REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

Tema:

EVALUACIÓN DE LA SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN DEL GAD MUNICIPAL DE ESMERALDAS BASADO EN LAS NORMAS DE CONTROL INTERNO

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

Autor: Mgt. David Leonardo Rodríguez Portes

Director: Mgt. Mario Bernabé Ron Egas

IBARRA - ECUADOR

2024

DEDICATORIA

A mis padres; Leonardo+ y Janeth, que son el origen de mi vida, fuente inagotable de amor incondicional y apoyo desde niño hasta adulto, ejemplo de vida que con sacrificio y amor han forjado la persona que soy y cuyos preceptos me acompañan siempre en cada paso que doy.

A mi esposa: Lorena, por todo el apoyo recibido, sobre todo en esta etapa de preparación académica en donde no solo ha sido mi compañera de vida, sino el soporte fundamental para como siempre terminar con éxito lo emprendido.

A mis hijos: Juren, Josue y Mia, realmente el propósito de vida, mi mayor motivación para ser mejor, y así como para conmigo, poder guiarles y cuidarlos con paciencia, dedicación y amor incondicional.

A todos mis familiares y amigos, que de una u otra forma han contribuido en diferentes instancias, y han jugado un papel importante en cada etapa de mi vida por su cariño y consideración.

David Leonardo Rodríguez Portes

AGRADECIMIENTO

A Dios, por ser el que guía mis pasos y bendice los caminos que recorro, por la bendición de haber tenido esta oportunidad de crecer académicamente, profesionalmente y también como persona durante todo este tiempo en donde se han superado muchos obstáculos y limitaciones.

A la universidad Técnica del Norte, su personal administrativo, sobre todo nuestro Coordinador de la Maestría en Computación con mención en Seguridad Informática, el Ing. Alexander Guevara Vega por su acompañamiento, asistencia y colaboración durante todo el proceso de la carrera.

A mi tutor, Magister Mario Ron Egas, por su orientación y asesoría que a través de sus experiencias y tutela han permitido impregnar una visión y enfoque de mejora continua de la evaluación de la seguridad de la información considerando la ley de protección de datos personales del Ecuador.

A mis docentes y a todas aquellas personas que de alguna manera contribuyeron a la realización de este trabajo de investigación en donde cada una de las enseñanzas y experiencias del aula y la profesión han sido puestas en la práctica en beneficio de una institución orientada al servicio público que atiende a una comunidad.

Al Municipio de Esmeraldas, en la persona del Alcalde Magister Vicko Villacis Tenorio, por haberme dado las facilidades del caso para poder desarrollar la investigación, y en especial a todos los miembros de la Dirección de Tecnologías de la Información y Comunicación por toda la colaboración recibida durante el proceso de recolección de datos.

David Leonardo Rodríguez Portes

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	0802079772		
APELLIDOS Y NOMBRES:	Rodríguez Portes David Leonardo		
DIRECCIÓN:	Urbanización Tecnipetrol Mz 33 casa 02		
E-MAIL:	david.pucese@gmail.com		
TELÉFONO FIJO:	062019205	TELÉFONO MÓVIL:	0987080217

DATOS DE LA OBRA	
TÍTULO:	Evaluación de la seguridad de tecnología de información del GAD municipal de Esmeraldas basado en las normas de control interno.
AUTOR (ES):	Rodríguez Portes David Leonardo
FECHA: DD/MM/AA	14/06/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	PREGRADO [ ] POSGRADO [X]
TÍTULO POR EL QUE OPTA:	Magister en computación con mención en seguridad informática
ASESOR/DIRECTOR:	Phd. Daysi Imbaquingo / MSc. Mario Ron Egas

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

CONSTANCIAS

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es el titular de los derechos patrimoniales, por lo que asume a responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 4 días del mes de septiembre de 2024.

Firmado electrónicamente por:
DAVID LEONARDO
RODRIGUEZ PORTES

Firma: ……

Nombre: David Leonardo Rodríguez Portes

C.I. Nº 0802079772

Ibarra, 14 de junio de 2024

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señor(a) Decano(a):

Nos permitimos informar a usted que revisado el Trabajo final de Grado "EVALUACIÓN DE LA SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN DEL GAD MUNICIPAL DE ESMERALDAS BASADO EN LAS NORMAS DE CONTROL INTERNO" del maestrante DAVID LEONARDO RODRÍGUEZ PORTES, de la Maestría de Computación con mención en Seguridad Informáticacertificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	**Firma**
Director/a	MSc. Mario Ron Egas	MARIO BERNABE RON EGAS
Asesor/a	Phd. Daysi Imbaquingo	1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA Firmado digitalmente por 1002873048 DAISY ELIZABETH IMBAQUINGO ESPARZA Fecha: 2024.06.15 21:46:00 -05'00'

Tabla de Contenidos

Índice de Tablas

Índice de figuras

GLOSARIO

BIESS: Banco del Instituto Ecuatoriano de Seguridad Social

BID: Banco Interamericano de Desarrollo

CERT: Equipo de respuesta ante emergencias informáticas

CGE: Contraloría General del Estado

CNT: Corporación Nacional de Telecomunicaciones

COBIT: Control Objetives for Information and Related Technology

COSO: Committee of Sponsoring Organizations of the Tradeway Commission

COVID: Corona Virus Disease

GAD: Gobierno autónomo descentralizado

GADMCE: Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas

EGSI: Esquema Gubernamental de Seguridad de la Información

ETI: Evaluación Técnica Informática

IA: Inteligencia Artificial

IEC: International Electrotechnical Commission

INCIBE: Instituto Nacional de Ciberseguridad

INEN: Servicio Ecuatoriano de Normalización

IOT: Internet de las cosas

ISACA: Information Systems Audit and Control Association

ISO: International Organization for Standardization

ITIL: Information Technology Infrastructure Library

LOPDP: Ley de Orgánica de Protección de Datos Personales

NIST: National Institute of Standards and Technology

NCI: Normas de control interno

NTE: Norma Técnica Ecuatoriana

OEA: Organización de Estados Americanos

PWC: Price waterhouse Coopers

RGPD: Reglamento General de Protección de Datos

SGSI: Sistema de Gestión de Seguridad de la Información

TI: Tecnologías de Información

TIC: Tecnología de la Información y Comunicación

UIT: Unión Internacional de Telecomunicaciones

UNODC: Oficina de las Naciones Unidas para el Crimen y el Delito

WIFI: wireless fidelity

REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

EVALUACIÓN DE LA SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN DEL GAD MUNICIPAL DE ESMERALDAS BASADO EN LAS NORMAS DE CONTROL INTERNO

Autor: Nombre completo del estudiante

Tutor: Nombre completo del tutor

Año: 2024

RESUMEN

Esta investigación se centra en una auditoria de la seguridad de tecnologías de información, el cumplimiento de la normativa legal vigente, y la necesidad de evaluar constantemente el ambiente de control de un municipio de algo más de mil funcionarios, una base catastral de alrededor de 72.000 predios, y casi 10.000 usuarios recurrentes de la plataforma web municipal; en una ciudad que bordea los 200.000 habitantes urbanos. El objetivo general fue evaluar la seguridad de tecnologías de información de la institución en base a las normas de control interno de la Contraloría General del Estado. El tipo de investigación fue mixta: bibliográfica – descriptiva, y consistió, en la recopilación de información existente en investigaciones similares, artículos y revistas; esto permitió, la elaboración del marco de referencia. La investigación descriptiva, se utilizó para diagnosticar la problemática; las técnicas utilizadas para la recopilación de información fueron: encuestas, aplicadas a los funcionarios; entrevistas, dirigidas a los responsables de TI, y la observación, realizada la infraestructura tecnológica y a los procesos internos de la Dirección de TIC. Los resultados obtenidos mediante la aplicación de las normas ISO 27001:2022 y la aplicación de los métodos analítico, deductivo e inductivo; proporcionaron una visión más completa de la problemática y del nivel de cumplimiento de los controles de seguridad de información implementados. Durante la presentación y discusión de los resultados se realizó una exposición analítica y depurada de los principales hallazgos, evidenciado la incidencia que tienen las medidas actuales, y el bajo nivel de cumplimiento de las normas. En el informe final también se incluyeron las recomendaciones y acciones correctivas que la institución deberá incorporar para formalizar y fortalecer su SGSI, a través de un plan de mejora que supone la implementación de políticas de seguridad de la información para el GADMCE.

Palabras clave: SGSI, Normas de control interno, ISO27001:2022, Análisis y evaluación de riesgos, Política de Seguridad.

ABSTRACT

This research focuses on an audit of information technology security, compliance with current legal regulations, and the need to constantly evaluate the control environment of a municipality with more than a thousand employees, a cadastral base of about 72,000 properties, and almost 10,000 recurring users of the municipal web platform; in a city with a population of about 200,000 urban inhabitants. The general objective was to evaluate the security of the institution's information technologies based on the internal control standards of the Office of the Comptroller General of the State. The type of research was mixed: bibliographic - descriptive, and consisted of the compilation of existing information in similar research, articles and magazines; this allowed the elaboration of the frame of reference. The descriptive research was used to diagnose the problem; the techniques used to collect information were: surveys, applied to employees; interviews, directed to IT managers, and observation, carried out in the technological infrastructure and internal processes of the ICT Directorate. The results obtained through the application of ISO 27001:2022 standards and the application of analytical, deductive and inductive methods provided a more complete view of the problem and the level of compliance with the implemented information security controls. During the presentation and discussion of the results, an analytical and refined exposition of the main findings was made, evidencing the incidence of the current measures and the low level of compliance with the standards. The final report also included recommendations and corrective actions that the institution should incorporate to formalize and strengthen its ISMS, through an improvement plan that involves the implementation of information security policies for the GADMCE.

Keywords: ISMS, Internal Control Standards, ISO27001:2022, Risk Analysis and Assessment, Security Policy.

CAPÍTULO I
EL PROBLEMA

1.1. Problema de investigación

Codolà Vilahur et al. (2018), señalan que, desde la masificación de los sistemas de información y el uso indiscriminado de internet, los problemas derivados de la seguridad de la información evolucionaron mucho, y las soluciones a cada incidente se fueron adaptando a los nuevos requerimientos técnicos, que, ante la sofisticación de los incidentes, aumentaron la complejidad de la solución. Si bien, la tecnología evoluciona de una manera exorbitante y exponencial, los constantes avances e innovaciones tecnológicas lleva a las organizaciones a enfrentar amenazas contra la disponibilidad se sus sistemas, la integridad de sus datos, y la confidencialidad de su información, lo que obliga a las organizaciones a tomar medidas para proteger sus recursos. Muchas veces estas medidas constituyen inversión en tecnología y adquisición de equipos para aumentar la seguridad de información en las organizaciones, pero es necesario primero organizarse e implementar esquemas de seguridad, está claro que las instituciones se encuentran expuestas a los ataques de intrusos, que identifican vulnerabilidades, los famosos "huecos de seguridad", que son aprovechados por los atacantes, generando algún tipo de incidente.

Según Alvarado (2018), América Latina y el Caribe además de los problemas típicos e históricos, enfrenta grandes desafíos en materia de seguridad, es la única región del mundo en donde el homicidio es la principal causa externa de muerte. Los avances tecnológicos e innovaciones digitales han sofisticado los delitos tradicionales, inclusive con toda esa evolución tecnológica hemos sido testigos de ataques cibernéticos que jamás nos hubiéramos imaginado. El cibercrimen ya no es una amenaza del futuro para la que nos debemos preparar, es una amenaza del presente para la que muchas organizaciones no están preparadas. Esto se evidencia en las encuestas realizadas por SOPHOS (2019) en donde el 90% de las empresas que sufrieron ciberataques hasta la fecha, contaban con soluciones de seguridad simples y tradicionales que no entregaban un adecuado grado de confiabilidad sobre la protección que estos sistemas podrían brindarle a la compañía. Este tipo de situaciones desencadenan dudas respecto a la gestión realizada en las organizaciones a nivel de seguridad, ya que muchas de estas falencias podrían deberse a un comportamiento negligente de la alta dirección por no entregar un presupuesto idóneo para las áreas de TI, que va de la mano con la falta de competencias en las instancias

decisorias de las organizaciones que imposibilitan que se dirijan esfuerzos hacía garantizar niveles adecuados de la seguridad de la información, ya que en la mayoría de los casos se piensa más desde el componente financiero, pero no se tiene en cuenta que para lograr esto se debe sentar unas bases en el aseguramiento de la información (Domínguez y Solís, 2009).

La Unión Internacional de Telecomunicaciones (2019), señala que en esta nueva era urbana, son más de 4 billones de personas las que acceden a la gran red de redes: la internet; es decir representan algo más de la mitad de la población mundial. La creciente democratización de las tecnologías de la información y comunicación ha traído consigo una serie de retos y cambios, en donde la aplicación y uso de medios tecnológicos con fines delictivos se ha incrementado drásticamente, originado por las facilidades de anonimato que el Internet ofrece a un gran número de personas y grupos para ocasionar actividades de sabotaje y terrorismo, superando las fronteras físicas, constituyéndose en verdaderas amenazas a nivel global tanto para los individuos como para organizaciones.

El reporte elaborado en conjunto por BID y OEA (2020), sostiene que los países de la región no están preparados para contrarrestar los ataques originados en el internet, pues solo siete de los treinta y dos países analizados cuentan con mecanismos de protección en su infraestructura tecnológica, aunque una veintena países han determinado salvaguardas en respuesta a los incidentes, se evidencian las limitaciones para identificar ataques y contenerlos de forma adecuada. En Ecuador, las entidades públicas no han estado exentas de brechas de seguridad, prueba de ello es que, en el 2019, ocurrió la mayor filtración de información en la historia del país, cuando millones de ciudadanos quedaron expuestos en un servidor localizado en EEUU. La información contenía datos como números de cédula y de teléfono, registros financieros, historial laboral y salarios. Si bien los datos eran administrados por la empresa Novaestrat, provenían de fuentes externas, entre ellas el BIES. En 2021 ocurrieron más vulneraciones a la privacidad de las personas, una de ellas se registró en el MSP (Ministerio de Salud Pública), vinculada a los datos de pacientes que se habían realizado pruebas diagnóstico de Covid-19; y la otra ocurrió en la CNT (Corporación Nacional de Telecomunicaciones), cuando un ataque informático a sus sistemas, afectó a los servicios de atención al cliente por varios días. A pesar de que la CNT aseguró en ese entonces que los datos de sus clientes estaban "debidamente resguardados", quedó la incógnita de qué tan seguros estaban los datos (González, 2023).

La firma de auditoría PricewaterhouseCoopers (PWC, 2018), en un estudio realizado detectó que ante un ciberataque el principal impacto negativo para las empresas en el mundo recayó sobre la interrupción de la operación en un 40% de los casos, 39% fue la perdida de información confidencial, el 32% tuvo un impacto negativo en la calidad de los productos, el 29% significó daño a la propiedad física, mientras que el daño a la vida humana presentó el menor número con un 22%, es decir las organizaciones deben mantener planes, políticas y sistemas de seguridad de la información eficientes.

La Oficina para el Crimen y el Delito de las Naciones Unidas (UNODC, 2023), establece que la violencia en una localidad se mide por la tasa de muertes por cada 100.000 habitantes, con base en este parámetro y la información recogida por InSightCrime, Esmeraldas es catalogada como la tercera zona más violenta de América Latina (Primicias, 2023), muchos de esos crímenes quedan grabados en los sistemas de videovigilancia tanto del ECU 911 como del Proyecto de Ciudad Inteligente del GAD Municipal, lo que constituye un activo de información de alto riesgo para los usuarios, tanto para los funcionarios municipales, judiciales y de fuerzas armadas. A pesar de que existe un protocolo en lo relacionado con el manejo de la información en el acuerdo de confidencialidad entre las instituciones que inter operan, a nivel interno de la institución existe un procedimiento formal que garantice la seguridad de la información ahí contenida. Según decreto ejecutivo DE-681(2023), la provincia de Esmeraldas ha sido declarada en estado de excepción por los altos índices de violencia a cargo de bandas catalogadas como terroristas cuyo comportamiento y prácticas delictivas se han venido recrudeciendo durante los últimos meses, poniendo en riesgo la vida de los ciudadanos.

