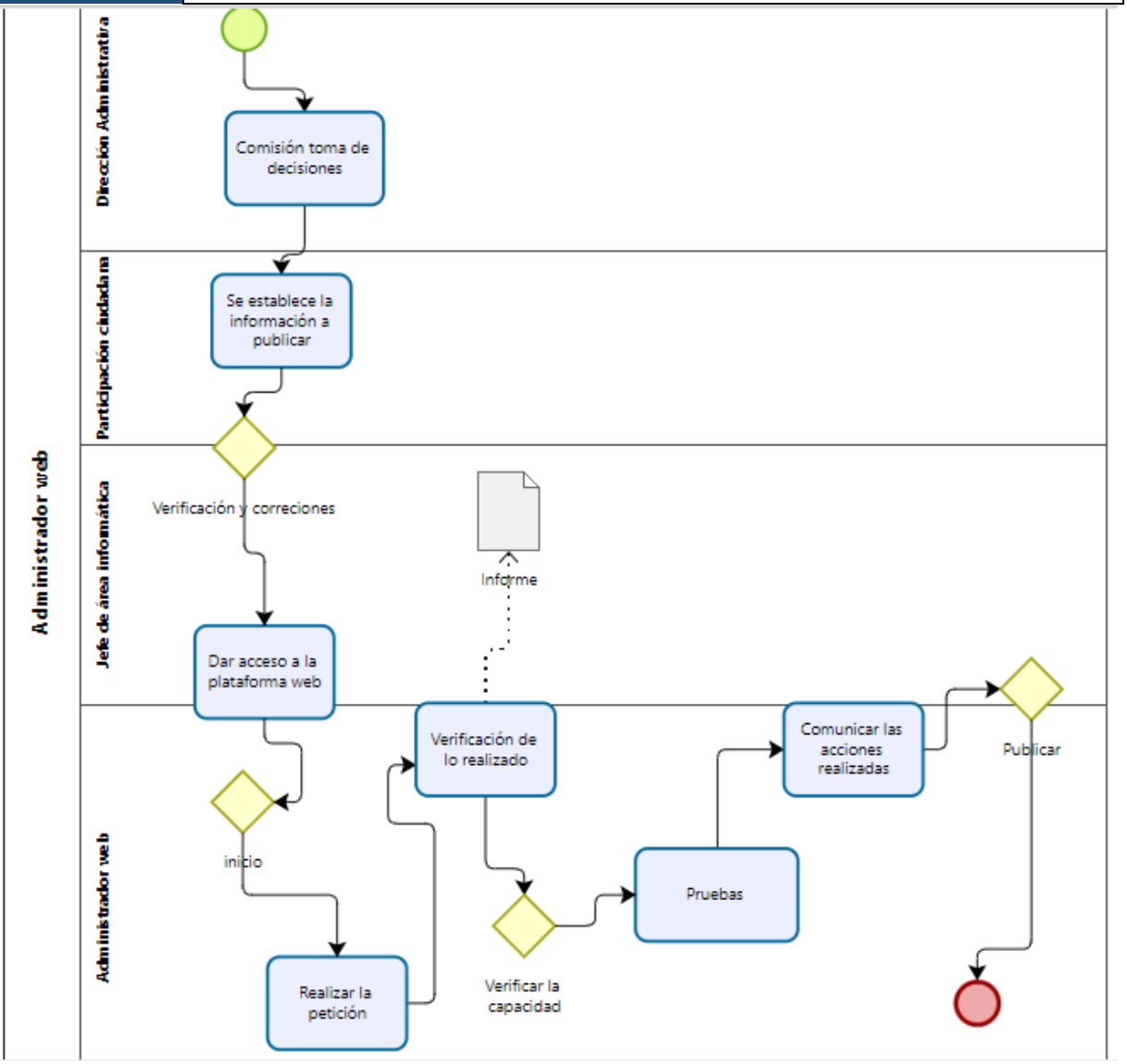


Figura 10 Proceso de administración web
Fuente: Elaboración propia

Tabla 7.
Administración de redes

	PROCESO TI

Proceso:	Administración de redes
Descripción:	Verificación del funcionamiento de red.
Responsable:	Jefe de Sistemas Administración de redes
Hallazgos:	• No existe monitoreo de red
Frecuencia:	Media

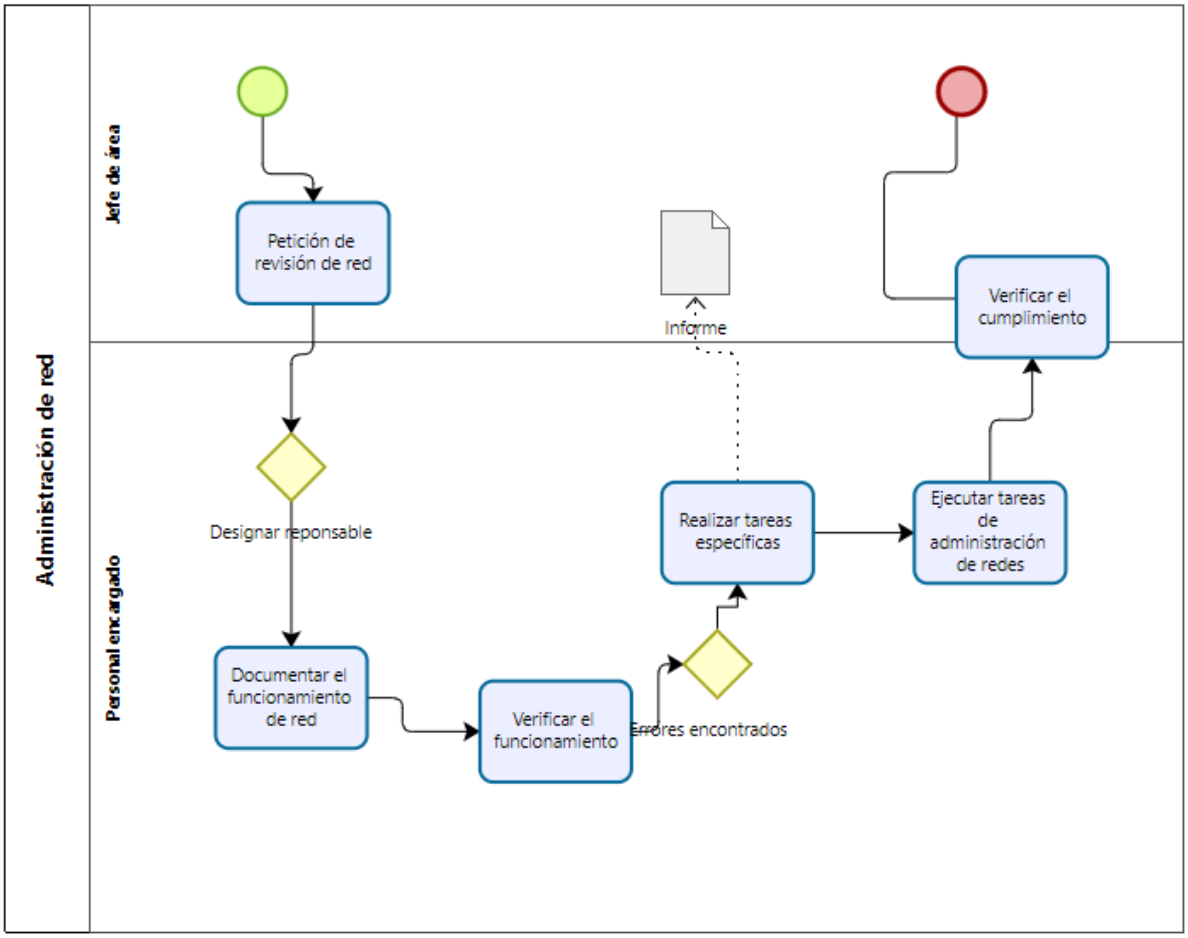


Figura 11 Proceso de administración de red
Fuente: Elaboración propia

Tabla 8.
Soporte técnico

	PROCESO TI

Proceso:	Licenciamiento de software
Descripción:	Realizar licenciamiento de software determinado por el mal funcionamiento de procesos
Responsable:	Jefe de Sistemas Mantenimiento y soporte técnico
Hallazgos:	• Actualizaciones no periódicas • Versiones de licencias sin verificación
Frecuencia:	Media

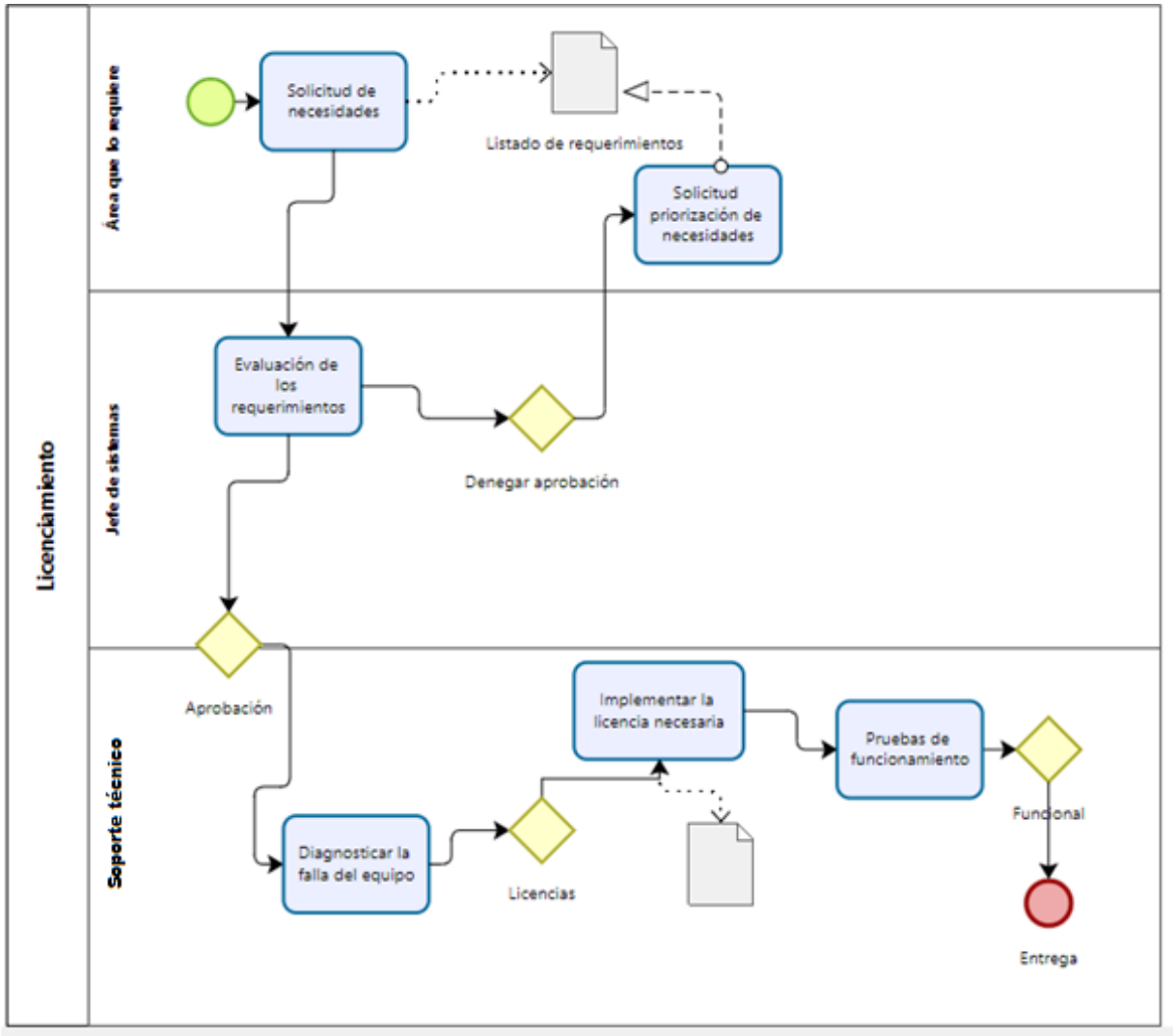


Figura 12 Proceso de licenciamiento de software
Fuente: Elaboración propia

4.1.5.2 Cumplimiento ISO/IEC 27002

Tabla 9.
14 Dominios, 35 Objetivos de control 114 controles

Dominios	Objetivos de Control	Controles	Descripción	SI	NO	No aplica
5	*1*	*2*	POLÍTICAS DE SEGURIDAD			
	5.1	**2**	**Directrices de la Dirección en seguridad de la información.**			
			Conjunto de políticas para la seguridad de la información		✓	
		5.1.2	Revisión de las políticas para la seguridad de la información.		✓	
6	*2*	*7*	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
	6.1	*5*	**Organización Interna**			
		6.1.1	Asignación de responsabilidades para la segur. de la información		✓	
		6.1.2	Segregación de tareas.	✓		
		6.1.3	Contacto con las autoridades.		✓	
		6.1.4	Contacto con grupos de interés especial.		✓	
		6.1.5	Seguridad de la información en la gestión de proyectos.		✓	
	6.2	*2*	**Dispositivos para movilidad y teletrabajo.**			
		6.2.1	Política de uso de dispositivos para movilidad.			✓
		6.2.2	Teletrabajo.		✓	
7	*3*	*5*	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.			
	7.1	*2*	**Antes de la contratación.**			
		7.1.1	Investigación de antecedentes.	✓		
		7.1.2	Términos y condiciones de contratación	✓		
	7.2	*2*	**Durante la contratación**			
		7.2.1	Responsabilidad de gestión		✓	
		7.2.2	Concienciación, educación y capacitación en segur. de la informac.		✓	
		7.2.3	Proceso disciplinario.		✓	
	7.3	***1***	**Cese o cambio de puesto de trabajo.**			
		7.3.1	Cese o cambio de puesto de trabajo.	✓		
8	*3*	10	GESTIÓN DE ACTIVOS			
	8.1	***4***	**Responsabilidad sobre los activos.**			
		8.1.1	Inventario de activos.	✓		
		8.1.2	Propiedad de los activos.	✓		
		8.1.3	Uso aceptable de los activos	✓		
		8.1.4	Devolución de activos	✓		
	8.2	**3**	**Clasificación de la información.**			
		8.2.1	Directrices de clasificación.		✓	
		8.2.2	Etiquetado y manipulado de la información.		✓	
		8.2.3	Manipulación de activos		✓	
	8.3	**3**	**Manejo de los soportes de almacenamiento**			
		8.3.1	Gestión de soportes extraíbles.	✓		
		8.3.2	Eliminación de soportes	✓		
		8.3.3	Soportes físicos en tránsito.			✓

9	*4*	14	CONTROL DE ACCESOS.			
	9.1	***2***	**Requisitos de negocio para el control de accesos.**			
		9.1.1	Política de control de accesos.		✓	
		9.1.2	Control de acceso a las redes y servicios asociados.		✓	
	9.2	***6***	**Gestión de acceso de usuario.**			
		9.2.1	Gestión de altas/bajas en el registro de usuarios.	✓		
		9.2.2	Gestión de los derechos de acceso asignados a usuarios.	✓		
		9.2.3	Gestión de los derechos de acceso con privilegios especiales.	✓		
		9.2.4	Gestión de información confidencial de autenticación de usuarios	✓		
		9.2.5	Revisión de los derechos de acceso de los usuarios.		✓	
		9.2.6	Retirada o adaptación de los derechos de acceso	✓		
	9.3	***1***	**Responsabilidades del usuario**			
		9.3.1	Uso de información confidencial para la autenticación.		✓	
	9.4	***5***	**Control de acceso a sistemas y aplicaciones.**			
		9.4.1	Restricción del acceso a la información.		✓	
		9.4.2	Procedimientos seguros de inicio de sesión	✓		
		9.4.3	Gestión de contraseñas de usuario.	✓		
		9.4.4	Uso de herramientas de administración de sistemas.		✓	
		9.4.5	Control de acceso al código fuente de los programas.		✓	
10	*1*	*2*	CIFRADO.			
	10.1	***2***	**Controles criptográficos**			
		10.1.1	Política de uso de los controles criptográficos.		✓	
		10.1.2	Gestión de claves.		✓	
11	*2*	15	SEGURIDAD FÍSICA Y AMBIENTAL.			
	11.1	***6***	**Áreas seguras.**			
		11.1.1	Perímetro de seguridad física.		✓	
		11.1.2	Controles físicos de entrada.		✓	
		11.1.3	Seguridad de oficinas, despachos y recursos		✓	
		11.1.4	Protección contra las amenazas externas y ambientales.		✓	
		11.1.5	El trabajo en áreas seguras.		✓	
		11.1.6	Áreas de acceso público, carga y descarga.			✓
	11.2	***9***	**Seguridad de los equipos.**			
		11.2.1	Emplazamiento y protección de equipos.		✓	
		11.2.2	Instalaciones de suministro.		✓	
		11.2.3	Seguridad del cableado.		✓	
		11.2.4	Mantenimiento de los equipos.		✓	
		11.2.5	Salida de activos fuera de las dependencias de la empresa.			✓
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones			✓
		11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	✓		
		11.2.8	Equipo informático de usuario desatendido	✓		
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	✓		

12	*7*	14	SEGURIDAD EN LA OPERATIVA.		
	12.1	***4***	**Responsabilidades y procedimientos de operación.**		
		12.1.1	Documentación de procedimientos de operación.		✓
		12.1.2	Gestión de cambios.		✓
		12.1.3	Gestión de capacidades.		✓
		12.1.4	Separación de entornos de desarrollo, prueba y producción.	✓	
	12.2	*1*	**Protección contra código malicioso.**		
		12.2.1	Controles contra el código malicioso.		✓
	12.3	*1*	**Copias de seguridad.**		
		12.3.1	Copias de seguridad de la información.		✓
	12.4	*4*	**Registro de actividad y supervisión.**		
		12.4.1	Registro y gestión de eventos de actividad.	✓	
		12.4.2	Protección de los registros de información**.**		✓
		12.4.3	Registros de actividad del administrador y operador del sistema.	✓	
		12.4.4	Sincronización de relojes.	✓	
	12.5	*1*	**Control del software en explotación.**		
		12.5.1	Instalación del software en sistemas en producción.	✓	
	12.6	*2*	**Gestión de la vulnerabilidad técnica.**		
		12.6.1	Gestión de las vulnerabilidades técnicas.		✓
		12.6.2	Restricciones en la instalación de software.	✓	
	12.7	*1*	**Consideraciones de las auditorías de los sistemas de información.**		
		12.7.1	Controles de auditoría de los sistemas de información.		✓
13	2	*7*	SEGURIDAD EN LAS TELECOMUNICACIONES.		
	13.1	*3*	**Gestión de la seguridad en las redes**		
		13.1.1	Controles de red.		✓
		13.1.2	Mecanismos de seguridad asociados a servicios en red.		✓
		13.1.3	Segregación de redes.		✓
	13.2	*4*	**Intercambio de información con partes externas.**		
		13.2.1	Políticas y procedimientos de intercambio de información.		✓
		13.2.2	Acuerdos de intercambio.	✓	
		13.2.3	Mensajería electrónica.	✓	
		13.2.4	Acuerdos de confidencialidad y secreto.		✓
14	*3*	*13*	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		
	14.1	***3***	**Requisitos de seguridad de los sistemas de información.**		
		14.1.1	Análisis y especificación de los requisitos de seguridad.		✓
		14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.		✓
		14.1.3	Protección de las transacciones por redes telemáticas.		✓
	14.2	*9*	**Seguridad en los procesos de desarrollo y soporte.**		
		14.2.1	Política de desarrollo seguro de software.	✓	
		14.2.2	Procedimientos de control de cambios en los sistemas.	✓	
		14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	✓	
		14.2.4	Restricciones a los cambios en los paquetes de software.		✓
		14.2.5	Uso de principios de ingeniería en protección de sistemas.	✓	
		14.2.6	Seguridad en entornos de desarrollo.	✓	
		14.2.7	Externalización del desarrollo de software.	✓	
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	✓	
		14.2.9	Pruebas de aceptación.	✓	
	14.3	***1***	**Datos de prueba.**		
		14.3.1	Protección de los datos utilizados en pruebas.	✓	

15	*2*	*5*	RELACIONES CON SUMINISTRADORES.			
	15.1	***3***	**Seguridad de la información en las relaciones con suministradores.**			
		15.1.1	Política de seguridad de la información para suministradores		✓	
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.		✓	
		15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.		✓	
	15.2	*2*	**Gestión de la prestación del servicio por suministradores.**			
		15.2.1	Supervisión y revisión de los servicios prestados por terceros.		✓	
		15.2.2	Gestión de cambios en los servicios prestados por terceros.		✓	
16	1	*7*	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
	16.1	*7*	**Gestión de incidentes de seguridad de la información y mejoras**			
		16.1.1	Responsabilidades y procedimientos.		✓	
		16.1.2	Notificación de los eventos de seguridad de la información.		✓	
		16.1.3	Notificación de puntos débiles de la seguridad.		✓	
		16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.		✓	
		16.1.5	Respuesta a los incidentes de seguridad.		✓	
		16.1.6	Aprendizaje de los incidentes de seguridad de la información.	✓		
		16.1.7	Recopilación de evidencias.	✓		
17	*2*	*4*	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.			
	17.1	*3*	**Continuidad de la seguridad de la información.**			
		17.1.1	Planificación de la continuidad de la seguridad de la información.		✓	
		17.1.2	Implantación de la continuidad de la seguridad de la información.		✓	
		17.1.3	información.		✓	
	17.2	*1*	**Redundancias.**			
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	✓		
18	*2*	*8*	CUMPLIMIENTO.			
	18.1	*5*	**Cumplimiento de los requisitos legales y contractuales.**			
		18.1.1	Identificación de la legislación aplicable.		✓	
		18.1.2	Derechos de propiedad intelectual (DPI).		✓	
		18.1.3	Protección de los registros de la organización.		✓	
		18.1.4	Protección de datos y privacidad de la información personal	✓		
		18.1.5	Regulación de los controles criptográficos.		✓	
	18.2	*3*	**Revisiones de la seguridad de la información.**			
		18.2.1	Revisión independiente de la seguridad de la información.		✓	
		18.2.2	Cumplimiento de las políticas y normas de seguridad.		✓	
		18.2.3	Comprobación del cumplimiento.		✓	

Figura 13 Cumplimiento de controles

Controles que no aplican

El área de sistemas no se ajusta a varios parámetros, es por eso que los procesos no fueron analizados.