La Alcaldía de Esmeraldas (2021) inauguro un proyecto de más de dos millones de dólares en infraestructura tecnológica para la ciudad, denominado Esmeraldas Ciudad Inteligente, con interoperabilidad al ECU 911; el cual consiste en usar tecnologías (cámaras IP, redes públicas de conectividad inalámbrica, sensores medioambientales) como un sistema integrado para la gestión y monitoreo de las competencias municipales, de sus unidades adscritas y empresas públicas con la finalidad de resolver o mitigar los problemas agobiantes de la ciudadanía relacionados a la seguridad, movilidad, y servicios públicos (sobre todo la recolección de la basura). La tabla 1.1 que se presenta a continuación, contiene los componentes en donde se encuentran agrupados la mayoría de activos informáticos de la institución.

Tabla 1.1
Componentes principales del Proyecto de Ciudad Inteligente del GADMCE

Item	Componentes del proyecto con activos informáticos	Valor en USD
1	Sistema de video vigilancia (cámaras)	240.000
2	Video wall con consola	120.000
3	Sistema de perifoneo IP	100.000
4	Sistema de energía autónoma	100.000
5	Centro de monitoreo de la ciudad	60.000
6	Centro de datos y sistema de almacenamiento	200.000
7	Puntos de control para acceso de la ciudad	40.000
8	Sistema de monitoreo ambiental mediante sensores	100.000
9	Plataforma de conectividad WIFI para la ciudad	90.000
10	Red de fibra óptica (100Km)	700.000
	Total	1’750.000

Nota. Estos componentes agrupan la mayoría de activos informáticos adquiridos en el proyecto.

Esta gran cantidad de activos (equipos informáticos, dispositivos de almacenamiento, monitoreo, de red, de comunicación, y aplicaciones web) exigen contar con medidas que garanticen operatividad y funcionamiento las 24 horas, los 365 días del año, es decir la continuidad de los servicios que la institución brinda, pero además de proteger y precautelar los bienes adquiridos, que son patrimonio de la ciudad, el manejo de información sensible debido a la fuerte ola de violencia que vive el país y sobre todo la ciudad, genera para la institución, una mayor responsabilidad en el tratamiento que se da a todo lo visualizado y almacenado en esos sistemas de monitoreo y videovigilancia.

Las ciudades inteligentes también conocidas como del futuro o Smart Cities en inglés, son áreas urbanas que utilizan soluciones innovadoras y tecnología avanzada para generar bienestar en los ciudadanos, impulsar la sostenibilidad ambiental, alcanzar la eficiencia de los servicios, y optimizar la gestación de recursos. Estas ciudades aprovechan las TIC para abordar una variedad de desafíos urbanos y proporcionar servicios más eficientes y efectivos. Dameri y Rosenthal-Sabroux (2018) sostienen que el objetivo de una ciudad inteligente es, desde una perspectiva académica y también por su sostenibilidad ambiental: mejorar la calidad de vida de sus ciudadanos, usando las últimas innovaciones tecnológicas disponibles o incluso sin ellas, ya que es el triunfo del conocimiento, su principal foco es una visión civicéntrica, sustentada en el ciudadano, sin menospreciar el desarrollo del espacio urbano y la productividad del sector empresarial, pero desde una perspectiva práctica el objetivo principal es conseguir que la ciudad sea eficiente en la solución de sus problemas con los mismos recursos existentes, con medidas de seguridad acordes a la era, de allí que una ciudad se considera inteligente en la medida en que resuelve sus problemas utilizando los recursos existentes.

Adicional a los activos del proyecto citado anteriormente, la institución cuenta con un parque informático, con los que usuarios interno y externos acceden a los diversos sistemas y aplicaciones, pero nunca se ha realizado un proceso de auditoría interna que evalúe técnicamente el sistema de gestión de la seguridad de la información, y sobre todo no existe un nivel de conciencia de la importancia que tiene la seguridad de la tecnología de la información en la institución, de allí que García-Cervigón y Alegre (2011, p. 26) afirman que: "la seguridad Informática es una parte esencial dentro de las instituciones, la información es uno de los activos primordiales que puede llegar a tener un valor incalculable y, por lo tanto, se necesita ejercer su protección".

El MINTEL(2021) señala que a raíz del COVID-19, los gobiernos a nivel mundial se vieron obligados tomar medidas que todavía se encontraban en su fase experimental en la mayoría de países, sobre todo los Latinoamericanos, como son trabajo remoto, las clases virtuales e incluso la telemedicina, esto incrementó de manera exponencial la cantidad de problemas provocado por la medida. Evidenciando que la mayoría de empresas, instituciones y la sociedad en sí, no estaba preparada para un cambio que implicó también enfrentar los riesgos, debido a que hasta esa fecha eran pocas las organizaciones con políticas, normativas, procedimientos, y herramientas que aseguren un ambiente seguro en este nuevo mundo virtual. Por lo que, la gestión y aplicación de la tecnología, y las crisis externas a las organizaciones son los principales focos de amenazas que conforman los riesgos de seguridad de tecnologías de información que encabezan la lista, y qué asociados ponen en inminente peligro la operación de las mismas, si no se evalúan en forma correcta identificando su mapeo relacional con los procesos de negocio y su entorno operativo (Numpaque, 2021).

El GADMCE tiene una base catastral conformada por aproximadamente 72 mil predios entre urbanos y rurales, sobre los que se dan servicios y atención de trámites a diario, pero debido a la falta de un edificio principal, se encuentra distribuido en 14 edificios ubicados en lugares distantes, en donde funcionan las direcciones que conforman la institución, lo que genera a nivel operativo: desfases tanto en atención al usuario, la comunicación interna entre funcionarios, y la misma ejecución de procesos entre direcciones, generando demoras e inconvenientes sobre todo en la reputación; y a nivel tecnológico una serie de inconvenientes en la red, que retardan los procesos y los expone a los activos de información a una gran cantidad de vulnerabilidades. Por lo que

es importante que la institución implemente esquemas metodológicos y estándares con las mejores prácticas para el asegurando, procesamiento, almacenamiento, transparencia y gestión de información que maneja. Así Cusme et al. (2020) menciona que de no implementar el cumplimiento obligatorio de la norma de control interno 410 de la CGE (Contraloría General del Estado), se pone en riesgo tanto la disponibilidad, confidencialidad e integridad de la información, como los servicios tecnológicos provistos por las unidades de TI de cada institución.

Según el MINTEL (2021), una problemática a nivel del sector público es las vetustez y obsolescencia del parque informático de la gran mayoría de instituciones, sumado a las limitaciones presupuestarias y poca inversión en licencias y software licenciado, al punto de tener un decreto que limita el gasto en torno a esto, configurándose en uno de los retos para las gestiones administrativas al momento de garantizar protección de la información. Las organizaciones son objeto de incontables intentos a diario por acceder a la información y el control de sus equipos, por parte de los delincuentes informáticos. Para las instituciones que han sido víctimas de ataques informáticos, no ha sido prioridad capacitar el personal y la indagación respecto a las posibles medidas de seguridad que deben tomarse para prevenirlos. En este sentido en abril de 2021, En el país se aprobó la Política Nacional de Ciberseguridad con aplicación a los sectores públicos y privados.

Los procesos de transformación digital de la institución y los riegos informáticos ocasionados por el uso de las tecnologías en los procesos, servicios, infraestructuras e instalaciones de la institución, la falta de planes reales, el bajo nivel de conciencia de los funcionarios públicos, el incumplimiento de la normativa vigente en relación a la seguridad; implica la adopción de mecanismos de control y la evaluación del cumplimiento de las normativa establecida por la CGE, Ante esto se desprende como problema general la siguiente pregunta: ¿Cómo la evaluar el grado de cumplimiento de las normas de control de interno de la Contraloría General del Estado a nivel de seguridad de tecnología de información en el GAD Municipal de Esmeraldas?

1.2. Interrogantes de la investigación

De la interrogante citada anteriormente se desprenden las siguientes interrogantes que relacionan los problemas específicos:

- ¿Qué temas deben considerarse en la revisión bibliográfica y documental para la sistematización del marco de referencia (estado del arte, la fundamentación teórica, y la normativa legal vigente) de esta investigación?
- ¿Cuáles son los mecanismos implementados por el GAD municipal de Esmeraldas a nivel de seguridad de tecnología de información para mantener un ambiente de control que asegure la continuidad de los servicios, la operatividad de la infraestructura tecnológica y salvaguarde los activos de información?
- ¿Cómo determino objetivamente los activos de información de la institución a nivel de parque informático, software, almacenamiento, redes y comunicaciones sobre los que se va a evaluar el riesgo informático?
- ¿Cuáles son los aspectos organizacionales, físicos, de personal y tecnológicos establecidos por las normas de control interno, que deben incluirse en el informe de resultados de la evaluación del GAD municipal de Esmeraldas?
- ¿Cómo asegurar que los hallazgos, observaciones y recomendaciones sean tomados en cuenta por la alta dirección para su implementación, la mejora continua y el fortalecimiento de su sistema de gestión de la seguridad de la información?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Evaluar la seguridad de tecnología de información del GAD municipal de Esmeraldas basado en las normas de control interno de la Contraloría General del Estado.

Hipótesis de trabajo

Los mecanismos aplicados en del GAD Municipal de Esmeraldas basados en las normas de control interno de la Contraloría General de Estado inciden en la seguridad de la información de la institución.

Variable independiente: Mecanismos basados en la norma de control interno.

Variables dependientes: Seguridad de la Información.

Hipótesis alternativa

Los mecanismos aplicados en del GAD Municipal de Esmeraldas basados en las normas de control interno de la Contraloría General de Estado no inciden en la seguridad de la información de la institución.

1.3.2 Objetivos específicos

- Analizar la infraestructura tecnológica y los mecanismos de seguridad informática existentes en el GAD municipal de Esmeraldas mediante la la gestión de riesgoinformático.
- Evaluar la seguridad que la institución tiene a nivel de parque informático, software, almacenamiento, redes y comunicaciones a través de una matriz de valoración del riesgo informático.
- Elaborar el informe de auditoría del GAD municipal de Esmeraldas considerando las normas de control interno de la Contraloría General del Estado.
- Proponer un plan de mejora a través de la implementación de políticas de seguridad.

1.4. Justificación

El MINTEL (2021) ha definido la Estrategia Nacional de Ciberseguridad de cumplimiento para todo el país, incluyendo Gobierno Nacional, organismos de control, instituciones judiciales, Gobiernos Autónomos Descentralizados, empresas privadas, entidades académicas y financieras. Su objetivo es generar un ciberespacio seguro para los ciudadanos, promoviendo agilidad en los procesos y creando confianza a escala internacional para que más empresas inviertan en el país. Esta estrategia nacional está alineada con los objetivos de desarrollo sostenible elaborado por la Organización de Naciones Unidades (ONU), para generar proteger al planeta y a las personas que lo habitan. Por tanto, al evaluar la seguridad de información del GAD Municipal de Esmeraldas bajo la normativa vigente, no solo que da primer paso para diagnosticar su situación actual, sino que inicia un proceso de mejora continua que le permita fortalecer los mecanismos y controles de protección y salvaguarda contra pérdida de datos y fugas de información de los medios físicos y digitales que soportan los sistemas de información de la institución.

Según Alarcón et al., (2023) después de la pandemia, el 80% de las instituciones que conforman el sector público en Ecuador han adoptado en un enfoque proactivo en sus marcos administrativos y modelos gestión de TI. Estos cambios significativos no solo tienen que ver con el cambio de época o con el post pandemia, sino que tiene que ver con la nueva visión que a nivel estratégico se ha marcado con procedimientos y reglamentación que van desde la gestión del inventario de los recursos informáticos, la asistencia y soporte por medio de la mesa de ayuda, hasta la administración de proyectos tecnológicos enfocados a garantizar la operación y continuidad de los servicios del sector. Pero estas no deben ser acciones de aisladas de la alta dirección o máxima autoridad de las instituciones, sino que debe tener una visión integral liderada por estas personas que garanticen un verdadero sistema de gestión de la seguridad de la información (SGSI) en las instituciones.

La seguridad es un estado de confianza, ese estado pude obtenerse de dos formas: por conocimiento o por desconocimiento, la función de la Dirección de Tecnologías es que sea por conocimiento, es decir por la aplicación de metodologías, herramientas y estándares, que no solo garanticen el cumplimiento de la normativa, sino la continuidad de los servicios que los usuarios internos y externos necesitan para generar calidad de vida en los ciudadanos de la urbe, y en el caso de la información sensible hoy más que nunca es necesario que se garantice la seguridad de la información que se almacena y procesa. En el sector público, sobre todo en los gobiernos locales, los riesgos con un alto impacto sobre la seguridad de la información se encuentran dentro de los riesgos con mayor valoración inherente dentro de las matrices de riesgos, donde la información se constituye como el activo más relevante. Por lo que en el caso del GADMCE, esta investigación fortalece los procesos de mejora continua de las operaciones de todos los estamentos monitoreados y controlados por el Centro de Operación del Proyecto de Ciudad Inteligente, beneficiando a la gestión de la administración, a sus funcionarios, autoridades, y a los propios ciudadanos que son usuarios directos o indirectos de los servicios del municipio.

Según Ponce (2023), socio legal de PricewaterhouseCoopers, luego de la entrada en vigor en el Ecuador de la Ley de Protección de Datos Personales, es necesario que todas las organizaciones identifiquen claramente el tratamiento que dan a los datos personales que manejan, los medios en donde se encuentran estos datos, de manera que

adapten sus recursos tecnologías, procedimientos y reglamentación (políticas) con la finalidad de no solo desde cumplir con la ley, sino más bien de proteger la información desde la seguridad que le brindan al tratamiento de los datos a nivel administrativo y técnico, a través de sistemas, servidores, bases de datos e inclusive, en el ámbito del manejo y capacitación de sus recursos humanos.

A pesar, de ser de aplicación obligatoria y de control por parte de la CGE, ni técnica, ni económicamente es posible implementar todos los controles sugeridos en el Esquema de Seguridad (EGSI) del gobierno nacional, por lo que es necesario hacer partir del análisis de los riesgos para justificar la falta de controles que no están asociados al tamaño, objetivos y gestión propia de la organización y enfocarse en la implementación de controles que protegen de grandes impactos organizacionales sobre todo materiales y monetarios, que es lo que se observa en las acciones de control de la CGE.

Por lo expuesto anteriormente, con esta investigación se evalúa el cumplimiento tanto de la normativa emitida por la CGE, como la normativa estipulada en la estrategia de ciberseguridad del Ecuador, y a la necesidad institucional de evaluar el ambiente de control y la seguridad de tecnología de información mediante un estándar internacional en una institución con 1.100 funcionarios públicos, con aproximadamente 72.000 predios urbanos, más de 10.000 usuarios recurrentes de los servicios web, en el GAD municipal de Esmeraldas con una población de superior a los 190.000 habitantes en la ciudad y de aproximadamente 290.000 en el cantón.

Este trabajo de investigación contribuye a la línea de investigación “Desarrollo, aplicación de software y cybersecurity (seguridad cibernética)”, aprobadas el 05 de agosto de 2016 por la UTN, según Resolución No. 122-SO-HCU-UTN; entendiendo por Líneas de Investigación al proceso continuo de investigación relacionado directamente a un área del conocimiento y que se constituye en una propuesta institucional, para dirigir y orientar los procesos de investigación (Modificado de Barrera y Hurtado, 2002).

CAPITULO II
MARCO REFERENCIAL

2.2. Marco teórico

2.2.1. Antecedentes investigativos (Estado del Arte)

Urbanovics (2022), analiza y compara las estrategias de seguridad de los principales países de latinoamericanos, y de cómo estos empiezan a centrar cada vez más su atención al desarrollo de sus capacidades de ciberseguridad, creando su propia estrategia nacional de ciberseguridad. El artículo tiene un diseño de investigación basado en métodos mixtos, enfocado en su mayor parte en el análisis de datos secundarios extraído de bases de datos internacionales, así como el análisis sistemático de las estrategias aplicadas en estos países, mediante técnicas de análisis documental. Los resultados que presentan sintetizan las principales estructuras de estas estrategias, identificando patrones considerando el contexto político e internacional de la región.

En un estudio descriptivo Ramírez y Rincón (2022) identifican algunos aspectos relevantes de seguridad de la información y el gobierno de TI en el sector público colombiano, basado en las normas ISO 27001:2013; comparándolo con los otros países de América Latina. Así mismo, el estudio hace énfasis en el nivel de cumplimiento del Gobierno Digital y Seguridad Digital, en especial en algunas alcaldías municipales de sexta categoría; esta evidencia constituye un punto de partida para la región y sobre todo comparte las experiencias y mejores prácticas de municipios de ciudades intermedias en el ámbito seguridad de la información.