6.2 Dispositivos para movilidad y teletrabajo

- 6.2.1 Política de uso de dispositivos para movilidad.

  No se considera el uso de dispositivos móviles para el entorno de trabajo.

11.1 Áreas seguras.

- 11.1.6 Áreas de acceso público, carga y descarga.

  El material entrante o saliente no depende directamente del área de sistemas, por lo tanto, el departamento de bienes y servicios es el encargado de este tipo de actividades.

11.2 Seguridad de equipos

- 11.2.5 Salida de activos fuera de las dependencias de la empresa.

  Él área de sistemas no está en la capacidad de realizar ese proceso, ya que depende de otras áreas el manejo de estos recursos.

- 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones

  Los funcionarios del área de sistemas no pueden estar a cargo de estos procedimientos que les pertenece a otras administraciones

4.1.6 Informe de Resultados

El porcentaje determinado por los 14 dominios es el resultado equivalente a la verificación del cumplimiento total de 114 controles en el área de sistemas.

Tabla 10.
Porcentaje de cumplimiento

Dominio	Descripción	Porcentaje de cumplimiento
5	Políticas de seguridad	0%
6	Aspectos organizativos de la seguridad de la información	16.66%
7	Seguridad ligada a los recursos humanos.	50%
8	Gestión de activos	66.66 %
9	Control de accesos.	50%
10	Cifrado.	0%
11	Seguridad física y ambiental.	25%
12	Seguridad en la operativa.	42.85%
13	Seguridad en las telecomunicaciones.	28.57%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	69.23%
15	Relaciones con suministradores.	0%
16	Gestión de incidentes en la seguridad de la información.	28.57%
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	25%
18	Cumplimiento.	14.28%

El nivel de cumplimiento de los dominios en su estado actual no se establece en un rango ideal para priorizar la seguridad de la información, por lo tanto, existen diversas fuentes de debilidades a solucionar dentro de las actividades en el área de sistemas que son indispensables para lograr mejoras significativas y contribuir con el rendimiento necesario dentro de la institución.

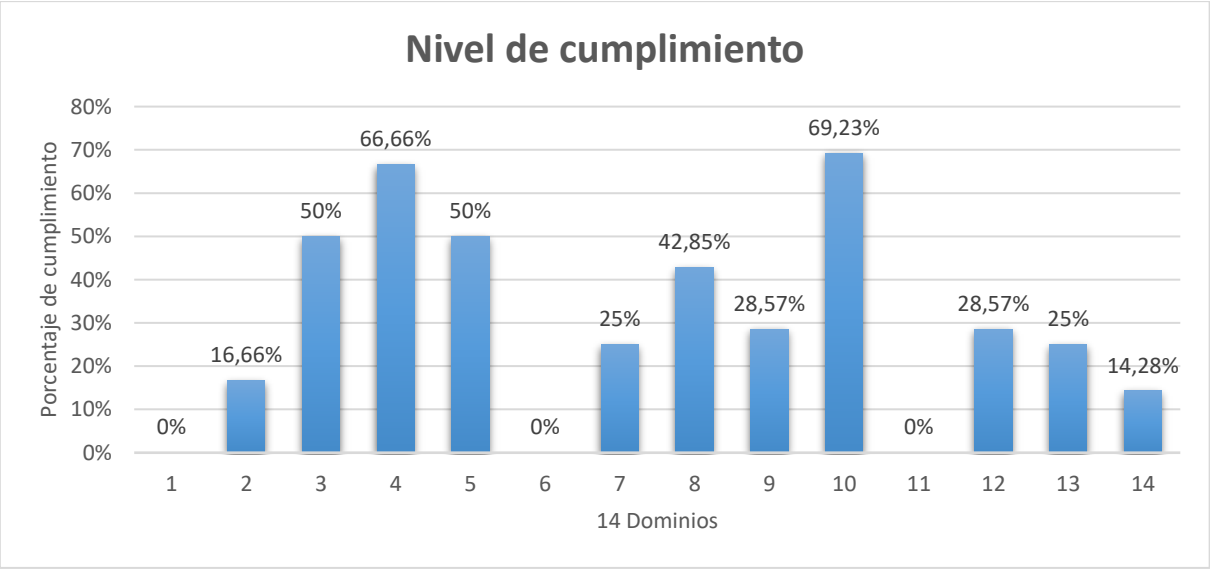


Figura 14 Porcentaje de cumplimiento actual

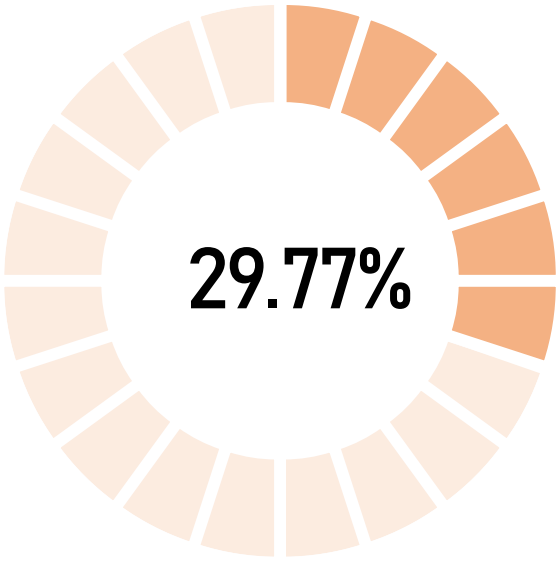


Figura 15 Porcentaje total del cumplimiento actual

Se puede determinar el porcentaje total del cumplimiento que actualmente está establecido, tomando en cuenta la verificación de los controles de seguridad de la información mediante la normativa analizada en la investigación, por lo tanto, al interpretar su bajo rendimiento se logra identificar falencias para así definir estrategias según los requerimientos detectados.

Tabla 11.
Incremento de cumplimiento en implementación de controles

Dominio	Descripción	Porcentaje de cumplimiento	Porcentaje implementado
5	Políticas de seguridad	0%	60%
6	Aspectos organizativos de la seguridad de la información	16.66%	60%
7	Seguridad ligada a los recursos humanos.	50%	86%
8	Gestión de activos	66.66 %	66.66%
9	Control de accesos.	50%	72.85%
10	Cifrado.	0%	50%
11	Seguridad física y ambiental.	25%	61.66%
12	Seguridad en la operativa.	42.85%	65.71%
13	Seguridad en las telecomunicaciones.	28.57%	60%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	69.23%	70.76%
15	Relaciones con suministradores.	0%	44%
16	Gestión de incidentes en la seguridad de la información.	28.57%	68.57%
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	25%	50%
18	Cumplimiento.	14.28%	57.5%

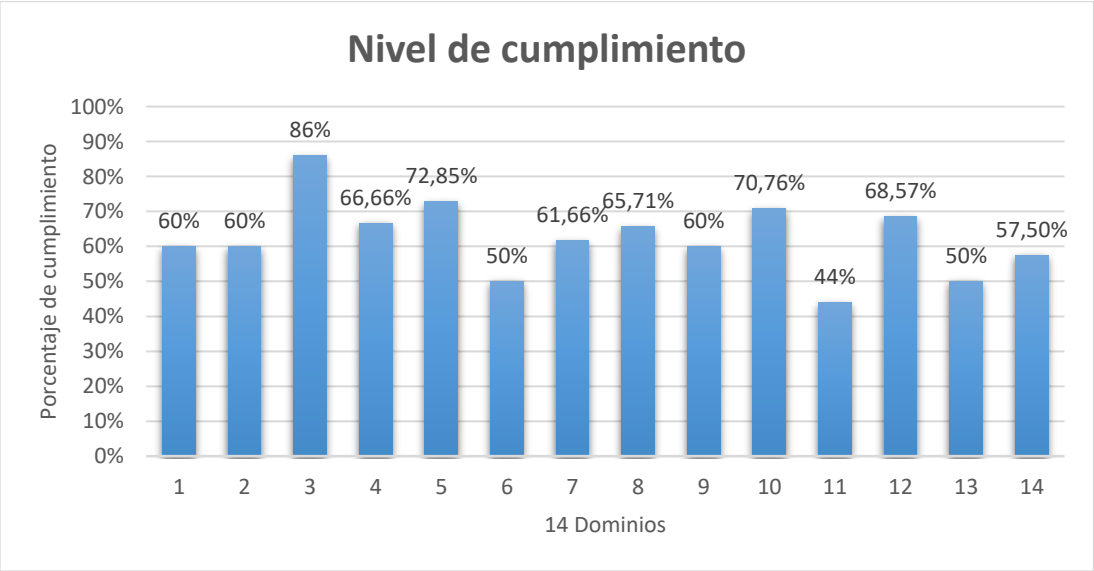


Figura 16 *Porcentaje de cumplimiento en una posible implementación*

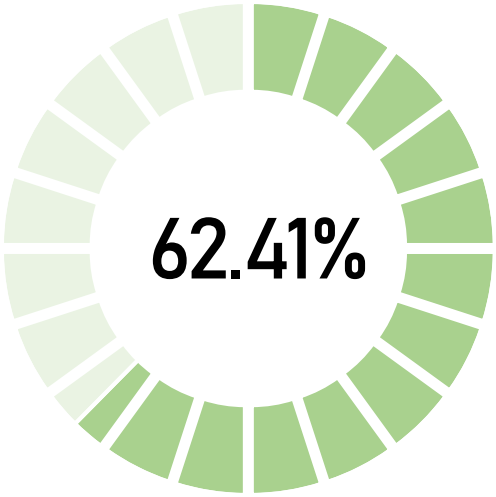


Figura 17 Porcentaje total del incremento de cumplimiento implementado

El incremento de seguridad de la información que se estima lograr al proponer la implementación alcanza un porcentaje óptimo, ayudando a reducir considerablemente los posibles riesgos asociados con las vulnerabilidades encontradas en la investigación, de modo que, las buenas prácticas y la mejora continua prevalece al ejecutar los controles que están vinculados a los requisitos de las instituciones.

De acuerdo al ministerio de Telecomunicaciones y de la Sociedad de la Información menciona que el Esquema Gubernamental de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, se establecen diversas normativas que para el cumplimiento total garantizando reducción de riesgos, revisiones continuas, continuidad de servicios, entre otros.

En base al análisis realizado mediante la normativa ISO/IEC 27002 se logra el 62.41% de cumplimiento dentro de los 114 controles que abarca el estándar, de modo que, al ser una institución gubernamental es necesario complementar el EGSI que contribuye con el porcentaje restante a la investigación como la ISO 27005 Gestión de Riesgos.

4.1.7 CONTROLES CON NO CONFORMIDAD Y HALLAZGO DE RIESGOS

De acuerdo a la normativa ISO 27002 los controles establecidos presentan falencias de seguridad de la información, por ende, se aplican estrategias de mitigación y representación de riesgos para establecer el impacto que genera el no implementar normativa correspondiente.

Tabla 12.

Estrategias de mitigación ISO/IEC 27002

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

ESCASA APLICACIÓN DEL POLÍTICAS DE SEGURIDAD			
R1	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción del riesgo			
Realizar procesos de manera inadecuada, sin documentación y normativa que lo respalde, siendo justificado por la experticia del personal del área de sistemas sin autorización de altos funcionarios genera vulnerabilidad en distintos campos ya que no llevan acciones correctivas de manera regular alterando la seguridad del gobierno de tecnología.			
Estrategias de Mitigación			
○ Establecer políticas específicas relacionada con la constitución y normativas legales enfocadas en nivel operativo, tecnológico, entre otros. ○ Definir la implementación del Sistema de Gestión de la Seguridad de la Información. ○ Realizar una auditoría de seguridad de la información para determinar normas aplicables para la implementación de controles. ○ Revisión de las políticas de seguridad de la información de manera regular. ○ Mantener su registro de revisiones y acciones correctivas supervisadas por dirección.			

- Controlar que la planificación de controles sea realizada por personal autorizado y competente o bajo supervisión de funcionarios de área de sistemas como también de expertos contratados para ese propósito.
- Socializar las políticas probadas por dirección a todos los funcionarios.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1	*Organización Interna*
6.1.1	Asignación de responsabilidades para la seguridad de la información
6.1.2	Segregación de tareas.
6.1.4	Contacto con grupos de interés especial.
6.1.5	Seguridad de la información en la gestión de proyectos.
6.2	*Dispositivos para movilidad y teletrabajo*
6.2.2	Teletrabajo.

PERSONAL INSUFICIENTE			
R2	**Prioridad** 16	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

Al no existir un oficial de seguridad de la información unas representaciones significativas de procesos de seguridad se verán afectados, siendo encargado del cumplimiento de las actividades basados en políticas o normas de seguridad y dar seguimiento de los controles que determinan los lineamientos necesarios para la protección de la institución.

Estrategias de Mitigación

- Contratar personal capacitado en temas de seguridad de la información responsable de procesos de control.
- Establecer en el manual de funciones responsabilidades de Oficial de seguridad para determinar el resguardo de la información y varias acciones dentro del control establecido.
- Instruir al oficial de sistemas siendo de emitir reportes de las áreas afectadas y su impacto por incidentes.
- Establecer un encargado de definir controles preventivos eliminando o mitigando vulnerabilidades de sistemas o servicios detectando debilidades recurrentes.

- Asegurar los lineamientos para el uso de recursos de las TI contemplando los requerimientos sobre seguridad de la información según su criticidad.
- Gestionar actividades de manera periódica para garantizar de manera oportuna y adecuada la seguridad de la información.
- Definir el responsable de documentar los controles necesarios para la detección y protección de los servicios de la institución.
- Establecer contactos con grupos de interés especiales manteniendo así la competitividad y actualización requerida por la seguridad de la información.
- Verificar el cumplimiento de la normativa mediante responsabilidades generando informes técnicos indistintamente de las acciones realizadas.
- Asignar responsabilidades para el desarrollo de proyectos y controles de seguridad de la información reduciendo vulnerabilidades.
- Definir estrategias de implementación que brinde seguridad de la información que se accede mediante teletrabajo.
- Realizar el registro de dispositivos incluyendo conexiones remotas y restricciones.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.2	*Durante la contratación*
7.2.1	Responsabilidad de gestión
7.2.2	Concienciación, educación y capacitación en segur. de la información
7.2.3	Proceso disciplinario.

NO SE APLICA UN PLAN DE CAPACITACIÓN SOBRE SEGURIDAD DE LA INFORMACIÓN

R3	**Prioridad** 9	**Tipo de riesgo**	Medio Media probabilidad – medio impacto

Descripción del riesgo

Existen capacitaciones orientadas por el jefe del área de sistemas, pero no adecuando normas, políticas o conocimiento sobre seguridad de la información a funcionarios de áreas específicas, las acciones dependen de la toma de decisiones sin ser socializado de manera oportuna.

Estrategias de Mitigación

- Concientizar la necesidad de adquirir conocimiento de la seguridad de la información durante la contratación.
- Acordar condiciones laborales apropiadas a sus funciones y responsabilidades incluyendo las métricas de seguridad de la información de la institución.

  -Encargado de administración de servidores, respaldos de información, almacenamiento, redes de datos, base de datos, aplicación de negocios, recursos informáticos, entre otros.

  -Líderes de proyecto, personal de capacitación, programadores, documentación de entornos para desarrollo, pruebas, capacitación y producción.
- Socializar de manera oportuna sobre las responsabilidades legales dentro de los procedimientos para la seguridad.
  - Considerando sanciones dependiendo cantidad y gravedad de violación e impacto.
- Se capacita mencionando controles y procesos implementados en la institución a todo el personal.
  - Nivel de capacitación, Ley de Comercio Electrónico, Firmas Electrónicas, SGSI y otros factores propios de la entidad.
- Dar a conocer el uso correcto de recursos o servicios de la información.
  - Aplicativos de servicios informáticos, soporte, reportes físicos y electrónicos, documentación de capacitaciones y evaluaciones.
- Establecer procesos de seguridad como: gestión de activos, uso de contraseñas seguras, limpieza de escritorios, entre otros.

8. GESTIÓN DE ACTIVOS	
8.2	*Clasificación de la información.*
8.2.1	Directrices de clasificación.
8.2.2	Etiquetado y manipulado de la información.
8.2.3	Manipulación de activos.

INFORMACIÓN SIN CATEGORIZAR			
R4	**Priorida**d 8	**Tipo de riesgo**	Medio
			Baja probabilidad – alto impacto
Descripción del riesgo			

No existe alineación para la clasificación de la información, siendo un proceso necesario para asegurar la información si ese es el caso, otorgando el grado de importancia se asegura la información en base a: confidencialidad, integridad y disponibilidad.

Estrategias de Mitigación

- Definir al personal adecuado responsable de supervisar el cumplimiento del proceso de generación de rotulación de activos.
- Clasificar en pública o confidencial la información.
- Elaborar un listado aprobado para la clasificación de la información considerando la normativa establecida.
- Categorizar la información basada en requisitos legales, sensibilidad e importancia hacia la institución.
- Su clasificación dependerá del nivel de protección valorando la confidencialidad, integridad y disponibilidad.
- Establecer un sistema de etiquetas en caso de formatos electrónicos se debe asociar un metadato único.
- Generar etiquetas de acuerdo al tipo de activos y a la funcionalidad, en caso de repetirse se deberá añadir un número secuencial.

  – En etiquetas físicas el personal responsable deberá verificar que sean legibles y se encuentre rotulado en un periodo de 6 meses aproximadamente.
- Establecer un inventario de los activos en caso de destrucción, para mantener un registro de las acciones realizadas asociadas a sus respectivas etiquetas.
- Generar código MD5 en caso de mantener documentos en formato electrónico.

9. CONTROL DE ACCESOS.

9.1	*Requisitos de negocio para el control de accesos.*
9.1.1	Política de control de accesos.
9.1.1	Control de acceso a las redes y servicios asociados.
9.2	*Gestión de acceso de usuario.*
9.2.5	Revisión de los derechos de acceso de los usuarios.
9.3	*Responsabilidades del usuario*
9.3.1	Uso de información confidencial para la autenticación.
9.4	*Control de acceso a sistemas y aplicaciones.*
9.4.1	Restricción del acceso a la información.

ESCASOS REQUISITOS DE CONTROL DE ACCESOS			
R5	**Prioridad** 12	**Tipo de riesgo**	Alto Media probabilidad – alto impacto
Descripción del riesgo			
Al no existir restricciones compromete a la intercepción de información o manipulación no autorizada de hardware y software, pérdida de servicios y otras amenazas, entre otras acciones fraudulentas.			
Estrategias de Mitigación			

- Establecer políticas de control de acceso para gestionar la autorización a los usuarios previniendo acciones no autorizadas.
- Definir el responsable encargado de otorgar el acceso de la información asignando la menor cantidad de privilegios y el tiempo determinado para el desarrollo.
- Depurar usuarios en un período aproximado de 30 días, en caso de cambios la gestión se la realizara de inmediato.
- Establecer la disponibilidad de acceso en los archivos log de los sistemas en el momento que sean requeridos.
- Retirar privilegios al acceso de información de manera inmediata al comunicar la terminación laboral socializando con el responsable de la seguridad de la información.
- Exigir a los usuarios la prioridad correspondiente a la autenticación y su confidencialidad.
- Definir políticas para el control que prohíba todos los accesos en funciones de sistemas o servicios y se permitan realizar acciones determinadas y autorizadas.
- Establecer derechos de accesos de lectura, eliminación y ejecución a usuarios que realizan procesos de la información.
- Realizar revisiones periódicas garantizando que la información se envíe únicamente en terminales autorizados.