En un proyecto de investigación institucional desarrollado dentro del grupo de investigación y financiado por la Dirección de Investigación de la Universidad Técnica de Machala, Cartuche et al. (2020), basándose en el juicio de expertos en el área de IoT presentan como resultado del estudio realizado la definición de una taxonomía de seguridad IoT según la categorización de los diferentes tipos de amenazas existentes y el nivel de impacto de riesgo que estas generan sobre los diferentes activos de IoT, en la adquisición, el intercambio y el procesamiento de información, constituyéndose como un referente para ciudades que tienen infraestructuras consideradas de smart city y cuentan con muchos dispositivos de IoT que deben ser preservados y salvaguardados ya que son parte de la infraestructura tecnológica de las ciudades.

En Ecuador, como en muchos otros países, las entidades gubernamentales han reconocido la necesidad de adoptar políticas y procedimientos robustos que regulen y optimicen el uso de las TI en sus operaciones, “este impulso hacia la transformación digital ha llevado a la implementación de una serie de normativas y estándares, con el objetivo de fortalecer la infraestructura tecnológica y garantizar la seguridad de la información” (Aponte y Cuenca, 2021). Sin embargo, el mantener un ambiente de control seguro y confiable es el objetivo principal de las NCI (normas de control interno) de la CGE, y con la vigencia de la Ley Orgánica de Protección de Datos Personales se constituyen en el reto de todas las áreas de TI no solo en los gobiernos autónomos, sino en toda organización que maneje datos sensibles.

En el estudio cuantitativo de Solórzano et al. (2013) de la ESPOL, sobre el Estado del Arte de la Seguridad Informática en el pais y sus necesidades reales, se analiza el mercado nacional de los servicios de gestión de seguridad a nivel nacional y los productos de seguridad informática ofertados, encontrando en una de sus conclusiones que las empresas ecuatorianas no destinan el presupuesto necesario, ni asignan el personal adecuado para cumplir estas funciones (salvo las organizaciones del sector financiero). Sin embargo, después de la pandemia, y sobre todo con la masificación de los servicios web en todas las organizaciones gubernamentales, existe un presupuesto y recurso humano dedicado para la gestión de los riesgos de seguridad, de allí que la misma Contraloría ha incorporado en sus capacitaciones herramientas y metodologías de gestión de riesgo, Cobit 5, las normas ISO 27001, por citar un ejemplo.

Sánchez (2019) en su tesis de Maestría en Seguridad Informática Aplicada, realiza una planificación para la implementación de un esquema de seguridad utilizando las normas ISO 27001:2013, en donde se identifican las potenciales amenazas y riesgos que tiene el GIS del GAD de Samborondón, con el propósito proteger la información sensible que este tiene, sobre todo la relacionada con el catastro, ya que constituye la base de la emisión predial que tienen todos los municipios en el país. Este estudio rescata la importancia que tienen los catastros en las ciudades, constituyéndose por lo general uno de los activos más valiosos de un municipio, debido a que de este depende la base tributaria y la información contenida ahí constituye de mucha importancia para de desarrollo territorial de las ciudades.

Aguilar (2019), en la tesis de Maestría en Gerencia de Sistemas de Información de la Universidad Técnica de Ambato, realizada en el GAD de la Provincia de Orellana plantea como método científico el enfoque mixto, es decir cuali-cuantitativo. Al ser un gobierno local, se evalúa el cumplimiento de las normas 410-10, 410-11 y 410-12 de la Contraloría General del Estado, sin embargo, es solo un punto de partida, pues es necesario que el cumplimiento de la normativa se dé con un enfoque integral y en todos los ámbitos, es decir: organizaciones, físicos, de personal y tecnológico. La investigación se basó en los efectos o impactos de tienen los ataques informáticos en los servidores de Linux y la manera en que la institución implemento las contingencias y administro el soporte.

En la ponencia de la Escuela Superior Politécnica Agropecuaria de Manabí (ESPAM), titulada “Procesos de Tecnologías de la Información: Norma 410 de la CGE”, Cusme et al. (2020), compara lo establecido por la norma con los estándares internacionales más utilizados para la gestión de TI, como son la ISO27001, ITIL y COBIT 5, estableciendo un instrumento de evaluación en instituciones púbicas, a través método bibliográfico.

En la tesis de maestría de la Universidad Estatal de Milagro, Castillo (2022) propone una evaluación de riesgos basado en las vulnerabilidades detectadas utilizando las normas ISO/IEC 27001, mediante la determinación en cada componente y clausula, para según lo establecido por la norma establecer las acciones de mitigación y plantear un listado de recomendaciones que son de seguimiento obligatorio y están basadas en los hallazgos encontrados.

En la Evaluación Técnico Informática, realizada por Tusa (2021), al sistema de Axis Cloud, para establecer si el servicio de matriculación vehicular al que acuden decenas de personas al día en calidad de usuarios, se presta con eficiencia, eficacia y calidad. El investigador utiliza las buenas prácticas y procesos desarrollados, perfeccionados y publicados por ISACA, complementando la gestión de riesgo de seguridad con COBIT 5.0, para elaborar el informe con los hallazgos y las recomendaciones.

Villegas (2019) en su tesis de maestría, señala la necesidad de establecer una línea de base mediante una Evaluación Técnica Informática (ETI), y asegurar los activos de

información para brindar a la ciudadanía servicios adecuados. Se fundamenta en metodologías, estándares y buenas prácticas como son: ISACA, ISO, IEC, INEN. En este caso, en forma particular, utiliza la norma ISO-IEC-NTE-27001-2013. Como resultado de este trabajo se presenta un informe con el resultado de un 7% del cumplimiento de los controles, las observaciones y recomendaciones respectivas. Por lo que este trabajo es un referente considerando la aplicación de ese estándar en un GAD.

2.2.2. La seguridad de la información

Cuando se habla de seguridad de las Tecnologías de Información y Comunicación, a menudo erróneamente utilizan las palabras "información" e "informática" como si fuesen lo mismo, si bien ambos son importantes y similares, existen una gran diferencia entre ellos. Garre (2018) sostiene que es importante no confundir ambos términos, puesto que, si bien el primero engloba al segundo, estos dos términos no son sinónimos. La seguridad informática se ocupa únicamente de la seguridad de los sistemas de información y, por tanto, queda circunscrita al ámbito de la información automatizada, siendo por ello un término mucho más restrictivo que el de seguridad de la información. Hablar de seguridad de la información refiere hablar en todas las formas en que se presenta la información (oral, escrita, impresa o digital) y en cualquier momento de su ciclo de vida (creación o captura, mantenimiento, distribución y uso, y, almacenamiento, archivo y destrucción), para protegerla de cualquier amenaza que pudiera suponer pérdida o disminución del valor de la misma. Según Romero et al. (2018), Cuando se habla de seguridad, las tres características de la información que se definen a continuación, se convierten en los pilares de la misma

- **Confidencialidad**: consiste en que solo debe tener acceso quien tiene el rol y los permisos para acceder, es decir únicamente quien está autorizado tienen acceso a la información, esto implica el acceso únicamente de quienes están autorizados; por lo tanto, el acceso a la información es solo mediante autorización y de forma controlada.
- **Integridad:** garantiza que la información y los métodos de procesamiento de esta son completos y exactos. No pueden ser manipulados sin autorización, esto conlleva a la exactitud, lo que implica que la información solo se puede modificar mediante autorización; Por tanto, debe ser integral, completa, exacta, sin modificaciones, desde el origen hasta destino.

- **Disponibilidad:** La información permanece accesible mediante autorización. El objetivo de la disponibilidad es prevenir interrupciones no autorizadas del acceso a la información. Se dice que la información está disponible cuando su implementación y diseño permite deliberadamente negar el acceso a datos determinados.

No obstante, según Garre (2018), en los últimos tiempos se consideran que son cinco los pilares, al incluir (además de los tres anteriores) otras dimensiones de la seguridad como:

- **Autenticidad y no repudio**: Si la autenticidad prueba quién es el autor de un documento y cuál es su destinatario, el "no repudio" prueba que el autor envió la comunicación (no repudio en origen) y que el destinatario la recibió (no repudio en destino). Es decir, "existe garantía de la identidad (usuarios o procesos) que trata la información, y de la autoría de una determinada acción".
- **Trazabilidad:** Determina "quién ha sido el autor de cada acción", mostrando la ruta o secuencia de la acción.

Garre (2018), también señala que, puede ser útil, considerar la privacidad de la información, debido a que esta garantiza que solo las personas autorizadas tienen acceso a información de carácter personal. Se debe diferenciar que confidencialidad y privacidad, aunque están muy relacionadas, no son sinónimos; la privacidad se refiere únicamente a datos de carácter personal, que pueden ser, o no ser públicos; mientras que la confidencialidad se refiere información que no necesariamente es personal, y que la organización, por algún motivo, quiere proteger de ser difundida abiertamente. Por tanto, todas las dimensiones de seguridad son relevantes y se deben considerar por igual, su importancia depende del tipo de información que se maneje, esto tiene más relevancia ahora que ley establece sanciones al incumplimiento y mal manejo de la misma.

Aplicar el término de seguridad a la información, implica que dicha información "tiene una relevancia especial en un contexto determinado", por tanto, hay que protegerla; Se la puede definir como: "el conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su información" (Codolà Vilahur, 2018). Según Cruz Allende (2018), la define como un proceso en constante actualización y renovación, considerando que en la actualidad es

uno de los procesos con mayor importancia que se llevan a cabo en una organización, se deben tener en cuenta los riesgos y los objetivos de la organización, en caso contrario no se alcanzaran los resultados esperados.

Sobre seguridad informática, existen diferentes varias definiciones, la definición establecida por el estándar ISO 27001 y por la IEC señala que: “la seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, y puede, además, abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio” (ISO27001, 2022). En algunas publicaciones definen a la seguridad informática como sinónimo de ciberseguridad, pero según el reglamento (UE) 2019/881 de la Unión Europea define a la ciberseguridad como las actividades necesarias para proteger las activos de información de las amenazas. Como se ilustra en la figura 2.1, la relación que tienen estos términos.

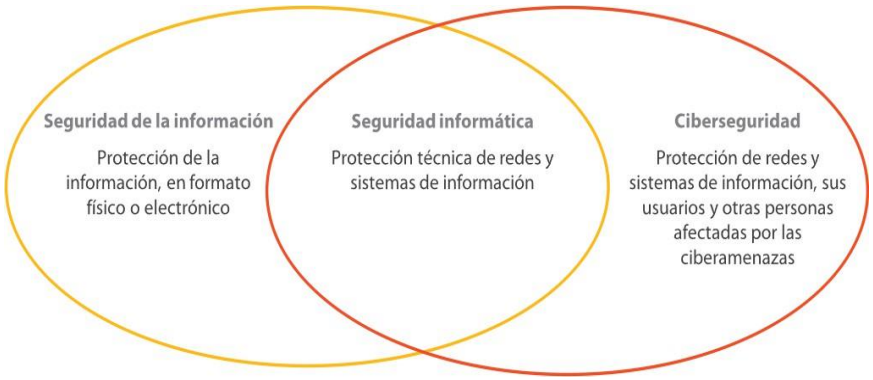


Figura 2.1. Ciberseguridad, seguridad de la información y seguridad informática

Nota: Tomado de ISO/IEC27001(2022)

La Seguridad de la Información, según ISO27001 (2022), se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: electrónicos, en papel, audio y vídeo, etc. Nasir et al. (2019) cita a la cultura de la seguridad de la información como “un patrón compartido de valores, modelos mentales y actividades que se intercambian entre los miembros de una organización utilizados a lo largo del tiempo, afectando la seguridad de la información”, otra definición es “el conjunto de percepciones, actitudes, valores, supuestos y conocimientos que guían a los seres humanos al interactuar con los activos de información en una organización con el objetivo de influir en el comportamiento de los empleados para preservar la seguridad de la información”.

2.2.3. Auditoria y evaluación de la seguridad de información

Trujillo et al. (2020) señala que no existe una única metodología para la ejecución de los trabajos de auditoría, sino que existen diferentes maneras de abordar las evaluaciones sin que ello signifique que no se tengan elementos suficientes para determinar cuál es la mejor alternativa para ejecutar las auditorias. De esta manera se brinda cierta libertad al auditor de TI para desarrollar su trabajo, dependiendo de su competencia y capacidad para ejecutar los trabajos de auditoría, de manera que se pueda lograr los objetivos que dieron origen a la auditoria. El trabajo de auditoría de la seguridad termina basándose entonces en una implementación de buenas prácticas, que teniendo en cuenta los casos de éxito, entreguen confianza para ser adoptadas en una organización.

La auditoría interna en un mundo globalizado, se centra como el estudio, análisis y evaluación permanente del control interno de los entes públicos o privados, y en las estructuras organizacionales por procesos o lineal, como un nivel de asesoramiento, es decir, en una asesora de la alta gerencia. De esta forma las entidades públicas y privadas que las requieren, delegan la administración del control a profesionales con conocimientos y habilidades en auditoría integral, a fin de que preparen informes periódicos dentro de un ejercicio fiscal con el objeto de alcanzar los objetivos y metas propuestas, cumpliendo los requisitos legales y reglamentarios vigentes aplicables en cada operación o actividad empresarial (Vásquez et al, 2023).

En el caso de Ecuador, es la CGE la institución encárgala de supervisar el buen uso de los bienes públicos, garantizando a la ciudadanía su uso efectivo. El artículo 18 de su propia Ley, estipula que la CGE debe ejecutar auditorias gubernamentales y exámenes especiales de manera inmutables, basada en técnicas y normas nacionales e internacionales (Caraguay, 2020). En el caso de las instituciones públicas y los gobiernos provinciales, la CGE establece la existencia de unidades de Auditoría Interna dentro de esas organizaciones, con la finalidad de evaluar la eficiencia del sistema de control interno, la administración de riesgos institucionales, la efectividad de las operaciones y el cumplimiento de leyes y regulaciones aplicables que permitan el logro de los objetivos institucionales, la protección de recursos y la generación de información oportuna y confiable (CGE, 2023), en el caso de los GAD municipales, estos equipos multidisciplinarios ya no forman parte de la estructura organizacional, y solo intervienen en exámenes especiales o intervenciones específicas de auditoria externa.

Otro reto importante que enfrentan los organismos de control en las organizaciones es hacer entender la importancia que tiene asegurar el proceso de TI con controles pertinentes que aporten a la eficacia de la Gestión en el área. Para esto, la comunicación entre estas dos dependencias (Auditoría Interna y TIC) es fundamental para dar a entender a la alta dirección de las compañías y en sí a todo el personal la importancia que tiene una adecuada gestión de la información (Chica, 2020). Sin embargo, en el caso de los municipios, al no tener unidades de auditoria interna desde hace algunos años, se suele contratar profesionales con experiencia en control interno para que realicen seguimiento o revisiones según sea el caso, pero es solo cuando existen exámenes especiales se suele evidenciar de forma muy general algún incumplimiento de la normativa.

La alta dependencia de TIC que tienen las organizaciones obliga a que se gestionen e implementen controles de seguridad que garanticen el uso adecuado de tecnologías bajo niveles de seguridad razonables. Esto representa a su vez un reto para las unidades de auditoría, pues en su rol de evaluación y control, son las llamadas a verificar el ambiente de control, incluyendo controles de TIC. Allí que, en la actualidad, existen varias metodologías y algunos marcos de referencia probados y establecidos como buenas prácticas, que facilitan los procesos de auditoría (Arief & Wahab, 2017), tal como se ilustra en la figura 2.2 en donde se puede visualizar y relación que tienen entre sí.