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

MANEJO INADECUADO DE DATOS CRÍTICOS			
R6	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

Los datos críticos son determinantes en una organización, se prioriza debido a su vulnerabilidad; en el GAD municipal no cuentan con sistemas de cifrados dejando a exposición datos relevantes.

Estrategias de Mitigación

- Estudiar la viabilidad de la criptografía como requerimiento de seguridad.
- Resguardar documentación que contengan descripciones técnicas con algoritmos y programas con sistemas de cifrado de archivos de toda la información indispensable que tengan relación con claves o firmas electrónicas.
- Establecer en los sistemas de almacenamiento de datos se logren recuperar en formatos legibles en un período determinado con sus respectivas restricciones.
- Determinar el nivel de protección que debe obtener la información considerando el tipo y la calidad de algoritmo de cifrado.
- Usar controles seguros que protejan las claves de acceso, siendo almacenadas de manera codificada y encriptada dentro de las bases de datos.
- Implementar procedimientos para la administración de claves, recuperación de información, daños de claves o en reemplazo de claves de cifrado.
- Adaptar nomas para la información clasificada que se transmita fuera de la institución, por medios móviles u otros dispositivos de comunicación.
- Establecer algoritmos de encriptación en toda la institución dependiendo el propósito, proceso o actividad a aplicar implementando controles que deben ser revisado y actualizados de manera periódica.

11. SEGURIDAD FÍSICA Y AMBIENTAL	
11.1	*Áreas seguras.*
11.1.1	Perímetro de seguridad física.
11.1.2	Controles físicos de entrada.
11.1.3	Seguridad de oficinas, despachos y recursos
11.1.4	Protección contra las amenazas externas y ambientales.
11.1.5	El trabajo en áreas seguras.
11.1.6	Áreas de acceso público, carga y descarga.
11.2	*Seguridad de los equipos.*
11.2.3	Seguridad del cableado.
11.2.4	Mantenimiento de los equipos.

DEFICIENTE RESTRICCIÓN DE ACCESO FÍSICO			
R7	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

No existen perímetros de seguridad controladas por bandas magnéticas o alguna barrera de protección, el acceso físico está disponible para cualquier usuario, no se realiza registro de ingreso al área de sistemas, al no evaluar la estancia en el área no se logra verificar las acciones realizadas en posibles daños y su causante, tomando en cuenta que es la base central de activos informáticos.

Estrategias de Mitigación

- Documentar perímetros de seguridad física necesarios mediante diversos accesos de control y adecuación. (barreras físicas, puertas de acceso, tarjetas magnéticas, entre otros.)
- Establecer un área de recepción para controlar el acceso dentro del área de sistemas.
- Disponer de cámaras de vigilancia para supervisar la permanencia de personas en áreas restringidas.
- Actividades dentro del área limitadas exclusivamente para personal autorizado utilizando controles de autenticación.
- Registrar del ingreso del personal en el área de sistemas definiendo la hora y fecha de su ingreso y salida.

- Establecer personal autorizado para escoltar a visitantes quienes deberán transitar en áreas restringidas.
- Actualizar en un periodo determinado la documentación de derechos de accesos en áreas restringidas firmados por los responsables.

ROBO DE EQUIPOS			
R8	**Prioridad** 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Descripción del riesgo

El robo de equipos es un riesgo fundamental que se debe proteger, considerado como delito informático por la cantidad de información confidencial que pueden almacenar, de igual manera puede originar divulgación de datos y otros delitos considerando la prioridad de la información.

Estrategias de Mitigación

- Instalar perímetros físicos de seguridad, restringiendo el paso de personal mediante tarjetas magnéticas, o barreras de protección.
- Supervisar el lapso de permanencia de individuos dentro de áreas restringidas, tomando registro de horario de su ingreso y salida**.**
- Proteger áreas restringidas que mantengan prioridad evitando así el acceso público a las instalaciones.
- Establecer dentro del área de sistemas acuerdos de responsabilidad de activos físicos.
- Aislar los equipos de procesamiento de información sensible que requieran protección especial evitando visualización a personas no autorizadas.
- Apoyo con cámaras y alarmas dentro del área restringida para detectar intrusos.

FALLAS ELÉCTRICAS			
R9	**Prioridad** 9	**Tipo de riesgo**	Medio
			Media probabilidad – Medio impacto

Descripción del riesgo

La interrupción de energía eléctrica puede ser frecuente en las instituciones, aunque representan un alto porcentaje en pérdida de datos, no disponibilidad de servicios y degradaciones de hardware, se puede lograr inestabilidad en un lapso no determinado bajando la productividad.

Estrategias de Mitigación

- Establecer mantenimiento de forma periódica de las instalaciones eléctricas.
- Disponer de protección contra descargas eléctricas.
- Implementación de generadores de energía
- Utilizar filtros protectores en el suministro eléctrico y en líneas de comunicación en toda la institución.
- Realizar respaldo de información cumpliendo todos los requisitos de seguridad establecidos.
- Permitir de manera ordenada el cierre/apagado de los servicios que soportan operaciones críticas.
- Adoptar estrategias dentro del plan de contingencia ante este riesgo.

INEXISTENCIA DE PLAN DE CONTINGENCIA			
R10	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto

Descripción del riesgo

La institución no cuenta con la alternativa de operaciones funcionales para cubrir incidentes o condiciones externas, ajenas a las actividades dentro la institución, garantizando la continuidad de operaciones, retomado con normalidad el cumplimiento de sus actividades.

Estrategias de Mitigación

- Definir el impacto y proporcionar cambios sobre la continuidad de servicios.
- Categorizar la información y su acceso para posteriormente analizar los riesgos dando solución y lograr adaptación.

- Establecer estrategias para minimizar el impacto en desastres inesperados en la institución.
- Aprobar el plan de contingencia identificando los posibles procedimientos que se deberán realizar en base a lo físico e intangible.
- Aplicar el plan de contingencia dependiendo de la funcionalidad o impacto que se haya generado.

RED CABLEADA EXPUESTA Y CON DETERIORO			
R11	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

Los equipos se encuentran sin ninguna protección que evite la manipulación de terceros, siendo víctimas de robo de estructura física, el cableado deteriorado causa mal funcionamiento a pesar de no establecer etiquetas para evitar conflictos al momento de supervisar y controlar sus funciones.

Estrategias de Mitigación

- Custodiar el cableado de red contra daño o intercepción bajo un responsable autorizado.
- Proteger dispositivos de comunicaciones bajo barreras físicas que tengan acceso a los módulos de conexión
- Separar los cables de red y comunicación a los cables de energía.
- Adaptar controles como firewalls en la red.
- Aplicar cableado estructurado de acuerdo a normas establecidas por el área de sistemas evitando errores de manejo enfatizando en el etiquetado.
- Establecer documentación de distribución de conexiones alámbricas e inalámbricas.
- Realizar mantenimiento de acuerdo a las especificaciones del proveedor de manera periódica.
- Definir controles para el mantenimiento preventivo o correctivo ya sean programados o emergentes.

INADECUADO MANTENIMIENTO DE EQUIPOS			
R12	**Prioridad** 9	**Tipo de riesgo**	Medio Media probabilidad – medio impacto
Descripción del riesgo			
No existe mantenimiento de manera periódica, se lo realiza por medio de peticiones de los funcionarios, esto disminuye la productividad en los procesos y responsabilidades establecidas diariamente ya que no se verifica la vida útil de los equipos en funcionamiento.			
Estrategias de Mitigación			
○ Establecer personal apropiado y autorizado para realizar procedimientos planificados. ○ Definir la gestión de reparación de inicio a fin con el respectivo responsable previamente en conocimiento del jefe de sistemas. ○ Realizar mantenimiento de equipos de forma periódica en software de servicio, gabinetes de servidores, telefonía, sistemas de UPS, instalaciones eléctricas, sistemas de climatización y ductos de ventilación. ○ Realizar mantenimientos de corrección y prevención solucionando fallas relevantes o dudosas. ○ Realizar mantenimiento de acuerdo a recomendaciones específicas de los proveedores. ○ Implantar controles asociados con el mantenimiento programado y emergente. ○ Notificar a los usuarios sobre los cambios a realizar y el lapso de ejecución. ○ Revisar los controles que garanticen la integridad y no comprometer con los cambios asociados. ○ Entregar documentación de las acciones realizadas			

SISTEMAS DE CLIMATIZACIÓN Y CONDUCTOS DE VENTILACIÓN MAL ESTRUCTURADO			
R13	**Prioridad** 9	**Tipo de riesgo**	Medio Media probabilidad – medio impacto
Descripción del riesgo			

El área no cuenta con sistemas de climatización apropiados y no existen conductos de ventilación o enfriamiento, arriesgando el funcionamiento de los equipos informáticos dentro de esta zona.

Estrategias de Mitigación

- Implementar sistemas de enfriamiento con aire de manera redundante para mantener la temperatura en caso de presentar fallas.
- Impulsar al consumo considerable de refrigeración como aire acondicionado ya que atribuye ineficiencias, establecer equipos de enfriamiento óptimo.
- Instalar racks en una configuración de pasillos fríos y calientes logrando patrones de flujo.
- Alinear los equipos con requisitos de temperatura similares y carga de calor, y aislar los equipos de temperatura y humedad de enfriamiento para disminuir el consumo de energía.
- Eliminar infiltraciones sellando o bloqueando entradas físicas en paredes o piso.
- Documentar servicios de calefacción, ventilación y aire acondicionado posibles a implementar para obtener la aprobación de la institución.
- Realizar mantenimiento de manera periódica en los sistemas de climatización y ductos de ventilación.
- Inspeccionar los suministros del área.

12. SEGURIDAD EN LA OPERATIVA.	
12.1	*Responsabilidades y procedimientos de operación.*
12.1.2	Gestión de cambios.
12.1.3	Gestión de capacidades.
12.2	*Protección contra código malicioso.*
12.2.1	Controles contra el código malicioso.
12.3	*Copias de seguridad.*
12.3.1	Copias de seguridad de la información.
12.3	*Gestión de la vulnerabilidad técnica.*
12.6.1	Gestión de las vulnerabilidades técnicas.
12.6.2	Restricciones en la instalación de software.
12.7	*Consideraciones de las auditorías de los sistemas de información.*
12.7.1	Controles de auditoría de los sistemas de información.

SOFTWARE MALICIOSO			
R14	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción del riesgo			
El riesgo de los programas maliciosos es su cobertura en un alto impacto enfrentando directamente la confidencialidad, disponibilidad e integridad de la información independiente del estado crítico de la misma, puede ejecutarse por varios medios, ya sea por usuarios internos o externos a la institución.			
Estrategias de Mitigación			
○ Documentar procedimientos dentro del área de sistemas para evaluar la información relativa a software malicioso. ○ Implementar controles para la protección contra software malicioso garantizando seguridad en los datos de los servicios de la institución. ○ Acuerdo de confidencialidad no ingresar ningún tipo de software que no sea autorizado. ○ Realizar un listado del acceso al personal de desarrollo y el uso de software bajo autorización. ○ Establecer responsables de procedimientos formales en instalación de equipos para evitar vulnerabilidad. ○ Implantar procesos para evitar descargas de archivos a través de redes externas. ○ Instalar y actualizar habitualmente software contra código malicioso. ○ Revisar de manera periódica el contenido de los equipos. ○ Contratar distintos proveedores de canales de datos de filtrado de servicios malware, virus, spam, entre otros. ○ Definir auditorías periódicas para una certificación de calidad y revisión de códigos para detectar código malicioso cumpliendo requerimientos de seguridad de software. ○ Realizar pruebas antes y después de la instalación de software para la detección de códigos maliciosos.			
INADECUADO RESPALDO DE INFORMACIÓN			
R15	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción del riesgo			

El respaldo de información debe contar con un proceso establecido que determine las acciones necesarias a realizar, siendo una copia de información de importancia se lo realizará periódicamente como precaución de daños a los dispositivos de almacenamiento o errores en estructuras lógicas, estableciendo simultáneamente el valor original.

Estrategias de Mitigación

- Definir el responsable del área de sistemas que determinará los procesos para el respaldo y contención de la información.
- Documentar detalladamente los procesos de restauración y respaldo de la información.
- Identificar el contenido de las copias a respaldar para determinar su periodicidad de acuerdo a los requisitos establecidos por la institución.
- Realizar de manera periódica respaldos de información.
- Respaldar la información y guardar en un lugar alejado a una distancia prudente para evitar vulnerabilidad si existe daños en el área principal.

RESTRICCIONES DE SOFTWARE SIN IMPLEMENTAR

R16	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

Al no controlar las restricciones necesarias para la implementación de software podemos limitar las capacidades de desarrollo o de usuarios, de otra manera se originan instalaciones con software dañino.

Estrategias de Mitigación

- Definir al personal capacitado para realizar revisiones en el software para garantizar que no se alteren los requerimientos por seguridad.
- Considerar los términos y condiciones establecidas en las licencias de software de código abierto o privativo.
- Establecer procesos de actualización de sistemas asegurando que loa parches sean autorizados.
- Elaborar informes que detallen cambios o acciones en el software.
- Corroborar los términos y condiciones que establecen las licencias de software.
- Verificar que se instale únicamente software autorizado.

- Controlar las versiones de software para mantener actualizaciones necesarias.
- Realizar cambios en una copia de software original para aplicar las versiones necesarias.
- Realizar pruebas y documentar detalladamente para mejoras a futuro si la aplicación es requerida.

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

INFRAESTRUCTURA SIN SEGMENTACIÓN DE RED APROPIADA			
R17	**Prioridad** 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Descripción del riesgo

El riesgo de no hacer uso de Vlans, es complicar la gestión de red provocando dificultad para detectar problemas que se puede ocasionar, dividir la red ayuda a un mejor rendimiento y mitigación de broadcast.

Estrategias de Mitigación

- Segmentar redes en el área de gestión o procesos con la capacidad considerable que sea necearía, mientras los recursos se ajusten a los requerimientos.
- Desinar responsabilidades para gestionar equipos remotos, puertos y accesos por VPNs.
- Ejecutar controles para salvaguardar la información, implicando la confidencialidad, disponibilidad e integridad, dentro de las redes públicas, inalámbricas y locales.
- Disponer de documentación donde se establezca la esquena de red, internet, enlaces, redes y sus dominios.

- Documentar los riesgos posibles a encontrarse en activos críticos identificando de los segmentos de red.
- Clasificar la información para realizar la separación de redes considerando la protección a los activos, considerando la división de dominios internos y externos.
- Realizar configuraciones para filtrar el tráfico de red permitiendo bloqueos a el acceso no autorizado.
- Separar redes inalámbricas enlazadas a redes privadas evitando el acceso de información a terceros.

INTRUSIÓN DE RED

R18	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto

Descripción del riesgo

Los sistemas de red que no son escaneados son los más vulnerables ya que no poseen un control que verifique conexiones de equipos o especificar el uso de una red, las personas que no tienen autorización fácilmente podrían acceder a la información por este medio causando fuga de información que es un riesgo silencio, en el que no se puede preservar información mediante transferencia de datos, no se puede asegurar la privacidad mediante este ataque.

Estrategias de Mitigación

- Definir gestiones asociadas con la vulnerabilidad técnica incluyendo monitoreo, rastreo, uso de parches en los activos requeridos.
- Implementar sistemas de firewall y equipos de comunicación.
- Poner en funcionamiento un sistema de prevención detección de intrusos. IDS/IPS.
- Configuración de firewall.
- Monitorear el acceso que tienen los funcionarios en la red para detectar ataques reales.
- Revisión periódica a sistemas de escaneo de red.
- Protección de cableado de red
- Establecer UTM como método de prevención.

CAÍDA DE SISTEMAS DE COMUNICACIÓN			
R19	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

El riesgo de error de comunicación afecta directamente en la disponibilidad de la información, causando acumulación de actividades cotidianas y pérdida de tiempo, el manejo de la red es indispensable para todos los funcionarios y causando disgustos en los usuarios que acceden a los servicios en línea de la institución.

Estrategias de Mitigación

- Establecer controles de datos en las redes públicas salvaguardando la integridad, confidencialidad y disponibilidad.
- Desarrollo de planes de gestión ante incidentes de disponibilidad
- Identificar incidentes de incumplimiento de leyes que provoquen no disponibilidad.
- Monitoreo y alertas en errores de fallas en los sistemas de comunicación.
- Determinar varios proveedores manteniendo el balance de carga para la disponibilidad de procesos en las instalaciones.
- Tener protección en líneas de comunicación en toda la institución.

INEXISTENCIA DE ACUERDOS DE CONFIDENCIALIDAD			
R20	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Descripción del riesgo

El personal del área de sistemas no cuenta con un acuerdo de confidencialidad o no divulgación de información, tomando en cuenta que son funcionarios encargados de mantener datos altamente importantes, al no determinar términos y condiciones se verá vulnerado la seguridad de los usuarios siendo la prioridad de la institución.

Estrategias de Mitigación

- Determinar términos y condiciones de contratación para la seguridad de la información.
- Establecer como requisito principal un acuerdo de confidencialidad o no divulgación, antes de adquirir información.

- Explicar la responsabilidad e importancia de las acciones de los funcionarios en base a la normativa.
- Acordar términos y condiciones bajo técnicas adecuadas para condiciones laborales que incluyen en la política de seguridad.
- Incluir la permanencia de requisitos para la protección de información mediante responsabilidades legales.
- Determinar en los acuerdos de confidencialidad actividades válidas aun después de su culminación laboral.
- Comunicar la importancia de acuerdos de confidencialidad en contratos laborales a nuevos funcionarios, contratistas o usuarios se deberá instaurar la documentación respectiva.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	
14.1	*Requisitos de seguridad de los sistemas de información***.**
14.1.1	Análisis y especificación de los requisitos de seguridad.
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3	Protección de las transacciones por redes telemáticas.

LIMITADOS REQUISITOS DE SEGURIDAD DE COMUNICACIONES			
R21	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción del riesgo			
No establecer los controles necesarios implica vulnerar los servicios informáticos ya que no aseguran su validación con métodos de protección en cualquier ambiente interno o externo.			
Estrategias de Mitigación			

- Establecer requerimientos de seguridad y controles apropiados manuales o automáticos.
- Definir los responsables del personal técnico que trabajarán en los sistemas.
- Establecer los niveles que se va a requerir en las aplicaciones para determinar requisitos de autenticación.

- Evaluar requerimientos proporcionales en costos y para protección de daños o fallas que se puedan ocasionar.
- Identificar que los proveedores establezcan contratos contemplando la seguridad en caso de adquirir productos.
- Proteger la información de actividades fraudulentas que un servicio puede prestar a través de redes públicas.
- Utilizar protocolos seguros en caso de transacción de información haciendo uso de firmas digitales.
- Hacer usos de sistemas de prevención de envío que no se permita en redes públicas.
- Implementar sistemas de protección contra envíos involuntarios de información.

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

INSUFICIENTES CONTROLES DE SERVICIOS PARA SUMINISTRADORES			
R22	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto
Descripción del riesgo			
Los servicios contratados contemplan un nivel apropiado dentro de la seguridad de la información, al no implementar acuerdos y monitorear el cumplimiento necesario podrían vulnerar conexiones o flujo de información indispensable de la institución.			
Estrategias de Mitigación			

- Documentar los requisitos necesarios para la seguridad de la información y acordar el acceso a proveedores.
- Definir procesos necesarios de acuerdo a la evacuación de la información antes de la contratación de servicios.

- Adecuar controles limitando el acceso innecesario a la información para el desarrollo de trabajos.
- Supervisar los procedimientos establecidos y acordados con proveedores y a los funcionarios encargados de la verificación.
- Establecer que el proveedor informe si existen cambios ya sea de personal o servicios y el momento en el que serán realizados.
- Solicitar informes a los proveedores de acuerdo al servicio prestado.

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

INADECUADO CONTROL EN LA GESTIÓN DE EVENTOS			
R23	**Prioridad** 9	**Tipo de riesgo**	Medio Medio probabilidad – alto impacto
Descripción del riesgo			
Los incidentes que no son notificados generan conflicto a largo plazo, causando daños mayores sin una revisión previa, su valoración ayuda a la toma de decisiones para prevenir y mejorar posibles incidentes.			
Estrategias de Mitigación			

- Reportar incidentes que generen vulnerabilidad monitoreando sistemas y ejecutando distintos procedimientos para gestionar incidentes.
- Planificar estrategias preventivas para incidentes o acciones correctivas para la seguridad de la información.
- Definir responsables de la seguridad de la información para reportar inconvenientes, que brinde disponibilidad y respuestas oportunas.
- Solucionar incidentes y notificar las acciones de restauración del sistema o servicio afectado.

- Realizar auditorías para establecer buenas prácticas y ayudar en la toma de decisiones.
- En caso de detectar vulnerabilidades por parte de funcionario o proveedores se notificará al jefe de área con registro de nombres, fecha, hora y el inconveniente, para tomar medidas pertinentes.
- Priorizar incidentes de acuerdo al criterio afectado, llevando registro para analizar los parámetros de resolución e impacto.
- Evaluar que el área de sistemas tenga la capacidad de resolver eventos o requiere apoyo externo.
- Realizar análisis de cada incidente para puntualizar las causas y evitar inconvenientes próximos.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
17. 1	*Continuidad de la seguridad de la información.*
17.1.1	Planificación de la continuidad de la seguridad de la información.
17.1.2	Implantación de la continuidad de la seguridad de la información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

INEXISTENCIA DE PLAN DE CONTINUIDAD DE NEGOCIO			
R24	**Prioridad** 9	**Tipo de riesgo**	Medio Media probabilidad – alto impacto
Descripción del riesgo			
Al no existir un plan de continuidad de negocio incrementa riesgos en procesos volviéndolos ineficientes, que pueden interrumpir operaciones de la institución, la disminución actividades sin planificación será el factor fundamental de vulnerabilidad siendo este un nivel importante de preparación para la organización.			
Estrategias de Mitigación			

- Establecer la planificación e implementación de aspectos de continuidad de la seguridad de la información recobrando su proceso en el menor tiempo.

- Determinar actividades con objetivos y alcance considerando el tiempo de recuperación.
- Definir equipos destacados responsables de la continuidad de los servicios informáticos.
- Capacitar al personal que contemplan los procedimientos establecidos dentro del plan de continuidad de la seguridad de la información.
- Realizar pruebas para revisión y validación de la capacidad de respuesta ante desastres.
- Ejecutar simulaciones que permitan evaluar el plan de continuidad.
- Actualizar y corregir actividades que contemplen el plan de continuidad para el funcionamiento de servicios informáticos.
- Establecer estrategias en base a auditorías internas y externas que ayuden a mitigar desastres.

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

ESCASOS REQUISITOS LEGALES SOBRE LA SEGURIDAD DE LA INF.			
R25	**Priorida**d 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto
Descripción del riesgo			
Los requisitos están relacionados con la privacidad, derechos de autor y leyes de protección, su cumplimiento es importante debido a la evolución de ataques que pueden enfrentar, por ende, su aplicación se lo realiza en todas las áreas garantizando aportaciones de acciones correctivas.			

Estrategias de Mitigación

- Inventariar todo activo de información que cumpla con normas o reglamentos para cada servicio informático o software que utilicen en la institución.
- Establecer normas que pertenezcan a la gestión de información electrónica.
- Adquirir software de proveedores que garanticen derechos de propiedad intelectual considerando términos y condiciones que no sean violados.
- Proteger derechos de propiedad intelectual con registros apropiados en los activos de la información.
- Mantener evidencias de la propiedad de licencias, contratos, manuales, toda la información correspondiente al software a utilizar.
- Controlar el número máximo de usuarios que se puede permitir para un programa de software libre o privativo.
- Verificar que no se duplique contenido ni se extraiga archivos si no está permitido por el autor.
- Requerir que los responsables de desarrollo utilicen software aprobado por la institución.
- Realizar clasificaciones de registros electrónicos y físicos con su respectivo periodo de retención y medios de almacenamiento.
- Especificar y documentar el uso de encriptación y en qué ámbito se o aplicará.

INCENDIO

R.E	**Prioridad** 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Descripción del riesgo

El incendio al ser un riesgo no controlado produce daño en gran escala en la estructura de la institución, esto puede ser originado por diversos factores, un suceso físico, sucesos derivados por la impericia o negligencia de usuarios.

Estrategias de Mitigación

- Supervisar de manera periódica el funcionamiento en los sistemas eléctricos.
- Realizar simulacros de incendios y capacitaciones por parte del cuerpo de bomberos.
- Proporcionar equipos apropiados contra incendios y mantenerlos ubicados de manera adecuada.

- Almacenar materiales peligrosos a una distancia prudente de los activos.
- Adoptar estrategias del cuerpo de bomberos para desastres de esta magnitud.
- Ubicar los equipos de respaldo a una distancia prudente de las instalaciones principales.
- Establecer estrategias del plan de continuidad de negocios frente a desastres.

SISMO			
R.E	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto
Descripción del riesgo			
El riesgo sísmico independiente de su magnitud causa daños severos a los activos informáticos, aunque la probabilidad de esta actividad es baja puede producirse en cualquier momento provocando vulnerabilidad en un porcentaje considerable, más aún por la ubicación geográfica del país, sin embargo, la prevención y protección queda definida por las acciones y decisiones de la institución.			
Estrategias de Mitigación			

- Almacenar equipos backup y soporte.
- Establecer que los edificios tengan mapas de riesgos de evacuación mínimo apropiado.
- Informar a los funcionarios sobre áreas seguras existentes.
- Incluir alertas.
- Establecer planes de seguridad física exclusiva para el área de sistemas
- Evaluar la continuidad de la seguridad de la información verificando la capacidad de respuesta ante desastres.
- Validar la capacidad de los responsables permitiendo mantener los planes establecidos.
- Realizar simulaciones de escenarios para controlar el peligro de la operación de los servicios informáticos.

DAÑOS POR VANDALISMO			
R.E	**Prioridad** 8	**Tipo de riesgo**	Medio Media probabilidad – alto impacto

Descripción del riesgo
El daño a causa del vandalismo genera eventos o consecuencias adversas dependiendo de la magnitud del impacto físico, el peligro está relacionado con los daños a la infraestructura, equipos e instalaciones que están ubicados en un lugar visible para los agresores.
Estrategias de Mitigación
o Vigilancia permanente en zonas exteriores al área de sistemas. o Ubicación o Establecer seguridad a nivel de racks que se encuentren en las instalaciones de la institución minimizando amenazas externas. o Capacitar a los funcionarios del área de sistemas contemplando la continuidad de los servicios informáticos. o Evaluar la capacidad de respuesta ante desastres permitiendo actualizar y mejorara planes establecidos. o Aplicar un plan de continuidad considerando el peligro de los servicios informáticos minimizando la discontinuidad de actividades.

4.1.8 DETERMINACIÓN DE RIESGOS

Los riesgos son mecanismos que pueden ser valorados para dar solución, debido a que estos se vinculan directamente con la vulnerabilidad y amenazas a los activos mediante distintos procesos, es por eso que el análisis de riesgo es fundamental para una buena operatividad.

4.1.8.1 Riesgos externos

Los riesgos externos provocan daños de fuerza mayor convirtiéndose en grandes amenazas, es por eso que se debe definir ciertas estrategias para actuar en forma adecuada ante algún incidente, podemos mencionar ciertos riesgos que se han adecuado a las amenazas que en la institución efectuarse.

Tabla 13.
Riesgos externos

Riesgos Externos

N°	Riesgos	Probabilidad	Impacto	Prioridad
R1	Incendio en el área de sistemas	2	4	8
R2	Sismo	3	4	12
R3	Robo de equipos	2	4	8
R4	Daños por vandalismo	2	4	8

Podemos determinar que los riesgos provenientes de un entorno externo logran condicionar directa o indirecta un alto impacto sobre los que la institución no tiene control.

La institución debe establecer los análisis necesarios para la reducción de catástrofes, sobre las que no se puede ejercer ningún control, mejorando así la adaptación a cambios requeridos teniendo la capacidad de afrontarlos.

4.1.8.2 Riesgos internos

Los riesgos internos aparecen directamente de la gestión de la organización y sus procedimientos afectando a todas sus áreas sin distinción, por ende, realizar planes de mitigación con el fin de verificar su cumplimiento para evitar incidentes que están en constante control de la institución.

Se considera principalmente 25 situaciones de riesgo que se presentan en el análisis realizado basado en los controles de la norma ISO/IEC 27002 en el área de tecnología, se puede demostrar el nivel de impacto que podría provocar el incumplimiento de controles.

Tabla 14.
Riesgos Internos

Riesgos internos				
N°	Riesgos	Probabilidad	Impacto	Prioridad
R1	Escasa aplicación de políticas de seguridad	3	4	12
R2	Personal insuficiente	4	4	16
R3	No se aplica un plan de capacitación sobre seguridad de la información	3	3	9
R4	Información sin categorizar	2	4	8
R5	Escasos requisitos de control de accesos	3	4	12
R6	Manejo inadecuado de datos de críticos	3	4	12
R7	Deficiente restricción de acceso físico	3	4	12
R8	Robo de equipos	2	4	8
R9	Fallas eléctricas	3	3	9
R10	Inexistencias de planes de contingencia	3	4	12
R11	Red cableada expuesta y con deterioro	3	4	12
R12	Inadecuado mantenimiento de equipos	3	3	9
R13	Sistemas de climatización y conductos de ventilación mal estructurado	3	3	9
R14	Software malicioso	3	4	12
R15	Inadecuado respaldo de información	3	4	12
R16	Restricciones de software sin implementar	3	4	12
R17	Infraestructura sin segmentación de red apropiada	2	4	8
R18	Intrusión de red	3	4	12
R19	Caída de sistemas de comunicación	3	4	12
R20	Inexistencia de acuerdos de confidencialidad	4	3	12
R21	Limitados requisitos de seguridad de comunicaciones	4	3	12
R22	Insuficientes controles para servicios de suministradores	3	4	12
R23	Inadecuado control de la gestión de eventos	3	3	9
R24	Inexistencia de plan de continuidad de negocio	3	3	9
R25	Escasos requisitos legales sobre la seguridad de la inf.	3	4	12

Determinando los riesgos correspondientes de manera interna basados en la norma internacional ISO/IEC 27002 se puede verificar su prioridad en una matriz de riesgos

Tabla 15

Probabilidad - Impacto

			Impacto			
			Insignificante	Baja	Mediana	Alto
			1	2	3	4
bbbbbbProbab	Improbable	4			2	1
	Poco probable	3			6	14
	Ocasional	2				6
	Probable	1				

Mediante la matriz de calor se determina el alcance de los riesgos encontrados con mayor probabilidad e impacto, lo cual permite brindar prioridad por los daños que puede causar si no se logra rectificar las acciones de procedimientos establecidos, por lo tanto, toda acción no verificada correctamente produce ciertos incidentes dentro de la institución.

4.2. DISCUSIÓN

El análisis de la aplicación de la normativa internacional ISO/IEC 27002 con sus 14 dominios, 35 objetivos de control y sus 114 controles de seguridad de la información en el área de sistemas del GAD Municipal tiene como finalidad elaborar un informe sobre mitigación de riesgos, tomando en cuenta la verificación y cumplimiento desarrollado por los funcionarios de tecnologías; fundamentada de bibliográficamente con su marco referencial, realizando el cumplimiento del 62.42% al ser implementando, difiriendo en la complementación del EGSI que abarca diversas normativas, por lo tanto, podemos mencionar que el porcentaje establecido está en un rango que proporciona y garantiza mejoras en su funcionamiento, pero se podría implementar la norma ISO 27005 Gestión de Riesgos para obtener mayor alcance en el esquema gubernamental.

El proceso de lo ejecutó en diversas etapas las que fueron complementadas de manera ordenada para obtener los resultados eficaces, así se logró generar documentación con estrategias de mitigación relevantes que se han identificado por cada riesgo y prevención de vulnerabilidad dentro de la institución debido a su impacto y frecuencia.

De la selección riesgos el porcentaje alto y que se debe brindar prioridad están establecidos por alto impacto y alta frecuencia, es por eso que es indispensable priorizar estas deficiencias causando vulnerabilidad dentro de la institución.

De acuerdo a la investigación de Criollo, S. (2017) menciona que la implementación de la normativa internacional es una de las herramientas indispensables para la seguridad de la información, por ende, la normativa ISO/IEC 27002 ayuda a solventar problemas existentes en instituciones gubernamentales realizando el análisis de principales amenazas que ocasionan incidentes en el área de sistemas, beneficiando en el rendimiento óptimo con el manejo de estrategias adecuado y controles se seguridad de acuerdo a sus necesidades.

Por otro lado, Reyes, J. (2019) pone en evidencia como la implementación de un SGSI está ligado al compromiso con la seguridad y protección de información, lo que permite establecer bases apropiadas que garantice buenas prácticas y mejoras continuas, tomando en cuenta el valor de los elementos a proteger, además el departamento de sistemas es quien faculta la confidencialidad, disponibilidad e integridad, por ello, el objetivo es minimizar acontecimientos a los que están expuestos los procedimientos que no son priorizados dentro de la institución.

En la investigación de Tobón, A. (2018) lleva a cabo el proceso de análisis de riesgos para evaluar la particularidad de situaciones identificando su impacto y probabilidad, en la investigación se ha coincidido de la importancia de determinar dicho aspecto ya que ayuda a establecer estrategias de mitigación o prevención de riesgos asociados al no cumplimiento de

normativa establecida por el área de sistemas y a la vulnerabilidad que se puede generar por diversos aspectos de manera interna o externa.

Desde otra perspectiva a la investigación de Paguay, C., y Zamora, G. (2017) y la comparación de marcos de referencias no brinda la certeza del uso específico de normas de acuerdo a las necesidades de la institución, sin embargo, el proceso de auditoría en base a la normativa ISO/IEC 27002 permite contemplar cómo está establecida actualmente la institución de manera jerárquica, la estructura del área, como está conformada de manera organizacional y responsabilidades que cumplen los funcionarios, por ende, se puede apreciar a detalle las actividades o procedimientos, y especificar las causas iniciales de vulnerabilidades y solventar con estrategias correspondientes.

V. CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

- Se concluye que mediante la fundamentación bibliográfica se puede identificar la importancia de la seguridad de la información dentro de las instituciones y como se puede ver vulnerada ante amenazas internas o externas.
- En base al uso de metodologías de investigación e instrumentos de recolección de datos permitieron determinar detalladamente la situación actual del área generando conocimiento necesario para determinar las vulnerabilidades y posibles soluciones.
- El marco referencial ISO/IEC 27002 permite implantar estrategias para acciones específicas en los 114 controles de seguridad, por ende, los incidentes bajo una normativa y responsabilidad adquirida obtendría solución inmediata, se definen soluciones correctivas o preventivas por lo cual su cumplimiento es moderado de acuerdo con los resultados del análisis.
- Se logra determinar que el cumplimiento actual es el 29.77% lo cual no garantiza la seguridad de la información en la institución, por ende, se realiza una posible implementación en base a estrategias establecidas por los controles de seguridad del estándar que se proyecta un incremento significativo del 62.41% permitiendo garantizar la confidencialidad, disponibilidad e integridad de la información.
- La probabilidad y el impacto que genera el no adecuar los controles necesarios permite definir la prioridad de activos asegurando los servicios que brinda la institución y la conformidad del usuario, de modo que, se puede concluir que es indispensable realizar implementaciones sobre la gestión de riesgos para solventar con mayor precisión los requerimientos de seguridad

5.2. RECOMENDACIONES

- Implementar la normativa ISO/27002 con 14 dominios 35 objetivos de control y 114 controles que incluye distintas estrategias y recursos de la gestión de la seguridad de la información ya que se encuentra expuesta a diversos tipos de amenazas sujetas a la vulnerabilidad que pueda presentar.
- Proponer el proceso de implementación del complemento de la propuesta de la ISO 27005 estableciendo el cumplimiento del esquema gubernamental en la institución, definiendo los riesgos para establecer la causa inicial de posibles ataques y definir estrategias de prevención según el impacto que pueda generar en un determinado tiempo.
- Establecer la normativa necesaria para la seguridad de la información perteneciente a la institución que es emitido por el Ministerio de Telecomunicaciones y de la Sociedad de la Información realizados en 5 meses: Evaluación y Planificación y 7 meses: Implementación de controles.

IV. REFERENCIAS BIBLIOGRÁFICAS

Albarrán, S., Perez, J., y Valero, L., (2017) Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares. *Ideas en Ciencias de la Ingeniería,* vol.1, núm.1, pág 49-70. Recuperado de: https://hemeroteca.uaemex.mx/index.php/ideasingenieria/article/view/14591/10992

Arcentales, D., y Caycedo, X., (2016) Auditoría informática, *Dominio de las ciencias.*vol.3, 157-173. Recueprado de: https://dialnet.unirioja.es/servlet/articulo?codigo=6102836

Ávila, G. (2017) *Los instrumentos y técnicas como cuestiones indisolubles en el corpus teórico-metodológico del accionar del Trabajador Social,* recuperado de: https://www.margen.org/suscri/margen86/avila_86.pdf

Baena, G (2017) *Metodología de la investigación.* (3ª. ed) Editorial Patria. All rights reserved.http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Bailon, W (2019) Auditoría informática al control y mantenimiento de una infraestructura tecnológica. Revista Interdisciplinaria de Humanidades, Educación, Ciencia y Tecnología Año V. Vol. V. N°1. Edición Especial. 2019 Recuperado de: https://www.cienciamatriarevista.org.ve/index.php/cm/article/view/248/272

Benavides, C. (2017) *Como crear un plan de mitigación o un plan de contingencia de riesgos*. Recuperado de: https://calidadparapymes.com/plan-de-mitigacion-de-riesgos/

Bolaños, F., y Chica,. I (2017) Modelo de Defensa en Profundidad para los GADS (Gobiernos Autónomos Descentralizados) *Municipales del Ecuador con base al Sistema de Gestión de Información.* (Trabajo de Postgrado) Universidad Espíritu Santo, Samborondón – Ecuador. Recuperado de: http://repositorio.uees.edu.ec/bitstream/123456789/1430/1/MATIPaper-Ingrid%20Chica%20Cisneros.pdf

Borrero, P. (2019) *Identificación de activos de información, riesgos y controles asociados para la empresa estrategias empresariales de Colombia bajo la norma ISO 27001 e ISO 31000.* Universidad Nacional abierta y a distancia UNAD. Cali – Colombia. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/35641/pcborreroo.pdf?sequence=3&isAllowed=y

Cabezas, E., Andrade, D., y Torres, J. (2018) *Introducción a la metodología de la*

investigación científica. Recuperado de: http://repositorio.espe.edu.ec/jspui/bitstream/21000/15424/1/Introduccion%20a%20la%20Metodologia%20de%20la%20investigacion%20cientifica.pdf

Carhuancho, I., Nolazco, F., y Monteverde, L, (2019) *Metodología de la investigación holística*, Guayaquil-Ecuador, Departamento de investigación y posgrados UIDE. Recuperado de: https://repositorio.uide.edu.ec/bitstream/37000/3893/3/Metodolog%c3%ada%20para%20la%20investigaci%c3%b3n%20hol%c3%adstica.pdf

Carrillo, C., y Montenegro, A. (2018) La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. (Trabajo de Grado) Universidad Señor de Sipán. Pimentel – Perú. Recuperado de: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/4514/Carrillo%20Diaz%20%26%20Montenegro%20Davila.pdf?sequence=1&isAllowed=y

Caycedo, X. y Arcentales, D. (2017) Auditoría informática. *Un enfoque efectivo*. Cuenca – Azuay. Vol. 3, núm. mon., agos., 2017, pp. 157-173. Recuperado de: file:///C:/Users/ADMIN/Downloads/Dialnet-AuditoriaInformatica-6102836.pdf

Criollo, S. (2017) *"Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo"* (Tesis de Grado) Universidad Técnica de Ambato, Ambato – Ecuador. Recuperado de: http://repositorio.uta.edu.ec/bitstream/123456789/26537/1/Tesis_%20t1318si.pdf

Castellanos, J. (2020) La gestión de la información en el paradigma algorítmico: inteligencia artificial y protección de datos. Métodos de Información, 11(21), 59-82 Recuperado de: https://dialnet.unirioja.es/descarga/articulo/7966054.pdf

Ferruzola, E., Duchimaza, J., Ramos, J., Alejandro, M. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología Magerit. Revista Científica y Tecnológica UPSE, 6(1), 34-41. Recuperado de: https://incyt.upse.edu.ec/ciencia/revistas/index.php/rctu/article/view/429/348

García, C (2016) *Auditoría Informática en la empresa Gomsa Automotriz S.A. de C.V.* (Trabajo de grado) Universidad Tecnológica del Centro de Veracruz, México. Recuperado de: http://reini.utcv.edu.mx/bitstream/123456789/707/1/005833.pdf

Gómez, R, (2017) *La importancia de la implementación de un sistema de gestión de*

seguridad de la información (SGSI) para una institución de seguridad del estado. (Trabajo de Grado). Universidad Piloto de Colombia, Colombia recuperado de: http://35.227.45.16/handle/20.500.12277/2753

GADMT (2021) *Estatuto Orgánico de Gestión Organizacional por procesos gobierno Autónomo Descentralizado "Municipio de Tulcán*". Recuperado de: http://www.gmtulcan.gob.ec/repositorio/2021/administrativo/ESTATUTO%20ORGANICO%202021%20-%20GAD%20TULCAN.pdf

Hernández, R. y Mendoza, C (2018). Metodología de la investigación. *Las rutas cuantitativas, cualitativa y mixta*, Ciudad de México, México: Editorial Mc Graw Hill Education, Año de edición: 2018, ISBN: 978-1-4562-6096-5, 714 p. recuperado de: https://dspace.scz.ucb.edu.bo/dspace/bitstream/123456789/21401/1/11699.pdf

Huayamave, R. (2017) *Implementación de un sistema de gestión de seguridad de la información (SGSI) aplicado a los activos de la empresa constructora Coetecorpza SA, basados en el estándar ISO 27002* (Tesis de Grado) Escuela Superior Politécnica del Litoral, Guayaquil – Ecuador.