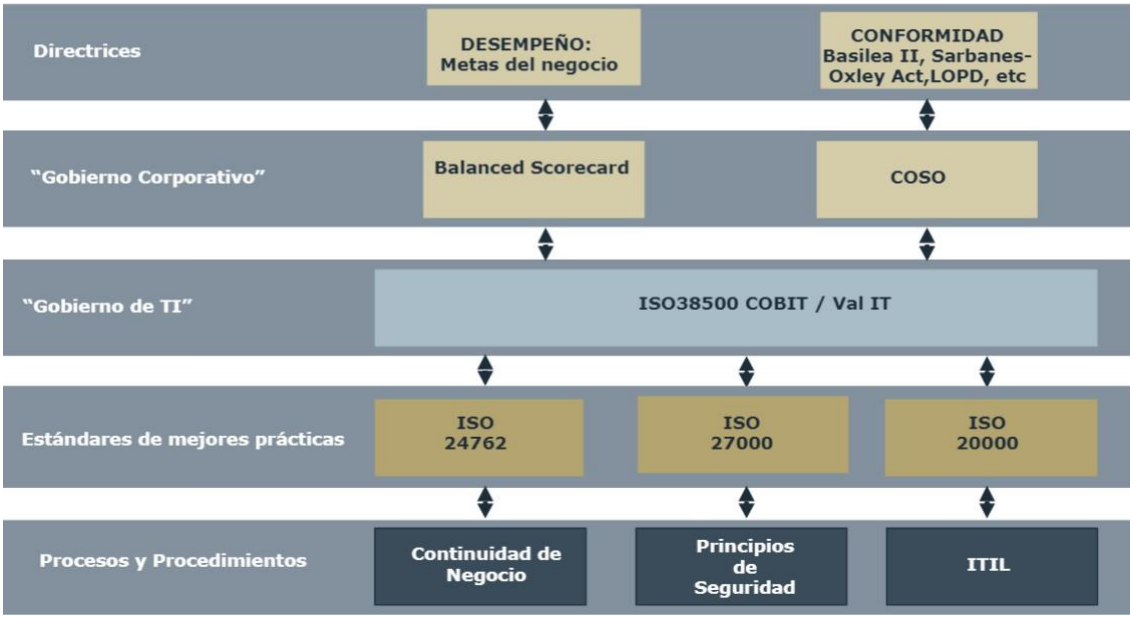


Figura 2.2. Estándares relacionados con la seguridad de la información

Nota: Tomado de ISACA (2012) y Ballester (2010)

Una vez seleccionado el estándar e identificados los puntos de necesidad de cumplimiento, se deben definir los planes de implementación o remediación necesarios, que deben incluir tanto a procesos, personas y tecnología. El resultado final debe aportar lo que se conoce como nivel de cumplimiento, con definiciones funcionales y técnicas que se verán representadas en el marco normativo. Se debe tener una visión global y multidisciplinaria, por lo que cada área de la organización debe participar en forma completa y desde sus funciones, tanto en actividades consultivas como operativas, según corresponda, y de acuerdo con sus alcances funcionales relacionados con el gobierno, riesgo y cumplimiento (Numpaque, 2021). Esto coincide con los controles establecidos por la ISO27001(2022) en sus cuatro secciones: Organización, personal, físicos y tecnológicos para establecer, implementar, mantener y mejorar continuamente el SGSI, y sobre todo considerando los requisitos obligatorios de la norma.

Otro estándar que puede ser implementado en las organizaciones es COBIT, el cual es un marco de referencia para organizar, desarrollar, e implementar estrategias en torno a la gestión de la información y su gobernanza (González et al., 2020). A través de este estándar, las organizaciones pueden determinar la madurez del sistema para los procesos gestionados por el área de TI. Para detectar este nivel de madurez, esta estándar entrega cinco principios básicos ilustrados en la figura 2.3, bajo los cuales se pretende abarcar el universo de TI de la empresa, pudiéndose aplicar tanto para gobierno como para gestión de TI (Arief y Wahab, 2017).

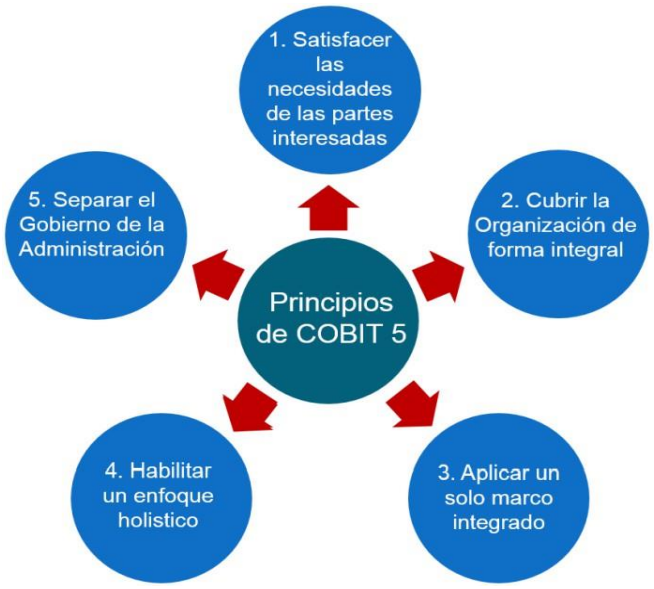


Figura 2.3. Principios del estándar COBIT 5

Nota: Tomado de ISACA (2012)

Definiciones, estándares, metodologías y guías coinciden en que las características de una auditoría de TI están estrechamente relacionadas con el aseguramiento de los controles de seguridad de la información y para esto no solo es necesario que la empresa tenga un adecuado estándar de seguridad implementado sino también que depende en gran parte de la competencia y capacidad tanto de auditores como de profesionales en la gestión para generar un trabajo conjunto que permita guiar los esfuerzos hacia el logro de los objetivos estratégicos de las organizaciones y en este caso específico hacia la continuidad del negocio (Gantz, 2013).

Para Chila (2020), la tendencia en las áreas de auditoría se está encaminando a incluir dentro de la planeación de sus trabajos el componente de seguridad de la información. En ocasiones, no se tiene claro de qué manera abordar este tipo de auditorías. Esta debilidad viene precedida por la ausencia de estándares implementados a nivel de gestión y gobierno por parte de las organizaciones. En este sentido, los trabajos de auditoría a la seguridad de la información no tendrían un criterio contra el cual contrastar la implementación de un sistema de gestión de seguridad de la información (SGSI), estándares como el ISO/IEC 27001 y COBIT presentan una guía importante para verificar la adecuación de las medidas de seguridad de la información.

Trujillo et al. (2020), concluye que las metodologías informáticas son guías para realizar las evaluaciones y tienen como resultado un diagnóstico y sugerencias de los auditores para lograr mejoras, su éxito depende, en gran parte, de la experiencia del auditor. Las buenas prácticas pueden apoyar a dar objetividad a las evaluaciones y las sugerencias finales de los informes de auditoría, debido a que son estas buenas prácticas y los estándares los que complementan las diferentes fases en las metodologías de auditorías informáticas para llegar a un fin en común: alinear las TIC al negocio con éxito.

Para Chica (2020), planear una auditoría a la seguridad de la información basada en la ISO 27001 es una buena decisión de las unidades de auditoría cuando se requiera verificar el grado de cumplimiento del SGSI, ya que, se puede encontrar una agrupación de procesos sistemáticos que entregan en cada etapa del ciclo Deming (cuyas siglas en inglés: PHVA, significan: Planificar, Hacer, Verificar y Actuar, y cuya estructura general se resume en la figura 2.4) integra los elementos fundamentales para garantizar que las organizaciones se encuentran aplicando adecuadamente controles de seguridad.

Figura 2.4. Estructura PDCA – ISO 27001

Nota: Tomado de ISO/IEC27001(2022)

A través de la auditoría se realiza el control del SGSI, y el enfoque que se utiliza se basa en un análisis de riesgos organizacionales. Se puede entender la auditoría como el proceso de acercamiento sistemático que se basa en la realidad comprobada para determinar la madurez del SGSI, verificando efectividad del SGSI, es decir el nivel de cumplimiento los controles. Los requisitos obligatorios de la ISO 27001:2022 que se deben cumplir, estas cláusulas no se pueden declarar como no aplicables. Las normas ISO 27001:2022 anexan 93 controles de seguridad a modo de buenas prácticas. La organización debe implementar estos controles, y tener la evidencia del cumplimiento del mismo, o en su defecto deberá justificar la "no implementación" de un control en particular. Existen diversos enfoques para llevar ejecutar con éxito un proceso evaluación. La organización deberá utilizar cualquier enfoque que se ajuste mejor a su circunstancia, debido a que en el caso de las ISO 27001, esta no dicta ningún método particular, la metodología de cómo evaluar el riesgo depende de la organización, lo que le permite ser complementada con otras metodologías o estándares.

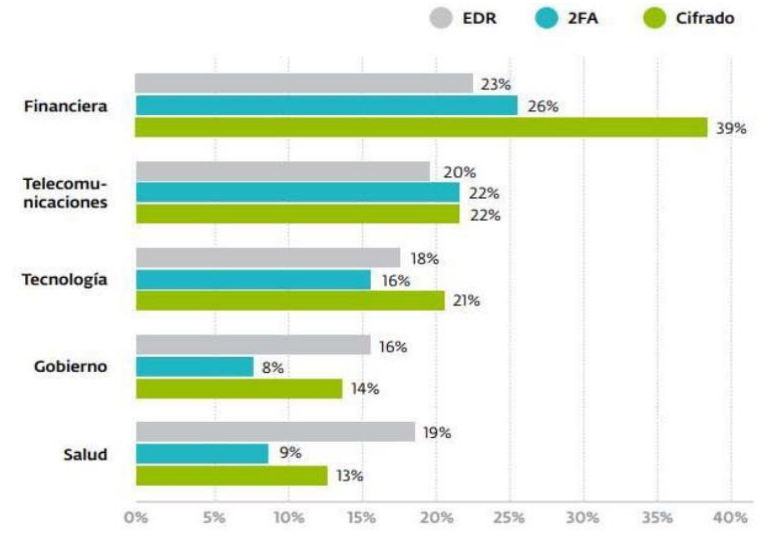
Según las ISO27001(2022) evaluar la seguridad, implica auditar el SGSI, para considerar la realización y frecuencia, se debe observar el riesgo del proceso o área a auditar, cualquier proceso de alto riesgo, ya sea porque tiene un alto potencial de fallo o porque las consecuencias serían graves en caso de fallo, deberá auditarse con mayor frecuencia que un proceso de bajo riesgo; La norma específica que los controles implementados dentro del alcance, los límites y el contexto de SGSI se deben basar en el riesgo, por lo que la aplicación de un proceso de gestión del riesgo en la seguridad de la información puede satisfacer este requisito.

Independiente de la metodología adoptada o el tipo de auditoría a desarrollar, toda evaluación de riesgos debe tener una fase de planeación y una fase de ejecución. En la fase de planeación, se determinan los riesgos que atentan contra la consecución de los objetivos. En este proceso se incluye también una revisión inicial de los controles identificados en la matriz. Finalmente, este análisis preliminar de los riesgos se enfoca, teniendo en cuenta los activos informáticos disponibles en las organizaciones y las vulnerabilidades, amenazas y riesgos que pudieran presentarse (Solarte et al., 2015).

2.2.4. Análisis y gestión de riesgos en las organizaciones

Tamayo et al. (2020) definen al riesgo como "Un fenómeno inherente a la humanidad y está presente en todas las esferas de la actividad humana, al punto de que no existe proyecto, empresa o decisión, que no sea ensombrecida por la presencia de uno o varios riesgos" (p.9).

En la figura 2.5 extraída del informe anual ESET (2020), se presenta el panorama en los sectores: financiero, de telecomunicaciones, tecnológico, gubernamental, y de salud de Latinoamérica, se evidencia que la adopción de mecanismo de protección en el sector financiero es mayor que el resto de sectores citados, esto se debe a las repercusiones que las afectaciones suelen ocasionar en sus estados de resultados, sobre todo cuando se obtienen pérdidas; ubicándose contraproducentemente en los dos últimos escaños, los sectores de salud y el gubernamental, siendo estos los llamados a liderar políticas públicas que precautelen el recurso más preciado: la vida.



Fuente: ESET Security Report 2019.
EDR: Endpoint Detection and Response, 2AF: Segundo factor de Autenticidad; Cifrado:

Figura 2.5. Medidas de protección de seguridad por sector en Latinoamérica

Según describe Cruz Allende (2018), el análisis de riesgos corresponde a la primera fase que una organización debe ejecutar para mejorar su seguridad, generalmente se relaciona al riesgo como algo aleatorio, pero esta percepción. “Un riesgo es una posible pérdida producida por eventos peligrosos e inciertos ligados a vulnerabilidades existentes” (Soler et al., 2018). Cruz Allende (2018) sostiene que el análisis de riesgos da respuesta a las tres interrogantes que una organización se hace en el ámbito de la seguridad, estas son:

- ¿Qué elementos de la organización hay que proteger o asegurar?
- ¿De qué peligros o de quién nos tenemos que proteger, y por qué?
- ¿Cómo nos debemos proteger?

Como respuesta a esta necesidad se crea el proceso de Análisis y evaluación de riesgos, la figura 2.6 ilustran el flujo de actividades que sigue esta metodología.

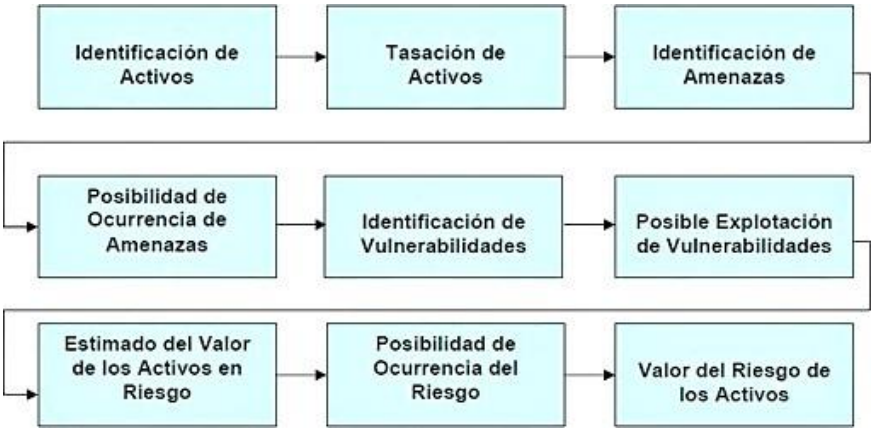


Figura 2.6. Proceso de Análisis y evaluación de riesgos

Codolà et al. (2018) señala que, dependiendo del enfoque de la organización, es posible ejecutar dos tipos diferentes de procesos: el análisis de riesgos intrínseco y análisis de riesgos residual, tal como se resumen en la tabla 2.1 que se presenta a continuación:

Tabla 2.1
Tipos de análisis de Riesgos

Tipo	Descripción
Intrínseco	se realiza sin tener en consideración las diferentes medidas de seguridad que ya están implantadas en una organización. Este proceso da como resultado un riesgo intrínseco
Residual	se realiza teniendo en consideración las medidas de seguridad que la organización ya tiene implantadas. Como resultado de este proceso se obtiene un riesgo real

Para un mejor entendimiento de las actividades relacionadas a la gestión de riesgos, es necesario la comprensión de los siguientes conceptos:

- **Activo:** Según la ISO 27001:2022 “es algo que una organización valora y por tanto debe protegerse”. Es decir, cualquier recurso que genere valor a la organización se puede considerar como activo.
- **Amenazas:** causa potencial de un incidente que puede afecte negativamente a una organización. Puede ser de origen natural, de origen industrial o del entorno, por defectos de aplicaciones, causadas por personas de forma accidental, y de forma delibrada. (Ministerio de Hacienda y Administraciones Públicas, 2016).
- **Vulnerabilidad:** Es toda debilidad o fallo aprovechada por una amenaza. Son las debilidades de los activos de información que facilitan el éxito de una amenaza potencial (Ministerio de Hacienda y Administraciones Públicas, 2016).
- **Salvaguardas**: también conocidas como contra medidas o controles de seguridad, son todas aquellas acciones de protección utilizadas para minimizar el efecto de las amenazas. Magerit la define como los procedimientos tecnológicos que reducen el riesgo. (Ministerio de Hacienda y Administraciones Públicas, 2016). Existen dos tipos de salvaguardas: preventivas (aquellas que reducen las vulnerabilidades), y correctivas (aquellas que reduce el impacto de la amenaza).
- **Impacto:** es el resultado de un suceso que afecta a los activos. (Ministerio de Hacienda y Administraciones Públicas, 2016). Para Imbaquingo et al. (2017) es la magnitud de daño a raíz de un ataque, es decir son las consecuencias que se producen en la organización cuando una amenaza aprovecha una vulnerabilidad para dañar a un activo.
- **Riesgo:** Imbaquingo et al. (2017) señalan que es la posibilidad de que una amenaza se materialice causando daños. Tal como se ilustra en la figura 2.7, el riesgo consiste en la relación que tiene estos tres primeros conceptos, los cuales al combinarlos entre sí dan origen a los diferentes tipos de riesgos a los que se expone una organización.