Ibarbo, L y Giraldo, V. (2019) *Estado de la norma técnica de seguridad ISO27002 como soporte para la norma ISO27001 en una empresa de telecomunicaciones de la ciudad de Medellín* (Trabajo de Grado). Institución Universitaria, Medellín, Colombia, recuperado de: https://dspace.tdea.edu.co/bitstream/handle/tda/499/Estado%20de%20la%20norma%20tecnica%20de%20seguridad.pdf?sequence=1&isAllowed=y

Kurniawan, E. y Riadi, I., (2018) Security Level Analysis of Academic Information Systems based on standard ISO 27002: 2013, International Journal of Computer Science and Information Security (IJCSIS), Vol. 16, No. 1, January.

Manzaba, G. (2017). *Análisis de riesgos informáticos en el GAD municipal San Francisco de Pueblo viejo* (Trabajo de grado) Universidad de Guayaquil. Ecuador. Recuperado de: http://repositorio.ug.edu.ec/bitstream/redug/27397/1/MANZABA%20GARC%c3%89S%20DAMIAN%20ALEXANDER.pdf

Metodología de la investigación (2018) recuperado de: http://www.essa.ara.mil.ar/cens/MATERIAS%20SEGUNDO%20A%C3%91O/2%C2%B0%20A%C3%91O/08-METODOLOGIA%20DE%20LA%20INVESTIGACION/SEGUNDO%20CUATRIMESTRE/Segundo%20cuatrimestre.pdf

Montenegro, M. (2018) *Validación del procedimiento científico técnico de gestión de riesgos*

tecnológicos en la unidad de desechos sólidos del GAD Ibarra. (Tesis de Grado) Universidad Técnica del Norte. Recuperado de: http://repositorio.utn.edu.ec/bitstream/123456789/8193/1/04%20IND%20122%20TRABAJO%20DE%20GRADO.pdf

Nieves, A. (2017) *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013* (Trabajo de grado) Institución Universitaria Politécnico Grancolombiano. Recuperado de: https://alejandria.poligran.edu.co/bitstream/handle/10823/994/Trabajo%20Final.pdf?sequence=1&isAllowed=y

Niño, N. (2018) *Modelo de un sistema de gestión de seguridad de información – SGSI, para fortalecer la confidencialidad, integridad, disponibilidad y monitorear los activos de información para el instituto nacional de estadística e informática*. (Trabajo de Grado) Universidad Nacional "Pedro Ruiz Gallo". Lambayeque – Perú. Recuperado de: https://repositorio.unprg.edu.pe/bitstream/handle/20.500.12893/5935/BC-TES-TMP-788%20NI%c3%91O%20MORANTE.pdf?sequence=1&isAllowed=y

Ochoa, C (2019) *Diseño y análisis en investigación,* Madrid, International Marketing Comunication. Recuperado de: _https://www.aepap.org/sites/default/files/documento/archivos-adjuntos/artl_2019_libro_diseno_y_analisis_de_investigacion.pdf

Orozco, H. 2017. *Definición y diseño de la investigación.* Universidad Autónoma del Estado de México. Recuperado de: http://ri.uaemex.mx/bitstream/handle/20.500.11799/70901/secme-35486_1.pdf?sequence=1

Otzen, T., Manterola, C. (2017) *Técnicas sobre una población a estudio.* Int J. Morphol 227 -232. Recuperado de: https://scielo.conicyt.cl/pdf/ijmorphol/v35n1/art37.pdf

Padilla, N., y Peña, Y., Rojas, D., (2018) *Diseño de políticas de seguridad informática para la empresa Sotransvega s.a.s* (Trabajo de Grado). Universidad Cooperativa de Colombia, Colombia. Recuperado de: https://repository.ucc.edu.co/bitstream/20.500.12494/14726/2/Dise%c3%b1o%20de%20politicas%20de%20seguridad%20informatica%20para%20la%20empresa%20SOTRANSVEGA%20S.pdf

Paguay, C., y Zamora, G. (2017) Diseño de un sistema de gestión de seguridad de información

bajo la norma ISO 27001:2013 en la E.P.S ASMET salud (Trabajo de Grado) Universidad Nacional Abierta y a Distancia. Timana Huila, Colombia. Recuperado de: http://201.159.222.36/bitstream/123456789/3845/1/PAGUAY%20LEMA%20CINTHYA%20y%20ZAMORA%20ARANA%20GABRIEL.pdf

Peña, R y Lugani, C. (218) *Monitoreo de riesgos de activos de información en la Universidad Nacional de Río Negro*. Universidad Nacional del Río Negro. Recuperado de: http://sedici.unlp.edu.ar/bitstream/handle/10915/89716/Documento_completo.pdf-PDFA.pdf?sequence=1&isAllowed=y

Quiroz, S,. y Macías, D,. (2017) Seguridad en informática: consideraciones, *Dominio de las ciencias, vol.3,* pp 676-688. Recuperado de: file:///C:/Users/Joselin/Downloads/Dialnet-SeguridadEnInformatica-6137824.pdf

Ramos, Y., Urrutia, O., Ordoñez, D., y Bravo, A., (2017) *Adoptar una política de seguridad de la información basados en un dominio del estándar NTC ISO/IEC 27002:2013 para la Cooperativa Codelcauca, AmITIC,* Congreso Internacional AmITIC 2017, Popayán, Colombia. Recuperado de: https://revistas.utp.ac.pa/index.php/memoutp/article/view/1475/2121

Recalde, J (2019). *Plan de implementación de un SGSI y aplicación de controles críticos en el centro de operaciones de seguridad en la empresa GM*S (Tesis de Grado), Escuela Politécnica Nacional, Quito, Ecuador

Reyes, J. (2019) *Diseño de un sistema de gestión de seguridad de información bajo la norma iso27001:2013 en la E.P.S ASMET salud* (trabajo de grado) Universidad abierta y a distancia, Timana Huila, Colombia. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/27057/%20%09jfreyesa.pdf?sequence=1&isAllowed=y

Roberti, B (2020). *Recuperado de: Plan de implementación de un SGSI basado en la norma ISO 27001 en el ámbito de la administración pública en Argentina*. Universidad Oberta Catalunya. http://openaccess.uoc.edu/webapps/o2/bitstream/10609/126647/7/brobertiTFM0121memoria.pdf

Rocha, C. y Recalde, P., (2019). *"Modelo de gestión de seguridad de la información para el sector público"* (Posgrado maestría en telemática) Universidad tecnológica Israel, Quito. Recuperado de: http://repositorio.uisrael.edu.ec/handle/47000/1863

Rodriguez D. , (2017) *Análisis del riesgo de los activos de software sobre la Universidad de*

Cundinamarca 2017-II/2018-I (Trabajo de Grado) Universidad de Cundinamarca, Colombia. Recuperado de: http://repositorio.ucundinamarca.edu.co/bitstream/handle/20.500.12558/1869/FORMATO%20REPOSITORIO.pdf?sequence=1&isAllowed=y

Rodriguez, J,. y Sámchez, D,. (2019) *Sistema de gestión de la seguridad de la Información bajo la norma ISO 27001*. (Trabajo de Grado) Univeridad Laica "Eloy Alfaro", Manta, Ecuador. Recuperado de: https://repositorio.uleam.edu.ec/bitstream/123456789/2061/1/ULEAM-INFOR-0037.pdf

Sanchez, Z,. (2017) *ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA,* (Trabajo de Grado) Universidad Nacional Abierta y a Distancia "UNAD", Colombia. Recuperado de: https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1&isAllowed=y

Sánchez, H., Reyes, C y Mejía, K (2018) *Manual de términos en investigación científica, tecnológica y humanística.* Lima, Perú. ISBN Nº 978-612-47351-4-1 *Recuperado* de: https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion.pdf

Sarmiento, W. (2020). Beneficios de utilizar metodologías para la implantación de Sistemas de Gestión de Seguridad de la Información» Revista PGI. Investigación, Ciencia y Tecnología en Informática, nº 7, pp.104-107. Recuperado de: https://scholar.googleusercontent.com/scholar?q=cache:8D5sZdje6tsJ:scholar.google.com/+beneficios+de+sgsi&hl=es&as_sdt=0,5&as_ylo=2017&as_yhi=2021

Sulca, G. y Becerra, E. (2017) Control interno. Matriz de riesgo: Aplicación metodología COSO II. Revista Publicando, 4 No 12. (2). 2017, 106-125. ISSN 1390-93. Universidad Central del Ecuador, Pontificia Universidad Católica del Ecuador. Recuperado de: https://revistapublicando.org/revista/index.php/crv/article/view/686/pdf_491

Tellez, E. (2018) "Tecnologías, seguridad informática y derechos humanos" Vol.4, nº 1, pp. 19-39 Universidad Nacional Autónoma de México. Recuperado de: https://idus.us.es/bitstream/handle/11441/79462/143-410-PB.pdf?sequence=1&isAllowed=y

Tobón, A. (2018) *Diseño del sistema de gestión de la seguridad de la información (SGSI) para*

la administración municipal del municipio de la ceja Antioquia, bajo los lineamientos emitidos por el programa G.E.L (Trabajo de Grado) Institución Universitaria Politécnico Grancolombiano. Recuperado de: https://alejandria.poligran.edu.co/bitstream/handle/10823/1235/PROYECTO%20FINAL%20DE%20GRADO.PDF?sequence=1&isAllowed=y

Torres, C. (2020) *Plan de seguridad informática basado en la norma ISO 27001, para proteger la información y activos de la empresa privada Megaprofer S.A."* (Trabajo de Grado) Universidad Técnica de Ambato. Recuperado de: http://repositorio.uta.edu.ec/bitstream/123456789/30690/3/Tesis_t1657si.pdf

Troncoso, C., Amaya, A., (2016) Entrevista: Guía para la recolección de datos cualitativos en investigación, Rev.Fac. Med. Vol. 65No. 2: 329-32. Recuperado de: http://www.scielo.org.co/pdf/rfmun/v65n2/0120-0011-rfmun-65-02-329.pdf

Valencia, F., y Orozco, M., (2017) Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000, *Revista Ibérica de Sistemas y Tecnologías.* Núm. 22. Recuperado de: http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952017000200006

V. ANEXOS

Anexo 1: Certificado o Acta del Perfil de Investigación

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FACULTAD DE INDUSTRIAS AGROPECUARIAS Y CIENCIAS AMBIENTALES
CARRERA DE INGENIERIA EN INFORMATICA

ACTA

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

NOMBRE JOSELÍN PAMELA IGUA ÁLVAREZ **CÉDULA DE IDENTID** 0402036032
NIVEL/PARALELO: 0 **PERIODO ACADÉMIC** PAO 2021B

TEMA DEL TIC: Análisis del sistema de gestión de la seguridad de la información y controles de seguridad dela información basada en la ISO/IEC27002 en el municipio de Tulcán

Tribunal designado por la dirección de esta Carrera, conformado por:
PRESIDENTE: MSC. CARLITOS ALBERTO GUANO CÁRDENAS
DOCENTE TUTOR: MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
DOCENTE: MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ

De acuerdo al artículo 32: Una vez entregados los documentos; y, cumplidos los requisitos para la realización de la pre-defensa el Director/a de Carrera designará el Tribunal, fijando lugar, fecha y hora para la realización de este acto:

EDIFICIO DE AULAS 4 **AULA:** 212
FECHA: martes, 15 de febrero de 2022
HORA: 15H00
Obteniendo las siguientes notas:
1) Sustentación de la predefensa: 5.97
2) Trabajo escrito 2.73
Nota final de PRE DEFENSA **8.70**
Por lo tanto: **APRUEBA CON OBSERVACIONES** ; debiendo 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 martes, 15 de febrero de 2022

Firmado digitalmente por CARLITOS ALBERTO GUANO CARDENAS

MSC. CARLITOS ALBERTO GUANO CÁRDENAS
PRESIDENTE

Firmado electrónicamente por: JAIRO VLADIMIR HIDALGO GUIJARRO

MSC. JAIRO VLADIMIR HIDALGO GUIJARRO
DOCENTE TUTOR

Firmado electrónicamente por: MARCO ANTONIO YANDÚN VELASTEGUÍ

MSC. MARCO ANTONIO YANDÚN VELASTEGUÍ
DOCENTE

Adj.: Observaciones y recomendaciones

Anexo 2: Certificado del Abstract por parte de idiomas

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI
FOREIGN AND NATIVE LANGUAGE CENTER

ABSTRACT- EVALUATION SHEET

NAME: Joselin Pamela Igua Alvarez
DATE: 10 de marzo de 2022

TOPIC: "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán"

MARKS AWARDED **Q U A N T I T A T I V E AND Q U A L I T A T I V E**

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: 1,5** ☐	**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**		

1

UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI FOREIGN AND NATIVE LANGUAGE CENTER

Informe sobre el Abstract de Artículo Científico o Investigación.

Autor: Joselin Pamela Igua Alvarez
Fecha de recepción del abstract: 10 de marzo de 2022
Fecha de entrega del informe: 10 de marzo de 2022

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 por lo cual se validad dicho trabajo.

Atentamente

Firmado electrónicamente por:
EDISON BOANERGES PENAFIEL ARCOS

Ing. Edison Peñafiel Arcos MSc
Coordinador del CIDEN

Anexo 3: Informe emitido por Turnitin

"Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán"

INFORME DE ORIGINALIDAD

10%	10%	%	%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

ENCONTRAR COINCIDENCIAS CON TODAS LAS FUENTES (SOLO SE IMPRIMIRÁ LA FUENTE SELECCIONADA)

1%

★ www.mysciencework.com

Fuente de Internet

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Apagado		

Firmado electrónicamente por:
JAIRO VLADIMIR HIDALGO GUIJARRO

Anexo 4 Certificado de Culminación

Gobierno Autónomo Descentralizado
Municipal de Tulcán

Tulcán, 31 de agosto del 2021

Certificado

Por medio del presente y en mi calidad encargado del Departamento del Sistemas del Gobierno Autónomo Descentralizado del cantón Tulcán, me permito Certificar la culminación del proyecto de investigación denominado "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán" mismo que se ha realizado con todo lo solicitado por la Institución y a entra satisfacción del departamento de Sistemas y la Institución en general, en tal sentido me permito agradecer a la estudiante de la carrera de Ingeniería en Informática de la Universidad Politécnica Estatal del Carchi: Joselin Pamela Igua Alvarez con CI 0402036032 por el trabajo realizado en este proyecto alcanzando los objetivos propuestos.

Particular que pongo en su conocimiento, para los fines pertinentes.

Atentamente

Msc. Freed Carrera
Jefe del Departamento de Sistemas

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE TULCAN
JEFATURA DE INFORMATICA

Anexo 5 Aprobación para realizar la investigación en la Institución

Gobierno Autónomo Descentralizado
Municipal de Tulcán

Tulcán, 31 de enero de 2020

Señorita

Joselin Igua

ESTUDIANTE DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA DE LA UNIVERSIDAD POLITÉCNICA ESTATAL DEL CARCHI

Presente. –

Cordial Saludo:

En atención a su oficio de fecha 15 de enero de 2020 sumillado al Departamento de Sistemas desde la Alcaldía de Tulcán con Reg.No. 6256, me permito informarle que se Autoriza su pedido, para realizar la tesis con el tema "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán".

Particular que me permito poner en su conocimiento, para los fines consiguientes.

Atentamente,

"Tulcán, para la Vida"

Ing. Oscar Freed Carrera

GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DE TULCAN
JEFATURA DE INFORMATICA

Anexo 6 Solicitud de entrevista

Tulcán, 05 de mayo de 2021

Msc.

Freed Carrera

Presente. -

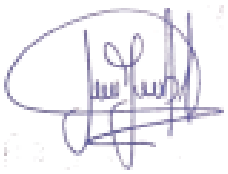
De mi consideración:

Reciba un atento y cordial saludo de quien conforma el informe de investigación con el tema: "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán", a la vez que le deseándole éxitos en las funciones que usted desempeña.

Yo, Joselin Pamela Igua Alvarez con el número de cédula 0402036032 estudiante de la carrera de Ingeniería en Informática, por medio de este presente solicito de la manera más comedida una entrevista de carácter presencial para recolección de información de la investigación previo al análisis requerido.

En espera de una favorable acogida al presente, anticipo mi más sincero agradecimiento.

Atentamente,



Srta, Joselin Igua

ESTUDIANTE DE LA CARRERA DE COMPUTACIÓN

INGENIERÍA EN INFORMÁTICA

Anexo 7 Entrevistas

Entrevistado: Jefe del área de sistemas

Msc. Freed Carrera

Teniendo en cuenta que ISO/IEC 27002 es un estándar internacional encargado de la seguridad de la información, siendo estos los activos más significativos dentro de las instituciones ya sea hardware, software e información confidencial.

Preguntas:

1. ¿Cuál es el estándar que se utiliza para la protección de activos informáticos?
2. Independientemente de la normativa de la institución ¿Cuáles son los controles establecidos para la gestión de la seguridad de la información y quienes son los responsables de verificar el cumplimiento?
3. ¿Cómo es el procedimiento para resguardar la información mediante normativas de seguridad?
4. Describa las funciones que tiene el personal encargado de la seguridad de la información lógica y física dentro del departamento de tecnología de la información.
5. ¿Cómo son controladas las normativas para la gestión de la información?
6. ¿Cuáles son las funciones del encargado de la seguridad de la información?
   ¿Se encuentra clasificada la información en privada, publica, confidencia y critica?
7. ¿Cómo se accede a los diferentes sistemas informáticos?
8. De acuerdo a la última auditoria ¿cuál fue el porcentaje de conformidad o inconformidad y cuáles son los aspectos más débiles dentro de la seguridad informática.?
9. ¿Qué medidas se toman en caso de fallas en la disponibilidad de la información?
10. ¿Cómo es el proceso para acceder la data center?
11. ¿Cuál es el procedimiento para que los proveedores accedan a los sistemas informáticos?
12. ¿Cómo se realiza la gestión de usuarios?
13. ¿Con qué frecuencia se realizan copias de seguridad, y se realiza una verificación posterior?
14. ¿Se realizan reportes de cumplimiento de funciones?
15. ¿Existen planes estratégicos en áreas específicas?
16. ¿Los manuales de usuario son verificados por funcionarios públicos de altos cargos?
17. ¿El personal del área de sistemas cuenta con activos a su cargo o responsabilidad?
18. ¿Existe documentación que respalde la evidencia de las actividades y responsabilidades?
19. ¿La información de alto riesgo cuenta con sistemas de cifrado?
20. ¿Se hace uso de firmas electrónicas como protección y verificación de información?

21. ¿Se hace uso de firmas electrónicas como protección y verificación de información?
22. ¿La seguridad de claves de acceso es custodiada por terceros?
23. ¿Cuentan con prestación de equipos para áreas distintas de la institución?
24. ¿Cuentan con sistemas de detección de intrusos?
25. ¿Cada qué tiempo se realiza monitoreo de red?
26. ¿Existen bloqueo de puertos para los funcionarios de todas las áreas?

Anexo 8 Solicitud de Verificación de Cumplimiento

Tulcán, 17 de agosto de 2021

Msc.
Freed Carrera
Presente. -

De mi consideración:
Reciba un atento y cordial saludo de quien conforma el informe de investigación con el tema: "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán", a la vez que le deseándole éxitos en las funciones que usted desempeña.

Yo, Joselin Pamela Igua Alvarez con el número de cédula 0402036032 estudiante de la carrera de Ingenieria en Informática, por medio de este presente solicito de la manera más comedida la verificación y cumplimiento de controles en base a la normativa ISO 27002 de carácter presencial para la realización del informe final de estrategias de mitigación de la investigación previo al análisis requerido.

En espera de una favorable acogida al presente, anticipo mi más sincero agradecimiento.

Atentamente,

Srta, Joselin Igua

ESTUDIANTE DE LA CARRERA DE COMPUTACIÓN
INGENIERÍA EN INFORMÁTICA

Anexo 9 Oficio Entrega del Informe Ejecutivo

Tulcán, 30 de agosto gosto de 2021

Msc.
Freed Carrera
Presente. -

De mi consideración:

Reciba un atento y cordial saludo de quien conforma el informe de investigación con el tema: "Análisis del sistema de gestión de la seguridad de la información y controles de seguridad de la información basada en la ISO/IEC 27002 en el municipio de Tulcán", a la vez que le deseándole éxitos en las funciones que usted desempeña.

Yo, Joselin Pamela Igua Alvarez con el número de cédula 0402036032 estudiante de la carrera de Ingeniería en Informática, por medio de este presente realizo la entrega formal del INFORME EJECUTIVO, resultado del análisis de investigación buscando evaluar el estado de procesos tecnológicos emitidos en el Departamento de Sistemas; y solicito comedidamente el documento de conformidad de finalización al realizar mi proyecto de titulación.

- Adjunto Informe Ejecutivo de manera físico y virtual

En espera de una favorable acogida al presente, anticipo mi más sincero agradecimiento.

Atentamente,

Srta. Joselin Igua

ESTUDIANTE DE LA CARRERA DE INGENIERÍA EN INFORMÁTICA

Anexo 10 Informe ejecutivo

"ANÁLISIS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN Y CONTROLES EN BASE A LA NORMA ISO/IEC 27002 EN EL GAD MUNICIPAL DEL TULCÁN"

DEPARTAMENTO DE SISTEMAS

INFORMACIÓN GENERAL

Jefe del Departamento de Sistemas	Msc. Fred Carrera
Tesista Auditora	Joselin Igua
Lugar	Tulcán (Departamento de Sistemas)
Fecha del Informe	

RESUMEN EJECUTIVO

En el departamento de Sistemas, ejerciendo sus actividades se realizó una evaluación independiente en cuestión al Sistema de Información de Gestión de la Seguridad de la Información.

La valoración para el análisis se efectuó basados en la normativa ISO/IEC 27002:2013 anexo A, la estimación del cumplimiento de controles de implementación relacionadas a:

- Políticas de seguridad de la Información
- Control de Acceso
- Seguridad Ligada a Recursos Humanos
- Gestión de Activos
- Cifrado
- Seguridad Física y Ambiental
- Seguridad en la Operativa

- Seguridad en las Telecomunicaciones
- Adquisición Desarrollo y Mantenimiento
- Relaciones con Suministros
- Gestión de Incidentes de Seguridad de la Información
- Aspectos en la Gestión de la Continuidad de Negocio
- Cumplimiento.

Se identificaron 25 observaciones con posibles riesgos a los cuales se les atribuye oportunidades de mejora.

INFORME EJECUTIVO

OBJETIVO

Analizar los controles y procesos internos en el área de sistemas del GAD Municipal de Tulcán, con el fin de evaluar el cumplimiento de normativa e identificar riesgos y el impacto que puede provocar en la institución.

ALCANCE

El alcance del análisis se enfoca en la norma internacional ISO/IEC 27002 un estándar de seguridad de la información, que permite controlar y evaluar procesos, para así proceder a ejecutar estrategias de mitigación para la mejora continua de procesos eficientes y seguros en un área específica.

FUNDAMENTOS DEL ANÁLISIS

Considerando el acuerdo ministerial N° 025-2019

El Ministerio de Telecomunicaciones y de la sociedad de la información acuerda:

Art 1. Expedir el Esquema Gubernamental de Seguridad de la Información – ESGSI-, el cual es de implementación obligatoria en las Instituciones de Administración Pública Central, Institucional y que dependen de la Función Ejecutiva.

Art 2. Recomendar a las Instituciones de Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, realizaran la Evaluación de Riesgos sobre sus activos de información críticos y diseñaran el plan para el tratamiento de riesgos de su Institución.

Art 3. Recomendar a las Instituciones de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva, utilicen como guía la norma técnica ISO/IEC 27000 para la Gestión de Seguridad de la Información.

RESULTADOS

Verificación de controles

Dominios	Objetivos de Control	Controles	Descripción	SI	NO	No aplica
	1	*2*	POLÍTICAS DE SEGURIDAD			
5		**2**	**Directrices de la Dirección en seguridad de la información.**			
	5.1		Conjunto de políticas para la seguridad de la información		✓	
		5.1.2	Revisión de las políticas para la seguridad de la información.		✓	
	2	*7*	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
		5	**Organización Interna**			
		6.1.1	Asignación de responsabilidades para la segur. de la información		✓	
6	**6.1**	6.1.2	Segregación de tareas.	✓		
		6.1.3	Contacto con las autoridades.		✓	
		6.1.4	Contacto con grupos de interés especial.		✓	
		6.1.5	Seguridad de la información en la gestión de proyectos.		✓	
		2	**Dispositivos para movilidad y teletrabajo.**			
	6.2	6.2.1	Política de uso de dispositivos para movilidad.			✓
		6.2.2	Teletrabajo.		✓	
	3	*5*	SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.			
		2	**Antes de la contratación.**			
	7.1	7.1.1	Investigación de antecedentes.	✓		
7		7.1.2	Términos y condiciones de contratación	✓		
		2	**Durante la contratación**			
	7.2	7.2.1	Responsabilidad de gestión		✓	
		7.2.2	Concienciación, educación y capacitación en segur. de la informac.		✓	
		7.2.3	Proceso disciplinario.		✓	
	7.3	***1***	**Cese o cambio de puesto de trabajo.**			
		7.3.1	Cese o cambio de puesto de trabajo.	✓		
	3	10	GESTIÓN DE ACTIVOS			
		4	**Responsabilidad sobre los activos.**			
		8.1.1	Inventario de activos.	✓		
	8.1	8.1.2	Propiedad de los activos.	✓		
		8.1.3	Uso aceptable de los activos	✓		
		8.1.4	Devolución de activos	✓		
8		**3**	**Clasificación de la información.**			
		8.2.1	Directrices de clasificación.		✓	
		8.2.2	Etiquetado y manipulado de la información.		✓	
	8.2	8.2.3	Manipulación de activos		✓	
		3	**Manejo de los soportes de almacenamiento**			
	8.3	8.3.1	Gestión de soportes extraíbles.	✓		
		8.3.2	Eliminación de soportes	✓		
		8.3.3	Soportes físicos en tránsito.			✓

9	*4*	14	CONTROL DE ACCESOS.			
	9.1	***2***	**Requisitos de negocio para el control de accesos.**			
		9.1.1	Política de control de accesos.		✓	
		9.1.2	Control de acceso a las redes y servicios asociados.		✓	
	9.2	***6***	**Gestión de acceso de usuario.**			
		9.2.1	Gestión de altas/bajas en el registro de usuarios.	✓		
		9.2.2	Gestión de los derechos de acceso asignados a usuarios.	✓		
		9.2.3	Gestión de los derechos de acceso con privilegios especiales.	✓		
		9.2.4	Gestión de información confidencial de autenticación de usuarios	✓		
		9.2.5	Revisión de los derechos de acceso de los usuarios.		✓	
		9.2.6	Retirada o adaptación de los derechos de acceso	✓		
	9.3	***1***	**Responsabilidades del usuario**			
		9.3.1	Uso de información confidencial para la autenticación.		✓	
	9.4	***5***	**Control de acceso a sistemas y aplicaciones.**			
		9.4.1	Restricción del acceso a la información.		✓	
		9.4.2	Procedimientos seguros de inicio de sesión	✓		
		9.4.3	Gestión de contraseñas de usuario.	✓		
		9.4.4	Uso de herramientas de administración de sistemas.		✓	
		9.4.5	Control de acceso al código fuente de los programas.		✓	
10	*1*	*2*	CIFRADO.			
	10.1	***2***	**Controles criptográficos**			
		10.1.1	Política de uso de los controles criptográficos.		✓	
		10.1.2	Gestión de claves.		✓	
11	*2*	15	SEGURIDAD FÍSICA Y AMBIENTAL.			
	11.1	***6***	**Áreas seguras.**			
		11.1.1	Perímetro de seguridad física.		✓	
		11.1.2	Controles físicos de entrada.		✓	
		11.1.3	Seguridad de oficinas, despachos y recursos		✓	
		11.1.4	Protección contra las amenazas externas y ambientales.		✓	
		11.1.5	El trabajo en áreas seguras.		✓	
		11.1.6	Áreas de acceso público, carga y descarga.			✓
	11.2	***9***	**Seguridad de los equipos.**			
		11.2.1	Emplazamiento y protección de equipos.		✓	
		11.2.2	Instalaciones de suministro.		✓	
		11.2.3	Seguridad del cableado.		✓	
		11.2.4	Mantenimiento de los equipos.		✓	
		11.2.5	Salida de activos fuera de las dependencias de la empresa.			✓
		11.2.6	Seguridad de los equipos y activos fuera de las instalaciones			✓
		11.2.7	Reutilización o retirada segura de dispositivos de almacenamiento.	✓		
		11.2.8	Equipo informático de usuario desatendido	✓		
		11.2.9	Política de puesto de trabajo despejado y bloqueo de pantalla.	✓		

12	*7*	14	SEGURIDAD EN LA OPERATIVA.		
	12.1	***4***	**Responsabilidades y procedimientos de operación.**		
		12.1.1	Documentación de procedimientos de operación.		✓
		12.1.2	Gestión de cambios.		✓
		12.1.3	Gestión de capacidades.		✓
		12.1.4	Separación de entornos de desarrollo, prueba y producción.	✓	
	12.2	*1*	**Protección contra código malicioso.**		
		12.2.1	Controles contra el código malicioso.		✓
	12.3	*1*	**Copias de seguridad.**		
		12.3.1	Copias de seguridad de la información.		✓
	12.4	*4*	**Registro de actividad y supervisión.**		
		12.4.1	Registro y gestión de eventos de actividad.	✓	
		12.4.2	Protección de los registros de información.		✓
		12.4.3	Registros de actividad del administrador y operador del sistema.	✓	
		12.4.4	Sincronización de relojes.	✓	
	12.5	*1*	**Control del software en explotación.**		
		12.5.1	Instalación del software en sistemas en producción.	✓	
	12.6	*2*	**Gestión de la vulnerabilidad técnica.**		
		12.6.1	Gestión de las vulnerabilidades técnicas.		✓
		12.6.2	Restricciones en la instalación de software.	✓	
	12.7	*1*	**Consideraciones de las auditorías de los sistemas de información.**		
		12.7.1	Controles de auditoría de los sistemas de información.		✓
13	2	*7*	SEGURIDAD EN LAS TELECOMUNICACIONES.		
	13.1	*3*	**Gestión de la seguridad en las redes**		
		13.1.1	Controles de red.		✓
		13.1.2	Mecanismos de seguridad asociados a servicios en red.		✓
		13.1.3	Segregación de redes.		✓
	13.2	*4*	**Intercambio de información con partes externas.**		
		13.2.1	Políticas y procedimientos de intercambio de información.		✓
		13.2.2	Acuerdos de intercambio.	✓	
		13.2.3	Mensajería electrónica.	✓	
		13.2.4	Acuerdos de confidencialidad y secreto.		✓
14	*3*	*13*	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		
	14.1	***3***	**Requisitos de seguridad de los sistemas de información.**		
		14.1.1	Análisis y especificación de los requisitos de seguridad.		✓
		14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.		✓
		14.1.3	Protección de las transacciones por redes telemáticas.		✓
	14.2	*9*	**Seguridad en los procesos de desarrollo y soporte.**		
		14.2.1	Política de desarrollo seguro de software.	✓	
		14.2.2	Procedimientos de control de cambios en los sistemas.	✓	
		14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	✓	
		14.2.4	Restricciones a los cambios en los paquetes de software.		✓
		14.2.5	Uso de principios de ingeniería en protección de sistemas.	✓	
		14.2.6	Seguridad en entornos de desarrollo.	✓	
		14.2.7	Externalización del desarrollo de software.	✓	
		14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	✓	
		14.2.9	Pruebas de aceptación.	✓	
	14.3	***1***	**Datos de prueba.**		
		14.3.1	Protección de los datos utilizados en pruebas.	✓	

15	*2*	*5*	RELACIONES CON SUMINISTRADORES.			
	15.1	*3*	**Seguridad de la información en las relaciones con suministradores.**			
		15.1.1	Política de seguridad de la información para suministradores		✓	
		15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.		✓	
		15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.		✓	
	15.2	*2*	**Gestión de la prestación del servicio por suministradores.**			
		15.2.1	Supervisión y revisión de los servicios prestados por terceros.		✓	
		15.2.2	Gestión de cambios en los servicios prestados por terceros.		✓	
16	1	*7*	GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.			
	16.1	*7*	**Gestión de incidentes de seguridad de la información y mejoras**			
		16.1.1	Responsabilidades y procedimientos.		✓	
		16.1.2	Notificación de los eventos de seguridad de la información.		✓	
		16.1.3	Notificación de puntos débiles de la seguridad.		✓	
		16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.		✓	
		16.1.5	Respuesta a los incidentes de seguridad.		✓	
		16.1.6	Aprendizaje de los incidentes de seguridad de la información.	✓		
		16.1.7	Recopilación de evidencias.	✓		
17	*2*	*4*	ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.			
	17.1	*3*	**Continuidad de la seguridad de la información.**			
		17.1.1	Planificación de la continuidad de la seguridad de la información.		✓	
		17.1.2	Implantación de la continuidad de la seguridad de la información.		✓	
		17.1.3	información.		✓	
	17.2	*1*	**Redundancias.**			
		17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	✓		
18	*2*	*8*	CUMPLIMIENTO.			
	18.1	*5*	**Cumplimiento de los requisitos legales y contractuales.**			
		18.1.1	Identificación de la legislación aplicable.		✓	
		18.1.2	Derechos de propiedad intelectual (DPI).		✓	
		18.1.3	Protección de los registros de la organización.		✓	
		18.1.4	Protección de datos y privacidad de la información personal	✓		
		18.1.5	Regulación de los controles criptográficos.		✓	
	18.2	*3*	**Revisiones de la seguridad de la información.**			
		18.2.1	Revisión independiente de la seguridad de la información.		✓	
		18.2.2	Cumplimiento de las políticas y normas de seguridad.		✓	
		18.2.3	Comprobación del cumplimiento.		✓	

Figura 1 Cumplimiento de controles
Fuente: Elaboración propia

El porcentaje determinado por los 14 dominios es el resultado equivalente a la verificación del cumplimiento total de 114 controles en el área de sistemas.

Tabla 1 Porcentaje de cumplimiento

Dominio	Descripción	Porcentaje de cumplimiento
5	Políticas de seguridad	0%
6	Aspectos organizativos de la seguridad de la información	16.66%
7	Seguridad ligada a los recursos humanos.	50%
8	Gestión de activos	66.66 %
9	Control de accesos.	50%
10	Cifrado.	0%
11	Seguridad física y ambiental.	25%
12	Seguridad en la operativa.	42.85%
13	Seguridad en las telecomunicaciones.	28.57%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	69.23%
15	Relaciones con suministradores.	0%
16	Gestión de incidentes en la seguridad de la información.	28.57%
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	25%
18	Cumplimiento.	14.28%

El nivel de cumplimiento de los dominios en su estado actual no se establece en un rango ideal para priorizar la seguridad de la información, por lo tanto, existen diversas fuentes de debilidades a solucionar dentro de las actividades en el área de sistemas que son indispensables para lograr mejoras significativas y contribuir con el rendimiento necesario dentro de la institución.

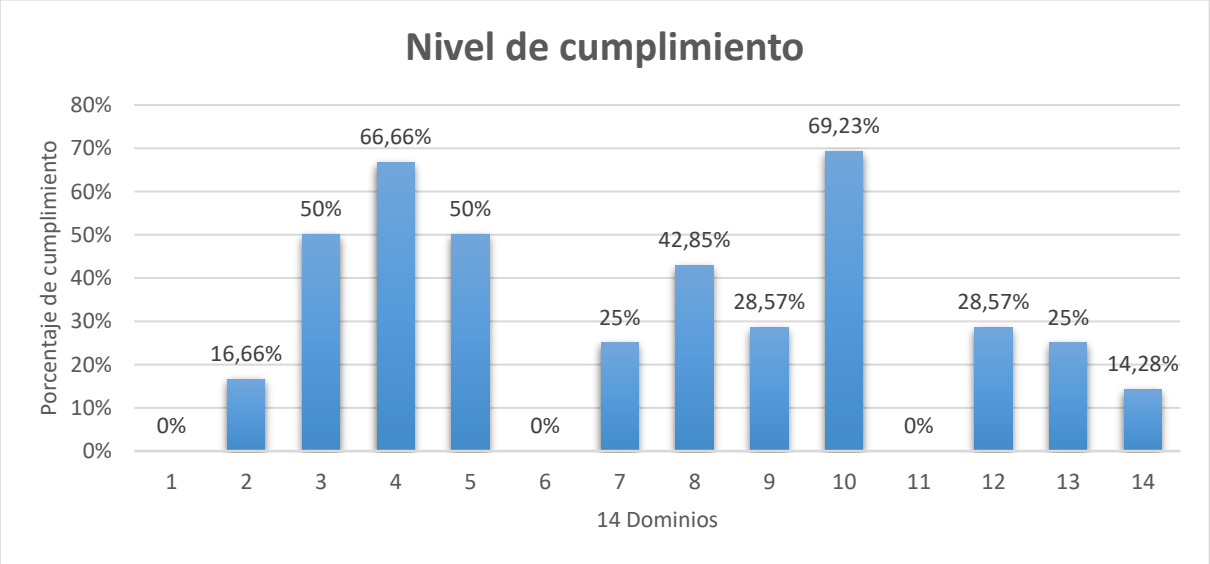


Figura 2 Porcentaje de cumplimiento actual

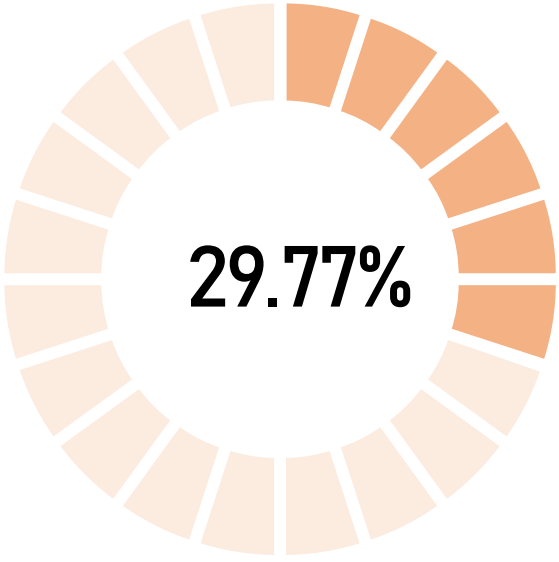


Figura 3 Porcentaje total del cumplimiento actual

Se puede determinar el porcentaje total del cumplimiento que actualmente está establecido, tomando en cuenta la verificación de los controles de seguridad de la información mediante la normativa analizada en la investigación, por lo tanto, al interpretar su bajo rendimiento se logra identificar falencias para así definir estrategias según los requerimientos detectados.