Figura 2.7. Relación entre el activo, amenaza y vulnerabilidad

La gestión de riesgos es un conjunto de actividades planificadas para minimizar las pérdidas ocasionadas debido a la concepción de riesgos en una organización (Soler et al., 2018). Según ISO 27001 (2022) el diagrama de flujo de la figura 2.8 se representa la gestión de riesgos, conformado por: el establecimiento del contexto, la evaluación del riesgo, el tratamiento del riesgo, la aceptación del riesgo, la comunicación del riesgo y monitoreo, y por último la revisión del riesgo;

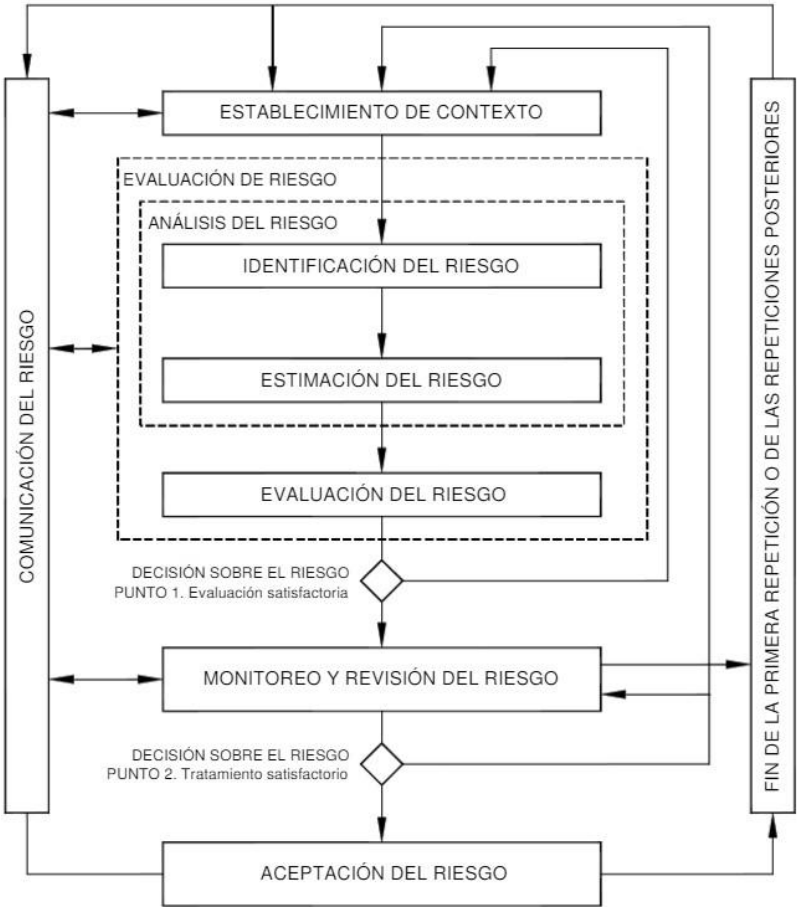


Figura 2.8. Proceso de gestión del riesgo de seguridad de la información

Nota: Tomado de ISO/IEC27001(2022)

Siendo el sistema de gestión de la seguridad de la información (SGSI) el elemento central de la ISO 27001, unificando criterios para la evaluación de los riesgos asociados a la administración de la información institucional. Según la ISO7005(2022) el proceso de gestión de riesgos es una aplicación sistemática de políticas, procedimientos y prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto e identificación, análisis, evaluación, tratamiento, seguimiento y revisión de riesgos. Esto implica: Evitar el riesgo al decidir no iniciar o continuar con la actividad que da lugar al riesgo; Asumir o aumentar el riesgo para aprovechar una oportunidad;

Eliminar la fuente del riesgo; Cambiar la probabilidad y las consecuencias; Aceptar el riesgo, para asumir un riesgo particular sin tratamiento o durante el proceso de tratamiento; Compartir el riesgo, es decir la distribución acordada del riesgo con otras partes; y, Retener el riesgo, es decir aceptar temporal el beneficio potencial de la ganancia, o la carga de la pérdida, de un riesgo particular.

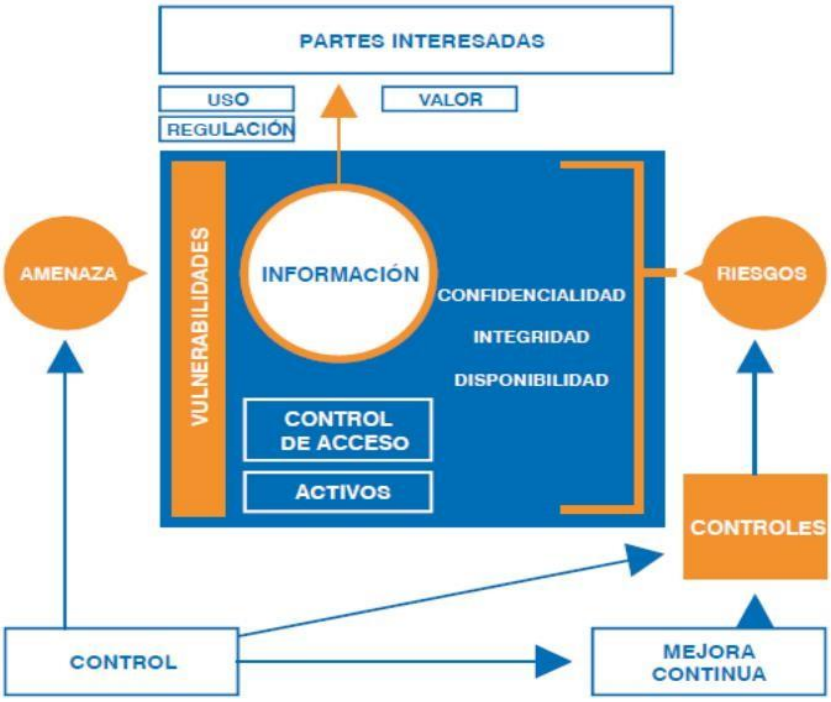


Figura 2.9. Esquema gráfico del modelo para la gestión de riesgos en un SGSI

En la figura 2.9 que antecede, se presenta un esquema gráfico del modelo, en el cual se interrelaciona los requisitos obligatorios de un SGSI, controles establecido en el anexo A de la norma 27001 y los riesgos, de las amenazas y vulnerabilidades, considerando los principios del sistema para la protección de los datos de la norma ISO27005. Las razones de que una organización no realice una correcta gestión de los riesgos son: la inmadurez, desinformación o desconocimiento de los beneficios que este proceso conlleva (Castro et al., 2020).

2.2.5. Metodologías de gestión de riesgos

Las normas ISO proponen a las organizaciones una forma de identificar el grado de cumplimiento, sin embargo, no brindan un método con los pasos o procedimientos específicos para cumplir con los objetivos que se han definido. Debido a que existen diversas metodologías de análisis de riesgos, en la tabla 2.2, se resume un comparativo de las metodologías más utilizadas:

Tabla 2.2

Resumen comparativo de metodologías utilizadas para la gestión de riesgos

Estándar	Ámbito de aplicación	Ventajas	Desventajas
OCTAVE	Pymes, organización públicas y privadas	Es auto dirigible. Se puede desarrollar con personal interno. Involucra a personal de todas las áreas. Construye perfiles basados en activos. Identifica infraestructura de vulnerabilidades. Desarrolla planes y estrategias de seguridad. Comprende etapas de gestión de riesgos. Relaciona amenazas y vulnerabilidades. Gratuita para uso interno	No tiene en cuenta el principio de no repudio. Requiere demasiada documentación. Requiere de amplios conocimientos técnicos. No define claramente los activos de información. Usa licencia si se quiere implementar a un tercero.
MAGERIT	Gobierno, corporación, compañías grandes, comerciales, Pymes.	Alcance completo de gestión de riesgos. Buena documentación Análisis cualitativo y cuantitativo. No requiere autorización para su uso. Prepara para procesos de evaluación, auditoria, certificación o acreditación. Efectiva con procesos bajo control en todo momento. Posee una buena base documental de acceso público. Posee una herramienta (PILAR).	En su modelo no involucra los procesos, recursos, ni vulnerabilidades. Posee falencias en el inventario de políticas. Se considera una metodología costosa en su aplicación.
MEHARI	Gobierno, organismos, empresas grandes y medianas, compañías comerciales y sin fines de lucro (educación, salud, ONG, públicas y privadas)	Utiliza un modelo cualitativo y cuantitativo Método para evaluar y disminuir riesgos en función del tipo de organización. Posee bases de datos de conocimientos con manuales, guías y herramientas, Compatible con ISO 27001, 27002 y 27005. Permite la detección de vulnerabilidades mediante auditorias Combina análisis y evaluación de riesgos. Posee un módulo de evaluación rápida y uno de evaluación lenta.	Se enfoca solo en los principios de integridad, confidencialidad y disponibilidad olvidando el no repudio. La recomendación de los controles no se incluye dentro de análisis sino dentro de la gestión de los riesgos. El impacto de los riesgos se estima en el proceso de gestión y evaluación.
NIST SP 800-30	Gobierno y ONG	Bajo costo relacionado con el riesgo analizado y solventado. Guía para la evaluación de riesgos de seguridad en las infraestructuras de TI. Presenta un resumen de los elementos claves de las pruebas de seguridad	No tiene contemplados elementos como los procesos, los activos, ni las dependencias. Solo cuenta con un tipo de anales Limitaciones con el idioma de las guías.

		Provee herramientas para la valoración y mitigación de riesgos. Asegura los sistemas informáticos Administración a partir de los resultados	
ORAS	Sector Público	Herramientas de apoyo: un editor gráfico y utiliza lenguaje basado en UML. Provee un repositorio de paquetes de experiencias reutilizables. Provee un reporte de vulnerabilidades encontradas. Útil en el desarrollo y mantenimiento de nuevos sistemas. Basada en modelos de riesgos de sistemas de seguridad críticos.	No realiza análisis de riesgo cuantitativo En su modelo no tiene contemplados elementos como los procesos y las dependencias.
CRAMM	Organización pública y privada	Aplica los conceptos de manera formal, estructurada y disciplinada Análisis de riesgos cualitativo y cuantitativo. Aplicable a todo tipo de sistemas y redes. Aplicable en todas las etapas del ciclo de vida del sistema de información. Identifica la seguridad y/o requisitos de contingencia para un SI o de la red. Identifica y clasifica los activos de TI Identifica y evalúa amenazas y vulnerabilidades. Evalúa niveles de riesgo e identifica los controles requeridos. Compuesta por más de 4.000 contramedidas.	En su modelo no tiene contemplados elementos como los procesos y los recursos.
EBIOS	Utilizada ampliamente en el sector público (ministerios) y en el sector privado en pequeñas y grandes empresas	Ayuda a tener un mayor reconocimiento en sus actividades de seguridad. Compatible con normas internaciones como la ISO. Es una herramienta de negociación y de arbitraje. Es utilizada para múltiples finalidades y procedimientos de seguridad. Herramienta de código libre y reutilizable. Se acopla al cumplimiento de los estándares ISO 27001, 27005, 31000. Posee una base de conocimientos	Se constituye más como una herramienta de soporte.

Nota: Tomado de Novoa, H. y Rodríguez, C. (2022), y Rodríguez y Sepúlveda (2023)

Sevilla (2023) señala como las más destacables a: OCTAVE, MAGERIT, CRAMM, sin embargo, independientemente de la metodología que se utilice, es necesario analizar y evaluar los riesgos que presentan los activos de información. Cruz Allende

(2018) asegura que el resultado de los análisis con todas las metodólogas será similar, ya que todas se fundamentan en los mismos elementos.

2.2.6. Control interno y sus normas en el Ecuador

La Contraloría lo define al control interno como "un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos públicos" (CGE, 2019). Está constituido por cinco componentes: ambiente de control, evaluación de riesgos, actividades de control, sistemas de información, y seguimiento o monitoreo (Vásquez et al. 2023), estos componentes relacionados entre si son los que conforman el denominado sistema de control interno.

Para Mendoza et al. (2018), el control interno se ha convertido para las organizaciones en uno de sus pilares más importantes, porque a través del cumplimiento de controles y las leyes permite determinar el grado de eficacia y eficiencia del ambiente de control para así aplicarlas en los procesos productivos. Por su parte Mendoza et al. (2023) señalan que la inexistencia de un sistema de control interno en de las instituciones del sector público, es la principal causa de registros inadecuados, improvisación administrativa y una gran cantidad de errores que inciden directamente en la calidad de la información presentada en los estados financieros.

La CGE (2023) ha desarrollado normas generales y otras específicas relacionadas con las áreas de talento humano, administrativa, finanzas, tecnologías y gestión ambiental; en base al marco de referencia emitido por el Comité de Organizaciones Patrocinadoras de Comisión Treadway (COSO), cuyo objetivo es ayudar a las organizaciones a cumplir sus objetivos. Por lo tanto, estas normas propician el mejoramiento del ambiente de control y la gestión pública, en relación con la consecución de los objetivos organizacionales y el manejo de los recursos públicos. En el caso de la norma 410, que regula la tecnología de información, establece en la subnormal 410-1: "que las entidades y organismos del sector público deben estar acopladas en un marco de trabajo para procesos de tecnología de información que aseguren la transparencia y el control, así como el involucramiento de la alta dirección" (CGE, 2023). Es decir que los procesos tecnológicos deberán estar a cargo de una unidad que regule y estandarice esos temas.

La CGE (2023) establece que la máxima autoridad de cada entidad es responsable de establecer las medidas de control y líneas de conducta para alcanzar los objetivos institucionales alineado con en el plan de desarrollo del país, para lo cual “mantendrá un ambiente de confianza basado en la seguridad, integridad y competencia de las personas; de honestidad y de respaldo hacia el control interno; así como, garantizará el uso eficiente de los recursos y protegerá el medio ambiente” (CGE, 2023). Es decir, la máxima autoridad de cada organización y su equipo directivo son las responsables del sistema de control interno; y en conjunto con todo el personal: “establecerán los mecanismos para identificar, analizar, valorar y responder a los riesgos a los que está expuesta la organización para alcanzar sus objetivos, cumplir las disposiciones legales, proteger los recursos públicos y generar información oportuna y confiable” (CGE, 2023).

2.2.7. Auditoria de protección de datos

Según la AEPD (2021), uno de los principales objetivos de la auditoria en protección de datos personales, es verificar la adaptación de las organizaciones a las obligaciones impuestas en la normativa vigente; por tanto, lo habitual en una auditoria o evaluación será determinar las posibles debilidades e incumplimientos, en aras de verificar el principio de responsabilidad proactiva a través de mecanismos que permitan tomar decisiones en el nivel respectivo y con la información suficiente determinar el grado de cumplimiento de la normativa. Para esto es necesario una correcta formación del recurso humano, debido a que la implementación las política y normas dependerá en gran medida de los mismos funcionarios y ciudadanos, quienes juegan un papel decisivo a nivel organizacional. Martínez (2021) sostiene que existen aspectos técnicos o de seguridad que son necesarios considerar para cumplir la ley, pero son las instituciones las que deciden el momento y contexto en que implementan los estándares, y en qué actividades de tratamiento deben ser implementadas. Algunos de estos aspectos técnicos son: controles para la continuidad de servicios y de contingencias; protección de sitios web, Cortafuegos y seguridad perimetral; cifrado de información digital, copias de seguridad y actualización de sistemas; sistemas de control de accesos y gestión de usuarios; gestión de brechas de seguridad; y por último, pero no menos importante: los controles informáticos para el aseguramiento de la información.

Las organizaciones deben realizar de forma periódica auditorias para determinar de cumplimiento de la ley del mismo para evaluar su nivel de cumplimiento y seguridad

de la privacidad y protección de información personal. En la figura 2.9 se grafica la estructura de la auditoría a la protección de datos personales, estas auditorías “deben proporcionar una visión independiente sobre el nivel de adecuación de los responsables y encargados de tratamientos a la legislación y normativas relativas a la protección de datos personales de los ciudadanos” (Martínez, 2022), por tanto se debe priorizar evaluar los controles y los riesgos que inciden sobre la protección de los datos personales que ha sido definidos e implementados por la institución.