Tabla 2 Incremento de cumplimiento en implementación de controles

Dominio	Descripción	Porcentaje de cumplimiento	Porcentaje implementado
5	Políticas de seguridad	0%	60%
6	Aspectos organizativos de la seguridad de la información	16.66%	60%
7	Seguridad ligada a los recursos humanos.	50%	86%
8	Gestión de activos	66.66 %	66.66%
9	Control de accesos.	50%	72.85%
10	Cifrado.	0%	50%
11	Seguridad física y ambiental.	25%	61.66%
12	Seguridad en la operativa.	42.85%	65.71%
13	Seguridad en las telecomunicaciones.	28.57%	60%
14	Adquisición, desarrollo y mantenimiento de los sistemas de información.	69.23%	70.76%
15	Relaciones con suministradores.	0%	44%
16	Gestión de incidentes en la seguridad de la información.	28.57%	68.57%
17	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.	25%	50%
18	Cumplimiento.	14.28%	57.5%

Fuente: elaboración propia

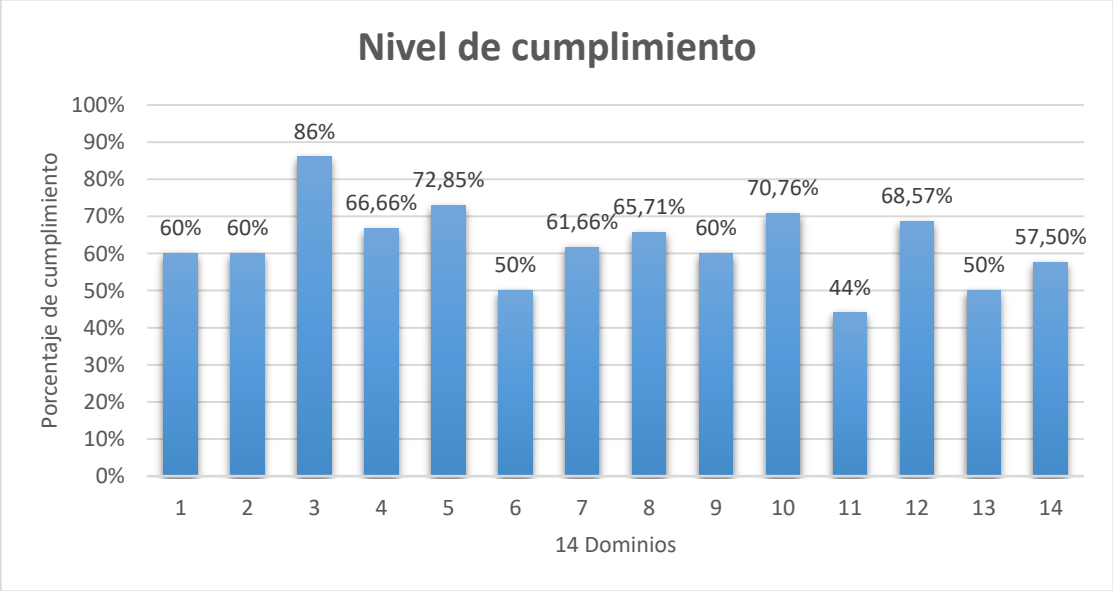


Figura 4 Porcentaje de cumplimiento en una posible implementación

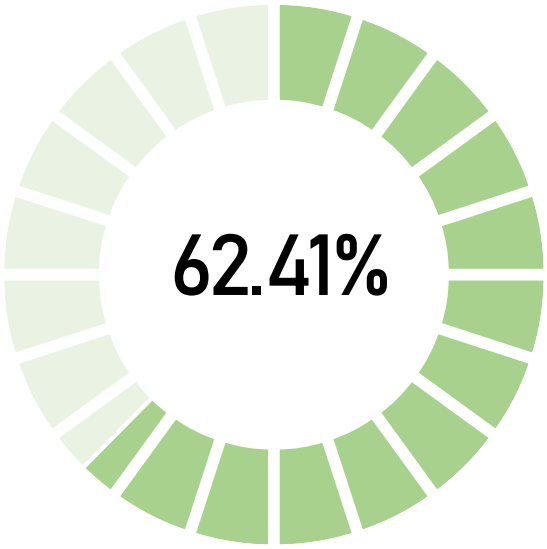


Figura 5 Porcentaje total del incremento de cumplimiento implementado

El incremento de seguridad de la información que se estima lograr al proponer la implementación alcanza un porcentaje óptimo, ayudando a reducir considerablemente los posibles riesgos asociados con las vulnerabilidades encontradas en la investigación, de modo que, las buenas prácticas y la mejora continua prevalece al ejecutar los controles que están vinculados a los requisitos de las instituciones.

De acuerdo al ministerio de Telecomunicaciones y de la Sociedad de la Información menciona que el Esquema Gubernamental de Seguridad de la Información tiene como objetivo preservar la confidencialidad, integridad y disponibilidad de la información, por lo tanto, se establecen diversas normativas que para el cumplimiento total garantizando reducción de riesgos, revisiones continuas, continuidad de servicios, entre otros.

En base al análisis realizado mediante la normativa ISO/IEC 27002 se logra el 62.41% de cumplimiento dentro de los 114 controles que abarca el estándar, de modo que, al ser una institución gubernamental es necesario complementar el EGSI que contribuye con el porcentaje restante a la investigación como la ISO 27005 Gestión de Riesgos.

DETERMINACIÓN DE RIESGOS

Los riesgos son mecanismos que pueden ser valorados para dar solución, debido a que estos se vinculan directamente con la vulnerabilidad y amenazas a los activos mediante distintos procesos, es por eso que el análisis de riesgo es fundamental para una buena operatividad.

Riesgos externos

Los riesgos externos provocan daños de fuerza mayor convirtiéndose en grandes amenazas, es por eso que se debe definir ciertas estrategias para actuar en forma adecuada ante algún incidente, podemos mencionar ciertos riesgos que se han adecuado a las amenazas que en la institución efectuarse.

Tabla 3 Riesgos externos

Riesgos Externos				
N°	Riesgos	Probabilidad	Impacto	Prioridad
R1	Incendio en el área de sistemas	2	4	8
R2	Sismo	3	4	12
R3	Robo de equipos	2	4	8
R4	Daños por vandalismo	2	4	8

Podemos determinar que los riesgos provenientes de un entorno externo logran condicionar directa o indirecta un alto impacto sobre los que la institución no tiene control.

La institución debe establecer los análisis necesarios para la reducción de catástrofes, sobre las que no se puede ejercer ningún control, mejorando así la adaptación a cambios requeridos teniendo la capacidad de afrontarlos.

Riesgos internos

Los riesgos internos aparecen directamente de la gestión de la organización y sus procedimientos afectando a todas sus áreas sin distinción, por ende, realizar planes de mitigación con el fin de verificar su cumplimiento para evitar incidentes que están en constante control de la institución.

Se considera principalmente 25 situaciones de riesgo que se presentan en el análisis realizado basado en los controles de la norma ISO/IEC 27002 en el área de tecnología, se puede demostrar el nivel de impacto que podría provocar el incumplimiento de controles.

Tabla 4 Riesgos Internos

Determinando los riesgos correspondientes de manera interna basados en la norma internacional ISO/IEC 27002 se puede verificar su prioridad en una matriz de riesgos

Riesgos internos				
N°	Riesgos	Probabilidad	Impacto	Prioridad
R1	Escasa aplicación de políticas de seguridad	3	4	12
R2	Personal insuficiente	4	4	16
R3	No se aplica un plan de capacitación sobre seguridad de la información	3	3	9
R4	Información sin categorizar	2	4	8
R5	Escasos requisitos de control de accesos	3	4	12
R6	Manejo inadecuado de datos de críticos	3	4	12
R7	Deficiente restricción de acceso físico	3	4	12
R8	Robo de equipos	2	4	8
R9	Fallas eléctricas	3	3	9
R10	Inexistencias de planes de contingencia	3	4	12
R11	Red cableada expuesta y con deterioro	3	4	12

R12	Inadecuado mantenimiento de equipos	3	3	9
R13	Sistemas de climatización y conductos de ventilación mal estructurado	3	3	9
R14	Software malicioso	3	4	12
R15	Inadecuado respaldo de información	3	4	12
R16	Restricciones de software sin implementar	3	4	12
R17	Infraestructura sin segmentación de red apropiada	2	4	8
R18	Intrusión de red	3	4	12
R19	Caída de sistemas de comunicación	3	4	12
R20	Inexistencia de acuerdos de confidencialidad	4	3	12
R21	Limitados requisitos de seguridad de comunicaciones	4	3	12
R22	Insuficientes controles para servicios de suministradores	3	4	12
R23	Inadecuado control de la gestión de eventos	3	3	9
R24	Inexistencia de plan de continuidad de negocio	3	3	9
R25	Escasos requisitos legales sobre la seguridad de la inf.	3	4	12

Tabla 5 Probabilidad - Impacto

			Impacto			
			Insignificante	Baja	Mediana	Alto
			1	2	3	4
bbbbbbProbab	Improbable	4			2	1
	Poco probable	3			6	14
	Ocasional	2				6
	Probable	1				

Fuente: Elaboración propia

Mediante la matriz de calor se determina el alcance de los riesgos encontrados con mayor probabilidad e impacto, lo cual permite brindar prioridad por los daños que puede causar si no

se logra rectificar las acciones de procedimientos establecidos, por lo tanto, toda acción no verificada correctamente produce ciertos incidentes dentro de la institución.

CONTROLES CON NO CONFORMIDAD Y HALLAZGO DE RIESGOS

De acuerdo a la normativa ISO 27002 los controles establecidos presentan falencias de seguridad de la información, por ende, se aplican estrategias de mitigación y representación de riesgos para establecer el impacto que genera el no implementar normativa correspondiente.

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

ESCASA APLICACIÓN DEL POLÍTICAS DE SEGURIDAD			
R1	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Establecer políticas específicas relacionada con la constitución y normativas legales enfocadas en nivel operativo, tecnológico, entre otros.
- Definir la implementación del Sistema de Gestión de la Seguridad de la Información.
- Realizar una auditoría de seguridad de la información para determinar normas aplicables para la implementación de controles.
- Revisión de las políticas de seguridad de la información de manera regular.
- Mantener su registro de revisiones y acciones correctivas supervisadas por dirección.
- Controlar que la planificación de controles sea realizada por personal autorizado y competente o bajo supervisión de funcionarios de área de sistemas como también de expertos contratados para ese propósito.
- Socializar las políticas probadas por dirección a todos los funcionarios.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	
6.1	*Organización Interna*
6.1.1	Asignación de responsabilidades para la seguridad de la información
6.1.2	Segregación de tareas.
6.1.4	Contacto con grupos de interés especial.
6.1.5	Seguridad de la información en la gestión de proyectos.
6.2	*Dispositivos para movilidad y teletrabajo*
6.2.2	Teletrabajo.

PERSONAL INSUFICIENTE

R2	**Prioridad** 16	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto

Estrategias de Mitigación

- Contratar personal capacitado en temas de seguridad de la información responsable de procesos de control.
- Establecer en el manual de funciones responsabilidades de Oficial de seguridad para determinar el resguardo de la información y varias acciones dentro del control establecido.
- Instruir al oficial de sistemas siendo de emitir reportes de las áreas afectadas y su impacto por incidentes.
- Establecer un encargado de definir controles preventivos eliminando o mitigando vulnerabilidades de sistemas o servicios detectando debilidades recurrentes.
- Asegurar los lineamientos para el uso de recursos de las TI contemplando los requerimientos sobre seguridad de la información según su criticidad.
- Gestionar actividades de manera periódica para garantizar de manera oportuna y adecuada la seguridad de la información.
- Definir el responsable de documentar los controles necesarios para la detección y protección de los servicios de la institución.

- Establecer contactos con grupos de interés especiales manteniendo así la competitividad y actualización requerida por la seguridad de la información.
- Verificar el cumplimiento de la normativa mediante responsabilidades generando informes técnicos indistintamente de las acciones realizadas.
- Asignar responsabilidades para el desarrollo de proyectos y controles de seguridad de la información reduciendo vulnerabilidades.
- Definir estrategias de implementación que brinde seguridad de la información que se accede mediante teletrabajo.
- Realizar el registro de dispositivos incluyendo conexiones remotas y restricciones.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	
7.2	*Durante la contratación*
7.2.1	Responsabilidad de gestión
7.2.2	Concienciación, educación y capacitación en segur. de la información
7.2.3	Proceso disciplinario.

NO SE APLICA UN PLAN DE CAPACITACIÓN SOBRE SEGURIDAD DE LA INFORMACIÓN

R3	**Prioridad** 9	**Tipo de riesgo**	Medio Media probabilidad – medio impacto

Estrategias de Mitigación

- Concientizar la necesidad de adquirir conocimiento de la seguridad de la información durante la contratación.
- Acordar condiciones laborales apropiadas a sus funciones y responsabilidades incluyendo las métricas de seguridad de la información de la institución.

  -Encargado de administración de servidores, respaldos de información, almacenamiento, redes de datos, base de datos, aplicación de negocios, recursos informáticos, entre otros.

  -Líderes de proyecto, personal de capacitación, programadores, documentación de entornos para desarrollo, pruebas, capacitación y producción.

- Socializar de manera oportuna sobre las responsabilidades legales dentro de los procedimientos para la seguridad.
  - Considerando sanciones dependiendo cantidad y gravedad de violación e impacto.
- Se capacita mencionando controles y procesos implementados en la institución a todo el personal.
  - Nivel de capacitación, Ley de Comercio Electrónico, Firmas Electrónicas, SGSI y otros factores propios de la entidad.
- Dar a conocer el uso correcto de recursos o servicios de la información.
  - Aplicativos de servicios informáticos, soporte, reportes físicos y electrónicos, documentación de capacitaciones y evaluaciones.
- Establecer procesos de seguridad como: gestión de activos, uso de contraseñas seguras, limpieza de escritorios, entre otros.

8. GESTIÓN DE ACTIVOS	
8.2	*Clasificación de la información.*
8.2.1	Directrices de clasificación.
8.2.2	Etiquetado y manipulado de la información.
8.2.3	Manipulación de activos.

INFORMACIÓN SIN CATEGORIZAR

R4	**Priorida**d 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Estrategias de Mitigación

- Definir al personal adecuado responsable de supervisar el cumplimiento del proceso de generación de rotulación de activos.
- Clasificar en pública o confidencial la información.
- Elaborar un listado aprobado para la clasificación de la información considerando la normativa establecida.

- Categorizar la información basada en requisitos legales, sensibilidad e importancia hacia la institución.
- Su clasificación dependerá del nivel de protección valorando la confidencialidad, integridad y disponibilidad.
- Establecer un sistema de etiquetas en caso de formatos electrónicos se debe asociar un metadato único.
- Generar etiquetas de acuerdo al tipo de activos y a la funcionalidad, en caso de repetirse se deberá añadir un número secuencial.

  – En etiquetas físicas el personal responsable deberá verificar que sean legibles y se encuentre rotulado en un periodo de 6 meses aproximadamente.
- Establecer un inventario de los activos en caso de destrucción, para mantener un registro de las acciones realizadas asociadas a sus respectivas etiquetas.
- Generar código MD5 en caso de mantener documentos en formato electrónico.

9. CONTROL DE ACCESOS.	
9.1	*Requisitos de negocio para el control de accesos.*
9.1.1	Política de control de accesos.
9.1.1	Control de acceso a las redes y servicios asociados.
9.2	*Gestión de acceso de usuario.*
9.2.5	Revisión de los derechos de acceso de los usuarios.
9.3	*Responsabilidades del usuario*
9.3.1	Uso de información confidencial para la autenticación.
9.4	*Control de acceso a sistemas y aplicaciones.*
9.4.1	Restricción del acceso a la información.

ESCASOS REQUISITOS DE CONTROL DE ACCESOS			
R5	**Prioridad** 12	**Tipo de riesgo**	Alto Media probabilidad – alto impacto
Estrategias de Mitigación			

- Establecer políticas de control de acceso para gestionar la autorización a los usuarios previniendo acciones no autorizadas.
- Definir el responsable encargado de otorgar el acceso de la información asignando la menor cantidad de privilegios y el tiempo determinado para el desarrollo.
- Depurar usuarios en un período aproximado de 30 días, en caso de cambios la gestión se la realizara de inmediato.
- Establecer la disponibilidad de acceso en los archivos log de los sistemas en el momento que sean requeridos.
- Retirar privilegios al acceso de información de manera inmediata al comunicar la terminación laboral socializando con el responsable de la seguridad de la información.
- Exigir a los usuarios la prioridad correspondiente a la autenticación y su confidencialidad.
- Definir políticas para el control que prohíba todos los accesos en funciones de sistemas o servicios y se permitan realizar acciones determinadas y autorizadas.
- Establecer derechos de accesos de lectura, eliminación y ejecución a usuarios que realizan procesos de la información.
- Realizar revisiones periódicas garantizando que la información se envíe únicamente en terminales autorizados.

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

MANEJO INADECUADO DE DATOS CRÍTICOS			
R6	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Estudiar la viabilidad de la criptografía como requerimiento de seguridad.

- Resguardar documentación que contengan descripciones técnicas con algoritmos y programas con sistemas de cifrado de archivos de toda la información indispensable que tengan relación con claves o firmas electrónicas.
- Establecer en los sistemas de almacenamiento de datos se logren recuperar en formatos legibles en un período determinado con sus respectivas restricciones.
- Determinar el nivel de protección que debe obtener la información considerando el tipo y la calidad de algoritmo de cifrado.
- Usar controles seguros que protejan las claves de acceso, siendo almacenadas de manera codificada y encriptada dentro de las bases de datos.
- Implementar procedimientos para la administración de claves, recuperación de información, daños de claves o en reemplazo de claves de cifrado.
- Adaptar nomas para la información clasificada que se transmita fuera de la institución, por medios móviles u otros dispositivos de comunicación.
- Establecer algoritmos de encriptación en toda la institución dependiendo el propósito, proceso o actividad a aplicar implementando controles que deben ser revisado y actualizados de manera periódica.

11. SEGURIDAD FÍSICA Y AMBIENTAL	
11.1	*Áreas seguras.*
11.1.1	Perímetro de seguridad física.
11.1.2	Controles físicos de entrada.
11.1.3	Seguridad de oficinas, despachos y recursos
11.1.4	Protección contra las amenazas externas y ambientales.
11.1.5	El trabajo en áreas seguras.
11.1.6	Áreas de acceso público, carga y descarga.
11.2	*Seguridad de los equipos.*
11.2.3	Seguridad del cableado.
11.2.4	Mantenimiento de los equipos.

DEFICIENTE RESTRICCIÓN DE ACCESO FÍSICO

R7	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Documentar perímetros de seguridad física necesarios mediante diversos accesos de control y adecuación. (barreras físicas, puertas de acceso, tarjetas magnéticas, entre otros.)
- Establecer un área de recepción para controlar el acceso dentro del área de sistemas.
- Disponer de cámaras de vigilancia para supervisar la permanencia de personas en áreas restringidas.
- Actividades dentro del área limitadas exclusivamente para personal autorizado utilizando controles de autenticación.
- Registrar del ingreso del personal en el área de sistemas definiendo la hora y fecha de su ingreso y salida.
- Establecer personal autorizado para escoltar a visitantes quienes deberán transitar en áreas restringidas.
- Actualizar en un periodo determinado la documentación de derechos de accesos en áreas restringidas firmados por los responsables.

ROBO DE EQUIPOS

R8	**Prioridad** 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Estrategias de Mitigación

- Instalar perímetros físicos de seguridad, restringiendo el paso de personal mediante tarjetas magnéticas, o barreras de protección.
- Supervisar el lapso de permanencia de individuos dentro de áreas restringidas, tomando registro de horario de su ingreso y salida.
- Proteger áreas restringidas que mantengan prioridad evitando así el acceso público a las instalaciones.
- Establecer dentro del área de sistemas acuerdos de responsabilidad de activos físicos.

- Aislar los equipos de procesamiento de información sensible que requieran protección especial evitando visualización a personas no autorizadas.
- Apoyo con cámaras y alarmas dentro del área restringida para detectar intrusos.

FALLAS ELÉCTRICAS

R9	**Prioridad** 9	**Tipo de riesgo**	Medio
			Media probabilidad – Medio impacto

Estrategias de Mitigación

- Establecer mantenimiento de forma periódica de las instalaciones eléctricas.
- Disponer de protección contra descargas eléctricas.
- Implementación de generadores de energía
- Utilizar filtros protectores en el suministro eléctrico y en líneas de comunicación en toda la institución.
- Realizar respaldo de información cumpliendo todos los requisitos de seguridad establecidos.
- Permitir de manera ordenada el cierre/apagado de los servicios que soportan operaciones críticas.
- Adoptar estrategias dentro del plan de contingencia ante este riesgo.

INEXISTENCIA DE PLAN DE CONTINGENCIA

R10	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto

Estrategias de Mitigación

- Definir el impacto y proporcionar cambios sobre la continuidad de servicios.
- Categorizar la información y su acceso para posteriormente analizar los riesgos dando solución y lograr adaptación.
- Establecer estrategias para minimizar el impacto en desastres inesperados en la institución.
- Aprobar el plan de contingencia identificando los posibles procedimientos que se deberán realizar en base a lo físico e intangible.

- Aplicar el plan de contingencia dependiendo de la funcionalidad o impacto que se haya generado.

RED CABLEADA EXPUESTA Y CON DETERIORO

R11	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Custodiar el cableado de red contra daño o intercepción bajo un responsable autorizado**.**
- Proteger dispositivos de comunicaciones bajo barreras físicas que tengan acceso a los módulos de conexión
- Separar los cables de red y comunicación a los cables de energía.
- Adaptar controles como firewalls en la red.
- Aplicar cableado estructurado de acuerdo a normas establecidas por el área de sistemas evitando errores de manejo enfatizando en el etiquetado.
- Establecer documentación de distribución de conexiones alámbricas e inalámbricas.
- Realizar mantenimiento de acuerdo a las especificaciones del proveedor de manera periódica.
- Definir controles para el mantenimiento preventivo o correctivo ya sean programados o emergentes.