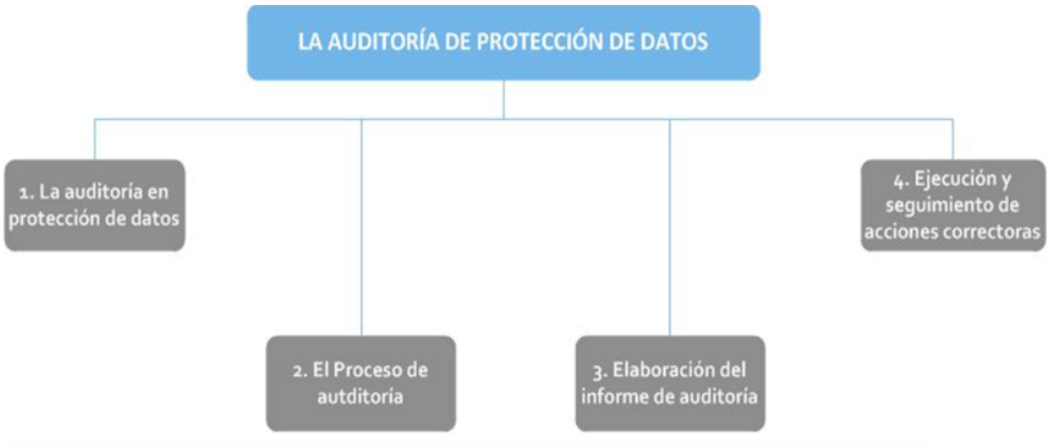


Figura 2.10. Mapa conceptual de la Auditoria de datos personales

Nota: Tomado de Euroinnova (2024)

La auditoría debe incluir las medidas, legales, técnicas y organizacionales, así como de las políticas y procedimiento que regulan la función del responsable del tratamiento en materia de protección de datos personales en la institución; debe realizarse periódicamente. En la figura 2.9 se agrupan los dominios funcionales que se deben considerar en el desarrollo de la auditoria de protección de datos.

Figura 2.11. Dominios funcionales de la Auditoria de protección de datos

Euroinnova (2024) establece que la auditoría se dará por finalizada, una vez se cumplan todas las actividades planificadas, o según lo establecido en el programa de auditoria acon el responsable del tratamiento, quien acuerdo a eso deberá conservar o eliminar la documentación relativa al proceso ejecutado; y realizará una exposición analítica y depurada de los principales hallazgos, observaciones y conclusiones recogidos en el informe final. Es recomendable que los resultados se comuniquen al DPO o al director del área de TIC en caso de que no se haya nombrado un delegado. Posteriormente, los resultados deberán ser comunicados a la máxima autoridad, basado en el estatuto de la institución. Para evidenciar que los resultados han sido conocidos, comprendidos y aceptados, es necesario documentar con firmas de asistencia los participantes a la reunión lectura del informe a través un acta.

Según Euroinnova (2024), como consecuencia de la etapa anterior, resulta habitual que se establezca el compromiso y las tareas de seguimiento que deberán ser realizadas por la institución, con el objetivo tomar correctivos e implementar controles; para esto se deberán basar en recomendaciones incluidas en el informe final. Por lo tanto, será necesario estimar para dichas tareas: la fecha de ejecución, responsables de ejecución, supervisión y seguimiento, estas nuevas las actividades pendientes podrán incorporarse como parte de un plan de mejora continua en la institución, o podrá verificarse en una auditoria subsecuente en donde será obligatorio constatar el seguimiento de las recomendaciones y el cierre final de las actividades pendientes, es decir el cumplimiento de las mismas.

2.2. Marco legal

2.2.1. Normas Nacionales

Para el BID y OEA (2020) la Ley N.º 2002-67 sobre comercio electrónico, firma electrónica y mensajes de datos describe de forma completa la normativa que rige el delito cibernético y señala las reformas pertinentes del Código Penal, puntualmente los artículos 229 a 234 del Código Penal constituyen el marco de referencia para el tratamiento de los delitos contra los activos de información.

En la LPDP (2021) se establece que los controles de seguridad deben ser implementadas por los DPO, o por quien establezca el estatuto orgánico funcional, debido a que es una responsabilidad de la institución a todo nivel. El incumplimiento de esta ley

implica sanciones, y las medidas legales que esta ley recoge son: tratar los datos personales; cumplir con el deber de transparencia hacia la parte interesada; gestionar el ejercicio del derecho de los interesados; regularizar las relaciones de corresponsabilidad; regularizar las relaciones de encargado del tratamiento; disponer del registro de actividades del tratamiento; implementar medidas de comunicación a la autoridad de control ante la violación de la seguridad la información; y, contar con un responsable o delegado de protección de datos personales.

La CGE (2019), emitió las Normas de Control Interno, con el objetivo de asegurar la correcta y eficiente administración de los recursos públicos; Esta normativa esta está orientada a "cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información" (CGE, 2023), por tanto, establece las condiciones adecuadas para ejercer control y corregir las deficiencias organizacionales.

Según el MINTEL (2019), la LOSNRDP (Ley Orgánica del Sistema Nacional de Registro de Datos Públicos), establece que los datos personales deben ser tratados de manera que se garantice la aplicación de medidas técnicas u organizativas apropiadas para evitar su pérdida, destrucción o daño accidental. El tratamiento de datos "se compone de la obtención, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción de datos personales" (MINTEL, 2019).

El 10 de enero de 2020 bajo Acuerdo Ministerial No. 25 –2019, el MINTEL expidió el EGSI (Esquema Gubernamental de Seguridad de la Información), el cual es un marco de referencia basado en las normas ISO 27001; de implementación y aplicación obligatoria para las instituciones públicas (MINTEL, 2020). Las normas técnicas nacionales relacionadas con el presente trabajo de investigación, de acuerdo con la CGE(2023), es la norma 410 bajo el título: TECNOLOGÍA DE LA INFORMACIÓN establece la normativa respectiva a través de 17 subnormas, que están codificadas desde la 410-01 hasta la 410-17, para asegurar un ambiente de control adecuado en las instituciones públicas, de las cuales las sub normas 410-11, 410-12 y 410-17 han sido resumidas en la tabla 2.3, por estar relacionadas directamente con el tema.

Tabla 2.3
Descripción de NCI 410 relacionadas a la seguridad de información

Subnorma	Descripción de la norma
410-11: Seguridad de tecnología de información	La unidad de TIC debe garantizar el cumplimiento de la normativa de protección de datos personales, propiedad intelectual del software, seguridad de la información, utilización de estándares, sistemas o plataformas establecidas para el sector público, y estarán alineadas a los objetivos de la organización, a los principios de calidad de servicio, y constarán en el plan informático y en el plan anual de contrataciones aprobado de la institución. Las entidades de la administración pública implementarán una política de seguridad de la información sobre la base de las disposiciones legales y reglamentarias.
410-12: Plan de contingencias	Establece que corresponde a la unidad de TIC la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.
410-17: Firmas electrónicas	Establece los funcionarios titulares de certificados de firma electrónica y dispositivos portables seguros son responsables de su buen uso y protección.

Nota: Tomado de CGE(2023)

La CGE (2023), en la norma de control interno 500, establece que la máxima autoridad en coordinación con la Dirección de TI o el Comité de TIC, deben definir las características para gestionar de manera oportuna (identificar, capturar, clasificar y comunicar) la información, con la finalidad que los funcionarios cumplan sus responsabilidades. Los sistemas de información serán manuales o automatizados según la naturaleza y tamaño de la organización, y mantendrán controles apropiados que garanticen la integridad y confiabilidad de la información. El usar sistemas informáticos para procesar la información implica considerar riesgos asociados principalmente con la era digital, por lo que se deben implementar controles generales, de aplicación y de operación que garanticen la protección de la información según su grado de sensibilidad y confidencialidad, así como su disponibilidad, accesibilidad y oportunidad. En resumen, hace referencia a contar con un SGSI que asegure el cumplimiento de la normativa legal vigente.

2.2.2. Normas Internacionales

Según Enríquez (2021), “el Reglamento General de Protección de datos (RGPD) cambió al mundo”, y la aplicación directa y alcance extraterritorial hacen que las organizaciones en todo el mundo deban cumplir con las obligaciones en él establecidas, incluido el Ecuador, el RGPD elaborado y aprobado por la Unión Europea es fruto de una larga evolución de más de cuatro décadas, influenciando en la mayoría de regiones del mundo, entre ellas América Latina.

Las normas ISO 27000 constituyen un conjunto de normas desarrolladas para facilitar un marco regulatorio de seguridad de la información aplicable a cualquier tipo de entidad, sea esta pequeña o grande, pública o privada; debido a la gran cantidad de su taxonomía, en la tabla 2.4, se resumen aquellas normas fueron revisadas en esta investigación, siendo en la actualidad la norma ISO 27001, el referente mundial para que una organización certifique su SGSI, y la ISO 27005 la norma utilizada para gestionar los riesgos de seguridad de la información.

Tabla 2.4
Descripción de Familia de Normas ISO 27000

Norma	Descripción del estándar
ISO 27001	Es el qué hacer: te dice qué controles debes tener para proteger tu información e implementar un SGSI.
ISO 27002	Es el cómo hacerlo: cómo llevar a la práctica los 114 controles de seguridad del Anexo A.
ISO 27003	Consiste en una guía de implantación de SGSI del empleo del modelo PDCA y los requisitos de sus etapas.
ISO 27004	Establece las técnicas aplicables para la determinación de la eficiencia de un SGSI y sus controles.
ISO 27005	Establece los principios para la gestión del riesgo en la seguridad de la información. Diseñada para ayudar a la aplicación de la seguridad de la información en el enfoque de gestión de riesgos.
ISO 27006	Establece los requerimientos de la acreditación de entidades auditoras y certificaciones de SGSI.
ISO 27007	Consiste en una guía para la auditoría, proporciona directrices para llevar a cabo la auditoría de un SGSI en las organizaciones.
ISO 27011	Es una guía de gestión de la seguridad de la información para las telecomunicaciones junto con ITU.
ISO 27015	Guía de SGSI orientada a organizaciones del sector financiero y de seguros
ISO 27017	Guía de seguridad para Cloud Computing.
ISO 27031	Recoge los principios y conceptos sobre las TIC con el objetivo de asegurar la continuidad de negocio a cualquier tipo de organización
ISO 27032	Guía vinculada a la ciberseguridad, es un marco para mejorar la seguridad en Internet, e intentar garantizar un entorno seguro.
ISO 27033	Esta norma da una guía detallada de seguridad de la administración, operación y uso de las redes. Se destina a la gestión de la seguridad.
ISO 27034	Guía de seguridad en aplicaciones, proporciona orientación sobre el diseño, selección, especificación y aplicación de los controles.
ISO 27035	Guía sobre la gestión de incidentes de seguridad en la información.
ISO 27036	Guía en cuatro partes de seguridad en las relaciones con proveedores.
ISO 27037	Directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales dispositivos móviles.
ISO 27040	Guía de seguridad para los sistemas y ecosistemas de almacenamiento, así como para la protección de datos.
ISO 27045	En desarrollo, cubrirá procesos de seguridad y privacidad en sistemas de big data.
ISO 27070	Establece requisitos de seguridad para establecer raíces de confianza para la provisión de entornos informáticos confiables.

Nota: Tomado de ISO27001security (2022)

CAPITULO III
MARCO METODOLÓGICO

3.1. Descripción del área de estudio / Descripción del grupo de estudio

La presente investigación se llevó a cabo en el Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas (GADMCE), cuyo edificio principal se encuentra ubicado en la calle Olmedo y Juan Montalvo del cantón Esmeraldas de la Provincia de Esmeraldas, tal como lo ilustra la figura 3.1 en el mapa.

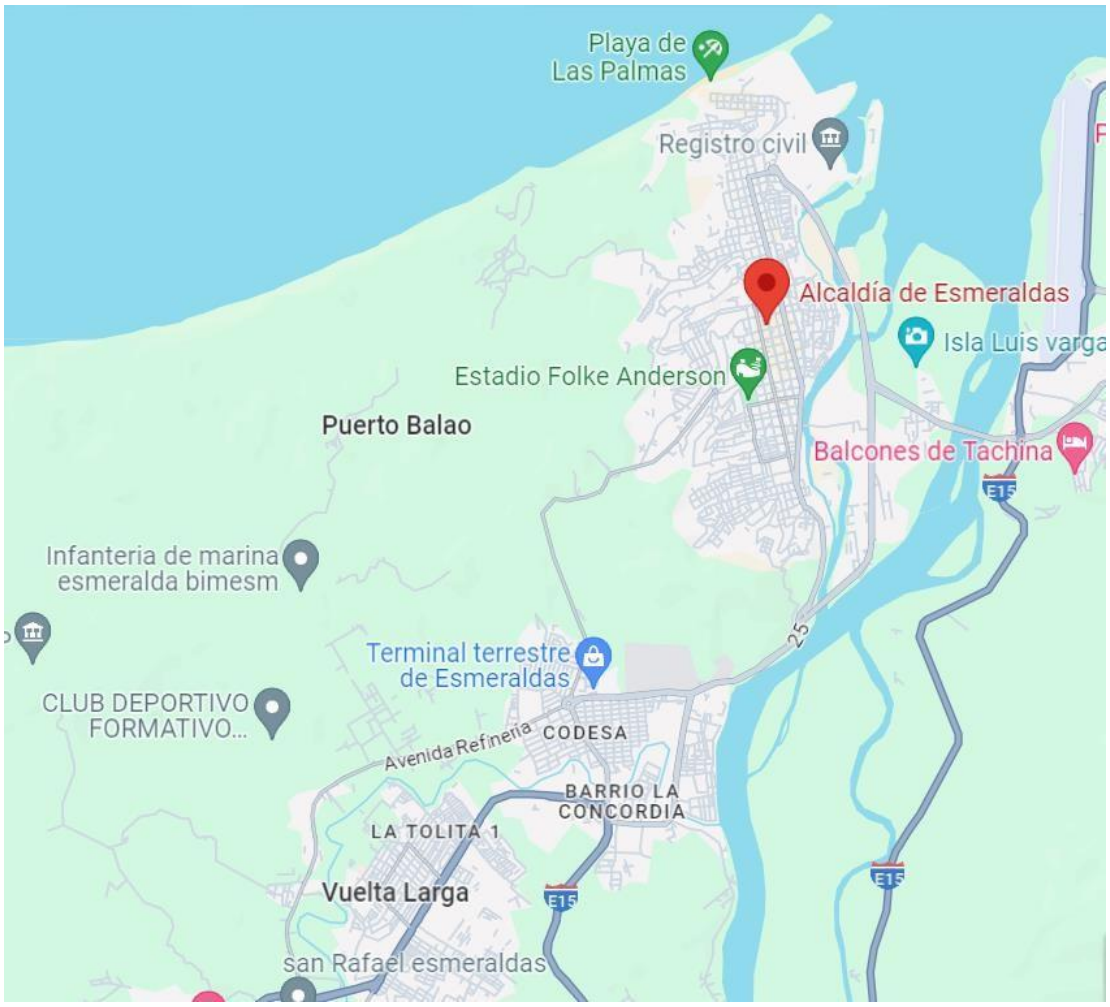


Figura 3.1. Ubicación del área de estudio adaptado del mapa de Google 2024

Nota: Tomado de Googlemaps (2024)

Los GAD municipales son esenciales en el desarrollo del territorio y en el mantenimiento de las infraestructuras con las que se atiene a las ciudades y vincularlas con sus territorios circundantes. Asimismo, pueden crear normativas y realizar controles ambientales para promover las industrias sostenibles y potenciar las organizaciones de economía popular y solidaria. De allí que la Alcaldía de Esmeraldas debe ejecutar:

propuestas para desarrollar infraestructuras fiables, sostenibles, resilientes y de calidad, que apoyen el desarrollo económico y el bienestar humano, con acceso igualitario y asequible para todos y todas; acciones para aumentar el acceso a la TIC para facilitar acceso universal al internet y a la información; e, Iniciativas para fortalecer los sistemas y políticas científicas, tecnológicas y de innovación.

Según el GADMCE (2021), en el PDOT vigente existe el sistema de conectividad, que puntualmente contempla el uso de las tecnologías de la información y comunicación para mejorar la calidad de vida de los ciudadanos mediante el uso de sistemas de información y aplicaciones que faciliten los trámites que los ciudadanos realizan en la Alcaldía, evitando colas y trámites presenciales innecesarios en las instalaciones, que generan saturación y hacinamiento de personas en las dependencias.

Según su misión definida, el GADMCE es una institución que planifica el desarrollo cantonal y genera confianza por su capacidad resolutiva para la prestación de servicios públicos de calidad a la población esmeraldeña. Municipalidad que apoya el desarrollo económico local y coadyuva a mantener el equilibrio del ambiente, su biodiversidad y pluriculturalidad; proyectada en función de los cambios y exigencias de la sociedad actual (GADMCE, 2020). Dentro de su estatuto orgánico funcional por procesos consta la Dirección de TIC, cuya misión es: Evaluar, planificar, implementar, soportar y monitorear las TIC para satisfacer los objetivos institucionales y soportar los avances tecnológicos mediante la integración productos y servicios que aseguren eficiencia operacional, la continuidad de servicios, la transparencia y el control en la institución GADMCE (2019); la dirección está en un nivel que permite asesorar a la alta dirección y demás unidades usuarias, la figura 3.2 ilustra los subprocesos conforman la dirección de TI.

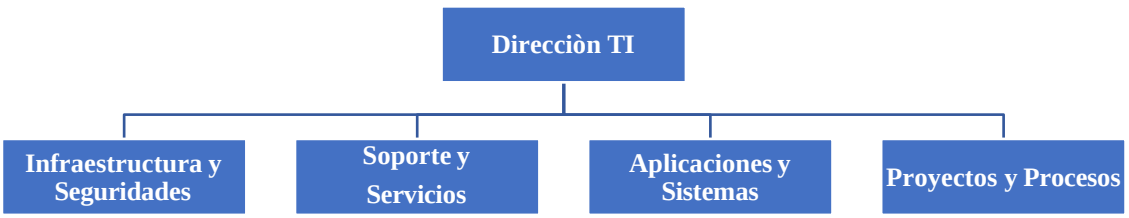


Figura 3.2. Estructura de la Gestión de TIC del GADMCE

Actualmente hay un parque informático de 390 equipos de cómputo y 60 impresoras, con los que unos 350 usuarios operan los diversos sistemas y aplicaciones,

distribuidos en 14 edificios para cumplir con las funciones municipales que permiten atender a una población de alrededor de 200 mil habitantes según la proyección INEC (2021), tanto en los trámites municipales como en los servicios públicos que se entregan a diario, teniendo como base predial unos 72 mil predios entre urbanos y rurales.

La población objeto de estudio estuvo conformada por 289 funcionarios públicos que laboran en la institución como usuarios administrativos de los sistemas de información, infraestructura tecnológica y demás activos informáticos de la institución; y los 22 miembros de la Dirección de Tecnologías como parte del SGSI, debido a que son en gran medida los custodios de la mayoría de activos informáticos considerados como equipos críticos, ya sea por su valoración monetaria o por su rol estratégico dentro del GADMCE.

En el caso de los funcionarios municipales, considerando el tamaño y naturaleza de la población es necesario aplicar la técnica de muestreo aleatorio estratificado con afijación proporcional por cada dirección departamental, para obtener mayor representatividad y minimizar el margen de error en la aplicación de las encuestas a la población objeto de esta investigación. Según Condori (2020), este tipo de muestreo asegurar que la muestra represente lo más aproximada a la realidad a la población objeto de estudio. Su objetivo es conseguir una muestra lo más semejante posible a la población. En la figura 3.3 se presenta la fórmula con la ecuación empleada para la aplicación del muestreo a poblaciones finitas (menos de 100.000 habitantes).

$$n = \frac{N * Z^2 * P * Q}{e^2(N-1) + Z^2 * P * Q}$$

Figura 3.3. Fórmula para calcular una muestra para población finidas

Cuyos parámetros se detallan y explican a continuación:

- n = ?, tamaño de la muestra a calcular;
- N = 322 (tamaño de la población); El tamaño de la población ha sido obtenido desde el formulario de talento humano de la institución según consta en su página web bajo la modalidad de LOSEP. GADMCE (2023).
- P/Q = 50/50 (Probabilidades con las que se presenta el fenómeno);
- Z = 1,96 (nivel de confianza elegido 95%);
- E = 10% (Margen de error o de imprecisión permitido);

Al reemplazar los valores explicados en la fórmula que antecede en la figura 3.3, el resultado que se obtiene como muestra 74,15; es decir, redondeando, la muestra obtenida fue de 74, lo que se lee: si se encuesta a 74 personas, el dato real que se busca será el 95% de las veces en el intervalo ±10% en relación con los datos que se observan en la encuesta. Con ese resultado se procede a ponderar por direcciones departamentales tal como se detalla en la 3.1, en donde se presenta el muestreo estratificado que se obtuvo.

Tabla 3.1

Distribución muestral de la encuesta aplicada a funcionarios del GADMCE

Item	Área departamental	Población	Peso	Muestra
1	Alcaldía*	14	4,35%	3
2	Administrativa	26	8,07%	6
3	Avalúos y Catastros	18	5,59%	4
4	Compras Publicas	4	1,24%	1
5	Comunicación Social	13	4,04%	3
6	Desarrollo Comunitario	39	12,11%	9
7	Economía Innovación y Turismo	8	2,48%	2
8	Financiera	30	9,32%	7
9	Gestión de Riesgo	12	3,73%	3
10	Higiene	32	9,94%	7
11	Junta Cantonal Protección Derechos	5	1,55%	1
12	Medio Ambiente	11	3,42%	3
13	Obras Publicas	16	4,97%	4
14	Patrimonio y Cultura	20	6,21%	5
15	Planificación	18	5,59%	4
16	Procuraduría Sindica	7	2,17%	2
17	Secretaria General	15	4,66%	3
18	Talento Humano	19	5,90%	4
19	Tecnologías de Información	15	4,66%	3
	Total	322	100,00%	74

Nota. Tomado de GADMCE(2023), *Se incluye la Coordinación General Institucional.

En el caso de los miembros de la Dirección de TIC al ser una población muy pequeña no es necesario que se realice un muestreo, por lo que se trabajó con los miembros que la componen, es decir, con las 22 personas.

3.2. Enfoque y tipo de investigación

El enfoque es cuantitativo, debido a que esta investigación implica la recolección de datos para caracterizar la realidad institucional del GAD municipal de Esmeraldas y probar una de las hipótesis planteadas en relación a las medidas implementadas por parte de la Dirección de TIC y el cumplimiento de la normativa vigente para garantizar la seguridad de Tecnologías, de manera que se puedan evaluar las variables y realizar el análisis estadístico respectivo. La investigación fue mixta: bibliográfica – descriptiva, y

consistió en la recopilación de información existente en libros, revistas científicas, repositorios digitales e internet, esto permitió la elaboración del estado del arte, marco teórico, y marco legal, es decir el marco de referencia que fundamenta científicamente este trabajo de investigación. Se recurrió a la revisión documental de diversos trabajos de investigación a nivel de maestría y doctorado en el ámbito público y privado, sobre todo de gobiernos autónomos e instituciones similares al GADMCE.

La investigación es descriptiva, debido a que, para diagnosticar y ratificar la problemática expuesta inicialmente, fue necesario visitar instalaciones y describir la infraestructura tecnológica existente, así como sus procesos internos, esto fue llevado a cabo en sitio, es decir en los 14 edificios en donde funciona el Municipio. Los métodos investigativos utilizados para el analizar los resultados y establecer las conclusiones fueron: analítico, inductivo y deductivo.

El método analítico se aplicó para descomponer el fenómeno estudiado en sus componentes fundamentales. Con ello se procedió a examinar detalladamente los controles de la norma ISO 27001:2022 y los mecanismos de seguridad implementados por la Dirección de TIC, identificando los elementos clave de la gestión de la dirección desde la planificación de políticas hasta el gobierno y administración de las tecnologías de información. Este método facilitó la identificación de áreas que requerían una atención más profunda en el proceso de evaluación.

Con la aplicación del método deductivo se verificó y validaron teorías existentes y generalizaciones derivadas del método inductivo. Partiendo de principios generales establecidos en el estándar ISO 27001:2022, y la normativa legal vigente relacionada con la gestión de las TIC. La inferencia lógica se utilizó para aplicar estos principios a situaciones específicas, verificando con el Director de TIC, la pertinencia de los mecanismos aplicados en el GADMCE y la alineación con los estándares establecidos. Además, permitió evaluar las no conformidades con las normativas y principios generales y requisitos obligatorios del SGSI institucional.

El método inductivo fue fundamental en la investigación de campo, tanto en la recopilación de los datos como en la observación realizada a las instalaciones, debido a que permitió tener un análisis más detallado de los casos puntuales de los subprocesos de la dirección, sobre las de políticas existentes, la asignación de recursos, y los resultados

obtenidos. A partir de las observaciones se establecieron generalizaciones sobre las prácticas comunes identificadas en la gestión de la seguridad de la información en el GADMCE. Este enfoque permitió elaborar las conclusiones generales preliminares.

3.3. Procedimiento de investigación

La planificaron de las etapas y fechas para desplegar la evaluación de la seguridad de tecnologías en el GAD municipal de Esmeraldas se realizó en un periodo de tiempo de dos meses, tal como lo detalla el cronograma contenido en la figura 3.4, junto con las actividades respectiva por cada etapa.

Actividades	feb-24				mar-24				abr-24			
	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
1. Marco de referencia												
1.1.Solicitud de autorización institucional	X											
1.2.Reunion inicial con el Director de TI	X											
1.3.Revision documental de orgánico funcional	X	X										
1.4.Revision documental del inventario de activos		X										
1.5.Revision documental de la normativa legal		X										
2. Análisis de riesgo del SGSI												
2.1. Planificación y análisis de riesgos		X	X									
2.2. Reunión inicial con el equipo de TI		X	X									
2.3. Observación a instalaciones e infraestructura		X	X									
2.4. Elaboración de documentos internos		X	X	X	X	X	X	X	X			
2.5. Elaboración de instrumentos de auditoria		X	X	X								
2.6. Resultados de Evaluación del SGSI			X	X	X							
3. Evaluación y Gestión de riesgos de activos												
3.1. Análisis del riesgo Informático de activos		X	X									
3.2. Revisión Inventario de activos informático		X	X	X								
3.3. Entrevista con el Director de TIC		X	X	X								
3.4. Encuesta a empleados administrativos			X	X								
3.5. Entrevista con funcionarios de TIC				X	X							
3.6. Resultado de Evaluación del riesgo				X	X	X						
4. Informe de resultados												
4.1. Tabulación y cuantificación de encuestas					X	X	X	X				
4.2. Diseño de tablas y gráficos						X	X	X				
4.3. Análisis e interpretación de resultados						X	X	X				
4.4. Conclusiones y recomendaciones							X	X				
4.5. Discusión de hallazgos - Dirección de TI							X	X				
4.6. Presentación de Informe final								X	X			
5. Plan de mejora y seguimiento												
5.1. Análisis FODA								X	X			
5.2. Revisión de recomendaciones								X	X			
5.3. Revisión de Políticas de seguridad								X	X			
5.4. Plan de mejora: Políticas de Seguridad								X	X			

Figura 3.4. Diagrama de Gantt – Auditoria del SGSI del GADMCE

A pesar que en primera instancia se planifica la realización de la evaluación en el último trimestre del año 2023, debido a la ola de violencia que azotó al país, y sobre todo a la ciudad de Esmeraldas, fue necesario reprogramar toda la planificación realizada anteriormente, y una vez establecidas las condiciones de seguridad ciudadana se reprogramaron para el primer trimestre del año 2024.

3.3.1. Fase 1: Desarrollo del Marco de referencia de la investigación

En este nivel se realizó una amplia revisión bibliográfica y documental de los diferentes aspectos relacionados con el tema de investigación: la seguridad de la información, las auditorias y evaluación de la seguridad de información, el análisis y gestión de riesgo, las metodologías de gestión de riesgos, el control interno, la auditoria de protección de datos, y la normativa legal vigente tanto a nivel nacional con las NCI 410 y 500, como internacional con las ISO 27001:2022 y sus conexas; fueron a nivel general los temas consultados y resumidos según su taxonomía y dimensión. Se procuró contar con fuentes de información actuales, es decir de menos de cinco años de publicación, y de alta relevancia científica. Se revisaron los conceptos y definiciones básicas, su importancia y los enfoques que presentan las diferentes metodologías o estándares de la industria, las normas de control interno de la CGE actualizadas al 2023, sus aspectos más importantes y las nuevas disposiciones allí contenidas (norma 410-11) que incluye: propiedad intelectual, ley de protección de datos, seguridad de la información y utilización de estándares, sistemas y plataformas para el sector público.

En esta fase, se determinó que, en el Ecuador, existe un marco de referencia basado en la ISO 27001 denominado Esquema Gubernamental de Seguridad de la Información (EGSI) y fue emitido por el MINTEL de aplicación obligatoria para instituciones del Ejecutivo, GADS, y empresas del Estado y sujetas a control por parte de la CGE, lo que facilitó recopilar una serie de plantillas de las ISO27001:2022, es decir actualizadas a su última versión. De igual manera se pudo establecer que la normas de la CGE fueron actualizadas en el 2023, presentando cambios y modificaciones para la norma 410 de TI, en donde justamente la norma 410-10 de Seguridad de TI, fue reformada en su totalidad, siendo ahora la norma 410-11, y cambiando significativamente lo dispuesto en la misma, al incluir aspectos como el cumplimiento de la LOPD y la utilización de estándares, enriqueciendo el marco de referencia con el que se realizó la investigación.

3.3.2. Fase 2: Análisis de la Infraestructura tecnológica y los mecanismos de seguridad informática.

El análisis de la Infraestructura tecnológica y de los mecanismos de seguridad informática existentes en el GADMCE se realizó mediante la revisión documental del inventario de activos informáticos y el estatuto orgánico por procesos, facilitado por el Director de TI. Una vez analizado el ambiente de control, procesos internos, edificios e instalaciones; se desplegó una encuesta con preguntas cerradas dirigida a los empleados administrativos, este instrumento estuvo basado en los requisitos obligatorios y anexo de la norma ISO 27001:2022. La asignación de los empleados fue aleatorio estratificado. Debido a que algunos se encontraban o salieron de vacaciones fue necesario volver a entregar los cuestionarios casi en un 50%. Con este instrumento se recabó la información relacionada con el nivel de conciencia que tienen los empleados sobre el rol que tiene la seguridad de TI en la institución y los riesgos a los que están expuestos los activos informáticos asignados, que utilizan o con los que interactúan; convirtiéndose en un insumo de validación para la dirección a la hora de establecer el estado de cumplimiento de esos parámetros.

Se validó la fiabilidad del instrumento utilizando el software de análisis estadístico SPSS, para lo cual se realizó la respectiva codificación de variables, y la generación de tablas y gráficos de los estadísticos descriptivos. Para una mejor compresión de los resultados se agruparon las preguntas en función de las secciones de los controles de las ISO 272001:2022, y se generó el análisis de los estadísticos descriptivos en base a las frecuencias mediante el programa SPSS versión 26. Al final, se presenta un análisis general de los resultados y su discusión al haber analizado la infraestructura tecnológica y los mecanismos de seguridad existentes en el GAD municipal de Esmeraldas. Esto fue contrastado con la entrevista al Director, inicialmente a través de una plantilla checklist con preguntas cerradas (cumple / no cumple) establecidas para cada dominio de los requisitos obligatorios y 93 controles que establece la ISO27001:2022, y clasificados en cuatro secciones (organizacionales, de personal, físicos y tecnológicas), para establecer el nivel de madurez o grado de cumplimiento del SGSI.

Para determinar el grado en que los mecanismos, procedimientos, controles, procesos, acuerdos y demás actividades implementadas por la Dirección de TIC cumplen con la normativa vigente se solicitó una segunda entrevista con el Director y los

funcionarios de TIC con la finalidad de validar el resultado inicial, confrontando las evidencias y/o respaldos de las respuestas facilitadas por el Director, consensuando entre ambas partes el grado de cumplimento. Esta cuantificación se realizó a través de una plantilla de valoración del estado del SGSI basada en los niveles de madurez, en cuya hoja de trabajo se registró el estado de cada parámetro evaluado tanto los elementos obligatorios y discrecionales como los controles de la ISO 27001:2022. En la tabla 3.2 se detalla cada uno de los posibles estados, su significado y la valoración con la que, basado a las evidencias presentadas u observadas, ha sido asociado según cada caso; a través de esta metodología se cuantificó el nivel de madurez que tiene la institución tanto para de los requisitos obligatorios del SGSI como para los controles establecidos por la norma en el anexo A. Esta tabla fue socializada previamente tanto con el Director como con los funcionarios de TI.