INADECUADO MANTENIMIENTO DE EQUIPOS

R12	**Prioridad** 9	**Tipo de riesgo**	Medio
			Media probabilidad – medio impacto

Estrategias de Mitigación

- Establecer personal apropiado y autorizado para realizar procedimientos planificados.
- Definir la gestión de reparación de inicio a fin con el respectivo responsable previamente en conocimiento del jefe de sistemas.
- Realizar mantenimiento de equipos de forma periódica en software de servicio, gabinetes de servidores, telefonía, sistemas de UPS, instalaciones eléctricas, sistemas de climatización y ductos de ventilación.
- Realizar mantenimientos de corrección y prevención solucionando fallas relevantes o dudosas.
- Realizar mantenimiento de acuerdo a recomendaciones específicas de los proveedores.
- Implantar controles asociados con el mantenimiento programado y emergente.
- Notificar a los usuarios sobre los cambios a realizar y el lapso de ejecución.
- Revisar los controles que garanticen la integridad y no comprometer con los cambios asociados.
- Entregar documentación de las acciones realizadas

SISTEMAS DE CLIMATIZACIÓN Y CONDUCTOS DE VENTILACIÓN MAL ESTRUCTURADO

R13	**Prioridad** 9	**Tipo de riesgo**	Medio
			Media probabilidad – medio impacto

Estrategias de Mitigación

- Implementar sistemas de enfriamiento con aire de manera redundante para mantener la temperatura en caso de presentar fallas.
- Impulsar al consumo considerable de refrigeración como aire acondicionado ya que atribuye ineficiencias, establecer equipos de enfriamiento óptimo.

- Instalar racks en una configuración de pasillos fríos y calientes logrando patrones de flujo.
- Alinear los equipos con requisitos de temperatura similares y carga de calor, y aislar los equipos de temperatura y humedad de enfriamiento para disminuir el consumo de energía.
- Eliminar infiltraciones sellando o bloqueando entradas físicas en paredes o piso.
- Documentar servicios de calefacción, ventilación y aire acondicionado posibles a implementar para obtener la aprobación de la institución.
- Realizar mantenimiento de manera periódica en los sistemas de climatización y ductos de ventilación.
- Inspeccionar los suministros del área.

12. SEGURIDAD EN LA OPERATIVA.	
12.1	*Responsabilidades y procedimientos de operación.*
12.1.2	Gestión de cambios.
12.1.3	Gestión de capacidades.
12.2	*Protección contra código malicioso.*
12.2.1	Controles contra el código malicioso.
12.3	*Copias de seguridad.*
12.3.1	Copias de seguridad de la información.
12.3	*Gestión de la vulnerabilidad técnica.*
12.6.1	Gestión de las vulnerabilidades técnicas.
12.6.2	Restricciones en la instalación de software.
12.7	*Consideraciones de las auditorías de los sistemas de información.*
12.7.1	Controles de auditoría de los sistemas de información.

SOFTWARE MALICIOSO			
R14	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto
Estrategias de Mitigación			

- Documentar procedimientos dentro del área de sistemas para evaluar la información relativa a software malicioso.
- Implementar controles para la protección contra software malicioso garantizando seguridad en los datos de los servicios de la institución.
- Acuerdo de confidencialidad no ingresar ningún tipo de software que no sea autorizado.
- Realizar un listado del acceso al personal de desarrollo y el uso de software bajo autorización.
- Establecer responsables de procedimientos formales en instalación de equipos para evitar vulnerabilidad.
- Implantar procesos para evitar descargas de archivos a través de redes externas.
- Instalar y actualizar habitualmente software contra código malicioso.
- Revisar de manera periódica el contenido de los equipos.
- Contratar distintos proveedores de canales de datos de filtrado de servicios malware, virus, spam, entre otros.
- Definir auditorías periódicas para una certificación de calidad y revisión de códigos para detectar código malicioso cumpliendo requerimientos de seguridad de software.
- Realizar pruebas antes y después de la instalación de software para la detección de códigos maliciosos.

INADECUADO RESPALDO DE INFORMACIÓN

R15	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto

Estrategias de Mitigación

- Definir el responsable del área de sistemas que determinará los procesos para el respaldo y contención de la información.
- Documentar detalladamente los procesos de restauración y respaldo de la información.

- Identificar el contenido de las copias a respaldar para determinar su periodicidad de acuerdo a los requisitos establecidos por la institución.
- Realizar de manera periódica respaldos de información.
- Respaldar la información y guardar en un lugar alejado a una distancia prudente para evitar vulnerabilidad si existe daños en el área principal.

RESTRICCIONES DE SOFTWARE SIN IMPLEMENTAR			
R16	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Definir al personal capacitado para realizar revisiones en el software para garantizar que no se alteren los requerimientos por seguridad.
- Considerar los términos y condiciones establecidas en las licencias de software de código abierto o privativo.
- Establecer procesos de actualización de sistemas asegurando que loa parches sean autorizados.
- Elaborar informes que detallen cambios o acciones en el software.
- Corroborar los términos y condiciones que establecen las licencias de software.
- Verificar que se instale únicamente software autorizado.
- Controlar las versiones de software para mantener actualizaciones necesarias.
- Realizar cambios en una copia de software original para aplicar las versiones necesarias.
- Realizar pruebas y documentar detalladamente para mejoras a futuro si la aplicación es requerida.

13. SEGURIDAD EN LAS TELECOMUNICACIONES	
13.1	*Gestión de la seguridad en las redes*
13.1.1	Controles de red.
13.1.2	Mecanismos de seguridad asociados a servicios en red.
13.1.3	Segregación de redes.

13.2	*Intercambio de información con partes externas.*
13.2.1	Políticas y procedimientos de intercambio de información.
13.2.4	Acuerdos de confidencialidad y secreto.

INFRAESTRUCTURA SIN SEGMENTACIÓN DE RED APROPIADA

R17	**Prioridad** 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Estrategias de Mitigación

- Segmentar redes en el área de gestión o procesos con la capacidad considerable que sea necearía, mientras los recursos se ajusten a los requerimientos.
- Desinar responsabilidades para gestionar equipos remotos, puertos y accesos por VPNs.
- Ejecutar controles para salvaguardar la información, implicando la confidencialidad, disponibilidad e integridad, dentro de las redes públicas, inalámbricas y locales.
- Disponer de documentación donde se establezca la esquena de red, internet, enlaces, redes y sus dominios.
- Documentar los riesgos posibles a encontrarse en activos críticos identificando de los segmentos de red.
- Clasificar la información para realizar la separación de redes considerando la protección a los activos, considerando la división de dominios internos y externos.
- Realizar configuraciones para filtrar el tráfico de red permitiendo bloqueos a el acceso no autorizado.
- Separar redes inalámbricas enlazadas a redes privadas evitando el acceso de información a terceros.

INTRUSIÓN DE RED

R18	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Definir gestiones asociadas con la vulnerabilidad técnica incluyendo monitoreo, rastreo, uso de parches en los activos requeridos.
- Implementar sistemas de firewall y equipos de comunicación.
- Poner en funcionamiento un sistema de prevención detección de intrusos. IDS/IPS.
- Configuración de firewall.
- Monitorear el acceso que tienen los funcionarios en la red para detectar ataques reales.
- Revisión periódica a sistemas de escaneo de red.
- Protección de cableado de red
- Establecer UTM como método de prevención.

CAÍDA DE SISTEMAS DE COMUNICACIÓN

R19	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Establecer controles de datos en las redes públicas salvaguardando la integridad, confidencialidad y disponibilidad.
- Desarrollo de planes de gestión ante incidentes de disponibilidad
- Identificar incidentes de incumplimiento de leyes que provoquen no disponibilidad.
- Monitoreo y alertas en errores de fallas en los sistemas de comunicación.
- Determinar varios proveedores manteniendo el balance de carga para la disponibilidad de procesos en las instalaciones.
- Tener protección en líneas de comunicación en toda la institución.

INEXISTENCIA DE ACUERDOS DE CONFIDENCIALIDAD

R20	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Determinar términos y condiciones de contratación para la seguridad de la información.

- Establecer como requisito principal un acuerdo de confidencialidad o no divulgación, antes de adquirir información.
- Explicar la responsabilidad e importancia de las acciones de los funcionarios en base a la normativa.
- Acordar términos y condiciones bajo técnicas adecuadas para condiciones laborales que incluyen en la política de seguridad.
- Incluir la permanencia de requisitos para la protección de información mediante responsabilidades legales.
- Determinar en los acuerdos de confidencialidad actividades válidas aun después de su culminación laboral.
- Comunicar la importancia de acuerdos de confidencialidad en contratos laborales a nuevos funcionarios, contratistas o usuarios se deberá instaurar la documentación respectiva.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	
14.1	*Requisitos de seguridad de los sistemas de información***.**
14.1.1	Análisis y especificación de los requisitos de seguridad.
14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.
14.1.3	Protección de las transacciones por redes telemáticas.

LIMITADOS REQUISITOS DE SEGURIDAD DE COMUNICACIONES			
R21	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Establecer requerimientos de seguridad y controles apropiados manuales o automáticos.
- Definir los responsables del personal técnico que trabajarán en los sistemas.
- Establecer los niveles que se va a requerir en las aplicaciones para determinar requisitos de autenticación.

- Evaluar requerimientos proporcionales en costos y para protección de daños o fallas que se puedan ocasionar.
- Identificar que los proveedores establezcan contratos contemplando la seguridad en caso de adquirir productos.
- Proteger la información de actividades fraudulentas que un servicio puede prestar a través de redes públicas.
- Utilizar protocolos seguros en caso de transacción de información haciendo uso de firmas digitales.
- Hacer usos de sistemas de prevención de envío que no se permita en redes públicas.
- Implementar sistemas de protección contra envíos involuntarios de información.

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

INSUFICIENTES CONTROLES DE SERVICIOS PARA SUMINISTRADORES

R22	**Prioridad** 12	**Tipo de riesgo**	Alto
			Alta probabilidad – alto impacto

Estrategias de Mitigación

- Documentar los requisitos necesarios para la seguridad de la información y acordar el acceso a proveedores.
- Definir procesos necesarios de acuerdo a la evacuación de la información antes de la contratación de servicios.

- Adecuar controles limitando el acceso innecesario a la información para el desarrollo de trabajos.
- Supervisar los procedimientos establecidos y acordados con proveedores y a los funcionarios encargados de la verificación.
- Establecer que el proveedor informe si existen cambios ya sea de personal o servicios y el momento en el que serán realizados.
- Solicitar informes a los proveedores de acuerdo al servicio prestado.

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

INADECUADO CONTROL EN LA GESTIÓN DE EVENTOS			
R23	**Prioridad** 9	**Tipo de riesgo**	Medio Medio probabilidad – alto impacto

Estrategias de Mitigación

- Reportar incidentes que generen vulnerabilidad monitoreando sistemas y ejecutando distintos procedimientos para gestionar incidentes.
- Planificar estrategias preventivas para incidentes o acciones correctivas para la seguridad de la información.
- Definir responsables de la seguridad de la información para reportar inconvenientes, que brinde disponibilidad y respuestas oportunas.
- Solucionar incidentes y notificar las acciones de restauración del sistema o servicio afectado.
- Realizar auditorías para establecer buenas prácticas y ayudar en la toma de decisiones.

- En caso de detectar vulnerabilidades por parte de funcionario o proveedores se notificará al jefe de área con registro de nombres, fecha, hora y el inconveniente, para tomar medidas pertinentes.
- Priorizar incidentes de acuerdo al criterio afectado, llevando registro para analizar los parámetros de resolución e impacto.
- Evaluar que el área de sistemas tenga la capacidad de resolver eventos o requiere apoyo externo.
- Realizar análisis de cada incidente para puntualizar las causas y evitar inconvenientes próximos.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	
17. 1	*Continuidad de la seguridad de la información.*
17.1.1	Planificación de la continuidad de la seguridad de la información.
17.1.2	Implantación de la continuidad de la seguridad de la información.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

INEXISTENCIA DE PLAN DE CONTINUIDAD DE NEGOCIO

R24	**Prioridad** 9	**Tipo de riesgo**	Medio Media probabilidad – alto impacto

Estrategias de Mitigación

- Establecer la planificación e implementación de aspectos de continuidad de la seguridad de la información recobrando su proceso en el menor tiempo.
- Determinar actividades con objetivos y alcance considerando el tiempo de recuperación.
- Definir equipos destacados responsables de la continuidad de los servicios informáticos.
- Capacitar al personal que contemplan los procedimientos establecidos dentro del plan de continuidad de la seguridad de la información.

- Realizar pruebas para revisión y validación de la capacidad de respuesta ante desastres.
- Ejecutar simulaciones que permitan evaluar el plan de continuidad.
- Actualizar y corregir actividades que contemplen el plan de continuidad para el funcionamiento de servicios informáticos.
- Establecer estrategias en base a auditorías internas y externas que ayuden a mitigar desastres.

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

ESCASOS REQUISITOS LEGALES SOBRE LA SEGURIDAD DE LA INF.

R25	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Inventariar todo activo de información que cumpla con normas o reglamentos para cada servicio informático o software que utilicen en la institución.
- Establecer normas que pertenezcan a la gestión de información electrónica.
- Adquirir software de proveedores que garanticen derechos de propiedad intelectual considerando términos y condiciones que no sean violados.
- Proteger derechos de propiedad intelectual con registros apropiados en los activos de la información.

- Mantener evidencias de la propiedad de licencias, contratos, manuales, toda la información correspondiente al software a utilizar.
- Controlar el número máximo de usuarios que se puede permitir para un programa de software libre o privativo.
- Verificar que no se duplique contenido ni se extraiga archivos si no está permitido por el autor.
- Requerir que los responsables de desarrollo utilicen software aprobado por la institución.
- Realizar clasificaciones de registros electrónicos y físicos con su respectivo periodo de retención y medios de almacenamiento.
- Especificar y documentar el uso de encriptación y en qué ámbito se o aplicará.

INCENDIO			
R.E	**Prioridad** 8	**Tipo de riesgo**	Medio Baja probabilidad – alto impacto

Estrategias de Mitigación

- Supervisar de manera periódica el funcionamiento en los sistemas eléctricos.
- Realizar simulacros de incendios y capacitaciones por parte del cuerpo de bomberos.
- Proporcionar equipos apropiados contra incendios y mantenerlos ubicados de manera adecuada.
- Almacenar materiales peligrosos a una distancia prudente de los activos.
- Adoptar estrategias del cuerpo de bomberos para desastres de esta magnitud.
- Ubicar los equipos de respaldo a una distancia prudente de las instalaciones principales.
- Establecer estrategias del plan de continuidad de negocios frente a desastres.

SISMO			
R.E	**Prioridad** 12	**Tipo de riesgo**	Alto Alta probabilidad – alto impacto

Estrategias de Mitigación

- Almacenar equipos backup y soporte.
- Establecer que los edificios tengan mapas de riesgos de evacuación mínimo apropiado.
- Informar a los funcionarios sobre áreas seguras existentes.
- Incluir alertas.
- Establecer planes de seguridad física exclusiva para el área de sistemas
- Evaluar la continuidad de la seguridad de la información verificando la capacidad de respuesta ante desastres.
- Validar la capacidad de los responsables permitiendo mantener los planes establecidos.
- Realizar simulaciones de escenarios para controlar el peligro de la operación de los servicios informáticos.

DAÑOS POR VANDALISMO			
R.E	**Prioridad** 8	**Tipo de riesgo**	Medio Media probabilidad – alto impacto

Estrategias de Mitigación

- Vigilancia permanente en zonas exteriores al área de sistemas.
- Ubicación
- Establecer seguridad a nivel de racks que se encuentren en las instalaciones de la institución minimizando amenazas externas.
- Capacitar a los funcionarios del área de sistemas contemplando la continuidad de los servicios informáticos.
- Evaluar la capacidad de respuesta ante desastres permitiendo actualizar y mejorara planes establecidos.
- Aplicar un plan de continuidad considerando el peligro de los servicios informáticos minimizando la discontinuidad de actividades.

CONCLUSIONES

- Al concluir se logra identificar las oportunidades de mejora y mitigación por los posibles riesgos encontrados mediante el análisis previo, es evidente que el Departamento de Sistemas está comprometido en el mejoramiento de gestión a su cargo para fortalecer regularidades en las normas establecidas.
- Políticas de seguridad

  El compromiso con la institución y autoridades se sustenta con normas documentadas que puedan respaldar los procesos o actividades dentro del área de Sistemas, se debe disponer de la implementación del SGSI como política de Seguridad de la Información como referencia.
- Aspectos organizativos de la seguridad de la información

  La asignación de responsabilidades de la información establece criterios de cumplimientos designados directamente para el personal de seguridad de la información, al no complementar estas funciones destinadas a un solo funcionario no se

las realiza a cabalidad, no siendo suficiente con las responsabilidades que se viene tomando con anterioridad.

- Seguridad ligada a los recursos humanos.

  Podemos concluir que es un dominio seguro al mantener todos los controles dentro de la normativa con un alto cumplimiento, por lo cual la mitigación de riesgos sería efectiva.

- Gestión de activos

  Dentro de la gestión de activos cabe recalcar que su funcionamiento es producente, sin embargo, podemos destacar que la información se debe categorizar para brindar mayor prioridad, ayudando al nivel de protección de confidencialidad, disponibilidad e integridad.

- Control de acceso.

  El control de acceso siendo el mecanismo directo a evitar vulnerabilidades es posible que se encuentren amenazas, para ello se debe otorgar mayor priorización en establecer privilegios para responsabilizar a funcionarios por sus acciones.

- Cifrado.

  Al no existir mecanismos de cifrado es por eso que, se debe resguardar documentación que contengan descripciones técnicas o de alta confidencialidad con algoritmos y programas con sistemas de cifrado de archivos de toda la información indispensable.

- Seguridad física y ambiental.

  Podemos tomar en cuenta que existe protección física al área restringida de activos, sin embargo, existen posibles riesgos que pueden ocasionar el no mantener un nivel más alto de protección, limitando restricciones con funcionarios.

- Seguridad en la operativa.

  La seguridad del presente dominio posee seguridad media, por lo tanto, existen factores que lo pueden vulnerar, siendo la prioridad establecer controles contra códigos maliciosos.

- Seguridad en las telecomunicaciones.

  Los equipos se encuentran sin ninguna protección que evite la manipulación de terceros, causando mal funcionamiento o siendo víctimas de robo de información confidencial,

el cableado es una amenaza física con la que se puede infectar de forma maliciosa provocando vulnerabilidad.

- Adquisición, desarrollo y mantenimiento de los sistemas de información.

  Se realizan los procesos bien estructurados que cumple la mayor parte de los controles dentro de la normativa, pero puede existir vulnerabilidad de la misma al no contar con ciertos criterios de encriptación.

- Relaciones con suministradores.

  Se debe establecer controles frente a los suministradores evitando convertirse en fuentes de vulnerabilidad o fuga de información mediante su contratación de servicios.

- Gestión de incidentes en la seguridad de la información.

  Existen informes de acontecimientos para su previo análisis y mitigación de riesgos, sin embargo, se debe implementar un plan de continuidad como también para la seguridad del personal involucrando procesos críticos.

- Aspectos de seguridad de la información en la gestión de la continuidad del negocio.

  Se debe considerar las actividades y procedimientos que cumplan con su objetivo, alcance y tiempo de recuperación, definir personal responsable y capacitado que contemplen planes de continuidad para el funcionamiento de servicios informáticos.

- Cumplimiento.

  El cumplimiento de políticas de seguridad de la información debe contar con acciones correctivas determinando la causa y evaluaciones para garantizar que no se repitan dichos acontecimientos.

- El marco referencial ISO/IEC 27002 permite implantar estrategias para acciones específicas en los 114 controles de seguridad, por ende, los incidentes bajo una normativa y responsabilidad adquirida obtendría solución inmediata, se definen soluciones correctivas o preventivas por lo cual su cumplimiento es moderado de acuerdo con los resultados del análisis.

- Se logra determinar que el cumplimiento actual es el 29.77% lo cual no garantiza la seguridad de la información en la institución, por ende, se realiza una posible implementación en base a estrategias establecidas por los controles de seguridad del

estándar que se proyecta un incremento significativo del 62.41% permitiendo garantizar la confidencialidad, disponibilidad e integridad de la información.

	Nombre/ Cargo	Firma
Revisado por:	Msc. Jairo Vladimir Hidalgo Guijarro	Firmado electrónicamente por: JAIRO VLADIMIR HIDALGO GUIJARRO
Elaborado por:	Joselin Pamela Igua Alvarez