Tabla 3.2
Escala de cumplimiento de los controles del SGSI y nivel de riesgo asociado

Estado	Significado del estado	Grado de cumplimiento	Nivel de Riesgo
Inexistente	Ausencia completa de una política, procedimiento, control, etc., legibles.	0%	Muy alto
Inicial	El desarrollo apenas ha comenzado y requerirá un trabajo significativo para satisfacer los requisitos.	20%	Alto
Limitado	Progresando bien pero no completado aún.	40%	Medio alto
Definido	El desarrollo está más o menos completo aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento vigente ni activamente avalado por la alta dirección.	60%	Medio bajo
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar.	80%	Bajo
Optimizado	El requisito está plenamente conforme, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar lo antedicho a los auditores.	100%	Muy bajo

Nota: Tomado de ISO27001security (2022) y CGE(2023)

En la plantilla de ISO27001security (2022) a través de los selectores de opciones en la columna de estado de la hoja de cálculo denominada "Requisitos obligatorios SGSI" y de la hoja "Controles del Anexo A", se procedió a la valoración del SGSI para registrar sistemáticamente para cada parámetro el estado de cumplimiento en función de las evidencias presentadas, observadas o revisadas. Una vez que las métricas acumularon la suficiente evidencia "registros" y fueron completadas, este documento (las plantillas) fueron mantenidas sin modificación, y pueden ser actualizadas solo cuando le cambio de riesgos o controles incidan. Por lo tanto, en esta fase al determinar el grado de cumplimiento de cada control, de obtuvo el nivel de madurez del SGSI del GADMCE.

3.3.3. Fase 3: Evaluación de riesgo de la seguridad de tecnologías de información.

Debido a que la finalidad en esta fase era la valoración del riesgo informático y la identificación de los controles de seguridad implementados por la institución para para salvaguardar los activos, se realizaron varias visitas a las instalaciones e infraestructura con la finalidad de verificar los activos informáticos con los que se cuenta. En todos los casos la visita fue guiada por los funcionarios responsables de cada subproceso, en la cual se describieron los aspectos técnicos y procedimentales de seguridad concernientes a: infraestructura tecnológica, instalaciones, data center, sistemas de información, bases de datos, datos personales, aplicaciones, redes, y la gestión operativa. El proceso seguido fue el siguiente:

1. Lo primero que se definió fue el alcance de la evaluación de riesgo por cada área de la dirección de TI: Infraestructura, Soporte, Sistemas, y Proyectos. Se determinó trabajar con categorías de activos considerando la gran cantidad de equipos inventariados, siendo aproximadamente 2.000 dispositivos. Desde donde se extrajo previamente el valor de cada uno de los activos informáticos para determinar una valoración monetaria. En este análisis no se incluyen otros activos de información, salvo los bienes registrados en el sistema SIGAME.
2. Se identificó las amenazas más importantes a las que están expuestos dichos activos, la plantilla proporcionada incluyó los más comunes, sin embargo, se solicitó que establezcan un mínimo de dos amenazas por cada activo. Para esta actividad se proporcionó un banco de amenazas con la finalidad que el análisis sea lo más aproximado a la realidad posible.
3. Se identificó la vulnerabilidad que originan las amenazas definidas anteriormente para cada activo. El criterio fue registrar las dos vulnerabilidades que generen mayor impacto bajo criterio de cada funcionario. Así mismo se solicitó establecer una salvaguarda para cada una de las vulnerabilidades. Para esta actividad también proporcionó un banco de datos de manera que se cuente con la mayor información posible, y la vulnerabilidad se ajuste a los escenarios reales.

   La tabla 3.3 ilustra los valores posibles que se pueden asignar como probabilidad de ocurrencia tanto de la amenaza como de la vulnerabilidad, esto representa el nivel de amenaza y vulnerabilidad que cada funcionario de TI estableció y asocio para cada uno de los activos informáticos escogido para el ejercicio.

Tabla 3.3
Valoración de amenazas y vulnerabilidades

Criterio	Probabilidad	Valoración
Amenaza	Alto	3
	Medio	2
	Bajo	1
Vulnerabilidad	Alto	3
	Medio	2
	Bajo	1

Nota: Tomado de CGE(2023)

A través de la plantilla de análisis de riesgo, con los valores establecidos a cada criterio, se evaluó el riesgo para cada registro, mediante el cálculo automático del promedio de los criterios establecido: en la tabla 3.4 se ilustra la valoración de riesgo el criterio: confidencialidad. En la tabla 3.5 se ilustra el criterio: integridad. Por ultimo en la tabla 3.6 se ilustra el criterio: disponibilidad.

Tabla 3.4
Impacto en términos de pérdida de la confidencialidad

Confidencialidad	Significado del Criterio
Alto (3)	La divulgación no autorizada de la información, tiene un efecto crítico para la institución.
Medio (2)	La divulgación no autorizada de la información, tiene un efecto limitado para la institución.
Bajo (1)	La divulgación no autorizada de la información no tiene un efecto limitado para la institución.

Nota: Tomado de CGE(2023)

Tabla 3.5
Impacto en términos de pérdida de la integridad

Integridad	Significado del Criterio
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución.
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución.
Bajo (1)	La destrucción o modificación no autorizada de la información tiene un efecto leve para la institución.

Nota: Tomado de CGE(2023)

Tabla 3.6
Impacto en términos de la pérdida de la disponibilidad

Disponibilidad	Significado del Criterio
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución.
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución.
Bajo (1)	La interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución.

Nota: Tomado de CGE(2023)

4. Una vez determinando el valor para cada criterio se obtuvo automáticamente en la plantilla, la valoración del impacto (pérdida) de los activos de la organización, que no es más que el promedio de los 3 criterios evaluados.
5. Para cada activo que se estableció dos amenazas: la que se considere más frecuente en presentarse o con mayor probabilidad de ocurrencia, y la que se considere de más grave impacto en cualquiera de las amenazas con la finalidad de poder calcular el riesgo.
6. Se determinó la probabilidad de ocurrencia de la amenaza en base a la tabla 3.7 de manera que los funcionarios tengan un criterio homologado y relativo a esta parametrización.

Tabla 3.7
Criterio de probabilidad de ocurrencia de amenaza

Nivel de amenaza	Criterio de probabilidad	Criterio de condición de ocurrencia	Criterio por atractivo
Alto (3)	La ocurrencia es muy probable (>50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable.
Medio (2)	La ocurrencia es probable (<=50%)	Por errores o descuidos	El atacante se beneficia medianamente por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable.
Bajo (1)	La ocurrencia es menos probable (>0 y <50%)	En rara ocasión	El atacante NO se beneficia

Nota: Tomado de CGE(2023)

7. Se determinó el criterio de probabilidad de ocurrencia de vulnerabilidades en base a la tabla 3.8 de manera que los funcionarios tengan un criterio homologado y relativo a esta parametrización.

Tabla 3.8
Criterio de probabilidad de ocurrencia de vulnerabilidades

Nivel de vulnerabilidad	Criterio
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza.
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable.
Bajo (1)	La medida de seguridad es adecuada.

Nota: Tomado de CGE(2023)

8. Por último, con todos los valores anteriormente establecidos, se calculó automáticamente el nivel de riesgo, la figura 3.5 ilustra el color y valoración que

la plantilla asigna según la ponderación realizada. El nivel de riesgo determinando en cada iteración se obtiene de la siguiente formula:

Riesgo = Valor de impacto(VA) x Nivel de amenaza x Nivel de vulnerabilidad

Nivel de Riesgo		Acciones
1 - 3	El riesgo es BAJO	Retención y monitoreo del activo
4 - 8	El riesgo es MEDIO	Requiere atención mediante la aplicación de controles que permita disminuir el riesgo, durante un tiempo determinado de acuerdo a la importancia del activo.
9 - 27	El riesgo es ALTO	Requiere atención inmediata, para modificar el riesgo del activo.

Figura 3.5. Cuadro valoración de nivel de riesgo
Nota: Tomado de CGE(2023)

Este procedimiento se repitió para establecer el nivel del riesgo de cada uno de los activos previamente identificados. Por estas razones y considerando las múltiples ocupaciones de cada funcionario, se seleccionaron solo dos activos o categorías de activos por cada funcionario, sugiriendo que sean los de mayor valor o de mayor importancia según sea el caso de cada subproceso. Una vez dimensionado el inventario de activos, y en compañía del Director de TIC se procedió al llenado de la plantilla, en donde cada funcionario proporcionó la información de los activos que tienen a cargo, de manera que se obtuvo una la matriz con información significativa considerando que esos ítems constituyen monetariamente del 90% del valor de todo el inventario de activo informático que la institución posee.

3.3.4. Fase 4: Informe de auditoría del GAD municipal de Esmeraldas

Para una mejor compresión de los resultados de la auditoria en base a los niveles de confianza determinados (presentados en detalle en el informe de auditoría del siguiente capítulo), se generó el gráfico radial en el cual se visualizan, para cada una de las variables, los resultados De este modo, y mediante una interpretación visual se pueden evaluar, fácilmente, cuáles son las normas en las que se presentan fortalezas del ambiente de control, así como cuáles son las normas en las que se representan mayores debilidades.

Se elaboró el informe de auditoría del GADMCE considerando una matriz de evaluación para cada una de las normas 410. En este documento se incluyeron los resultados de la investigación de campo, es decir las encuestas y sus resultados que ratifican la problemática, por lo que a través del análisis e interpretación de resultados se elaboró el respectivo informe con tablas, gráficos y análisis que permitieron sintetizar y

evidenciar el estado real de la seguridad de tecnología de la institución. Este informe contiene las conclusiones y recomendaciones de los hallazgos encontrados, así como las no conformidades y acciones de seguimiento que la institución deberá que atender o justificar su no tratamiento. Para este último punto, se entregó un acta para el seguimiento de las recomendaciones, estableciendo el funcionario responsable del tratamiento de la no conformidad, y el plazo de tiempo en el supuesto que la recomendación no fuese de cumplimiento inmediato.

Se utilizó un instrumento elaborado y utilizado en las auditorias de gestión que realiza la CGE a nivel de auditorías internas de los GAD provinciales, pero actualizado a las reformas de la norma 410 del 2023. Este instrumento consta de una matriz de preguntas para cada una de las 17 normas, de manera que se evidencie y cuantifique el grado de cumplimiento de las mismas. En este trabajo, se introduce el gráfico radial como nueva metodología para explicar la cobertura y cumplimiento en las 17 aristas que representa cada norma evaluada en la institución. A partir de la figura representada en el gráfico radial se puede apreciar el nivel de madurez del sistema de control interno en la institución.

3.3.5. Fase 5: Plan de mejora: implementación de políticas de seguridad

En base a los riesgos identificados en los activos informáticos, el riesgo asociado al nivel de cumpliento del SGSI, y a las recomendaciones del informe de auditoria que fueron entregadas a la Dirección de TIC del GADMCE; se elaboró una propuesta de mejora a través de la implementación de políticas de seguridad de información para la institución. El propósito de esta propuesta fue definir los objetivos, lineamientos y principios base, al más alto nivel, es decir emitida desde la máxima autoridad, con el objetivo de normar los aspectos prioritarios que debe cumplir el SGSI en la institución, con una vigencia de largo plazo.

Se definió el compromiso y lineamientos de la máxima autoridad y la alta dirección para proteger la información, garantizando en todo momento su confidencialidad, integridad y disponibilidad; además de prevenir y mitigar los riesgos que fueron identificados tanto para los activos informáticos, como para los controles del SGSI, que pueden afectarla.

A través de la aprobación formal y su divulgación oficial, se dejó plasmado el compromiso de la máxima autoridad con el cumplimiento de esta política, tanto para su aprobación, como para su publicación y difusión a todos los funcionarios del GADMCE. Este plan de mejora basado en los hallazgos encontrados en la de auditoría consideró las recomendaciones y acciones de seguimiento que la institución deberá que atender o justificar su no tratamiento en un tiempo determinado.

3.4. Instrumentos de evaluación

3.4.1. Información Primaria

En la recolección de la información primaria de esta investigación se utilizó técnicas tradicionales como son: la entrevista, la observación y la encuesta; combinadas con la aplicación de instrumentos de recopilación de la información como son las plantillas y checklist, que en conjunto fueron usadas en el trabajo de campo, de la siguiente forma:

- La encuesta, a través de un cuestionario con preguntas cerradas en base a la ISO 27001:2022, fue aplicada a los empleados para medir el nivel de concientización sobre el rol de la seguridad de la información y el riesgo de seguridad al que están expuestos en la institución, Estos instrumentos se aplicaron a inicios del primer trimestre del 2024 de manera aleatoria y de forma estratificada a los funcionarios administrativos de las direcciones o unidades consideradas usuarios de las TI. Una vez completados los cuestionarios se procedió a la recodificación en SPSS, mediante la codificación de todos los factores considerando que el instrumento aplicado utiliza las mismas escalas para todas las preguntas.
- A partir del paquete estadístico SPSS versión 26s, se sistematizaron y analizaron los datos primarios recogidos mediante la encuesta comparando los resultados cuantitativos, así como también, se estableció el nivel de confianza del instrumento, tal como se ilustra en la figura 3.9, obteniendo una fiabilidad alta en el resultado del Alfa de Cronbach α: 0,857. Lo que significa que, al tener una mayor consistencia entre las preguntas de la encuesta, implica una mayor confiabilidad de la misma.

Tabla 3.9
Estadísticas de fiabilidad del instrumento

Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	Número de elementos
,857	,855	20

- Las entrevistas se realizaron desde el último trimestre del 2023 hasta el primer trimestre del 2024, tanto al director como a los funcionarios de la Dirección TIC del Municipio, combinándolas con el uso de las plantillas (matriz) de valoración del riesgo informático de los activos de la institución; se emplearon dos plantillas de evaluación del grado de cumplimiento en cada uno de los aspectos escenciales del SGSI y los controles anexos incluidos en la norma ISO 27001 actualizada al 2022.
- La ficha de observación fue aplicada para levantar información de las instalaciones, áreas de trabajo, y activos informáticos, como son: el centro de datos (datacenter), parque informático, sala de reuniones, servidores, red, equipos de comunicación, y la infraestructura tecnológica existente; por lo que fueron necesarias múltiples visitas a las instalaciones durante el último trimestre 2023 e inicios del 2024.

3.4.2. Información Secundaria

Para enriquecer esta fase se procedió a investigar en otros GAD cómo se gestiona la seguridad de la información y de los datos personales en los departamentos de sistemas o TIC, mediante la información de sus páginas web, así como la que se encuentra publicada como parte del cumplimiento de la Ley de Transparencia durante el segundo semestre del año 2023. Se revisaron bases de datos de las amenazas y vulnerabilidades en las páginas web oficiales de estándares internacionales y de datos pre elaborados, de Internet, de medios de comunicación, artículos y documentos como libros, tesis, informes oficiales relacionados con la seguridad de tecnólogas de información.

3.5. Consideraciones éticas

Se han cumplido los principios éticos que orientan este tipo de investigación: beneficencia, precaución, responsabilidad, justicia y autonomía; sobre todo en el tema de confidencialidad de la información y el sigilo que debe existir todos los temas específicos considerados como sensibles por la institución. Considerando que esta investigación involucra a personas que forman parte de una institución pública, se cuenta con la respectiva autorización de la máxima autoridad, es decir el Alcalde del Cantón Esmeraldas, y el consentimiento informado de los participantes en la investigación. Para lo cual se envió un documento solicitando dicha autorización y explicado el alcance de la investigación.

CAPITULO IV
RESULTADOS Y DISCUSIÓN

4.1. Información obtenida mediante encuestas a empleados

4.1.1. Controles Organizacionales

Tabla 4.1
¿Las políticas de seguridad de la información son importantes para la institución?

Respuesta	N	%
Si	70	94,6%
No	1	1,4%
No conoce	3	4,1%

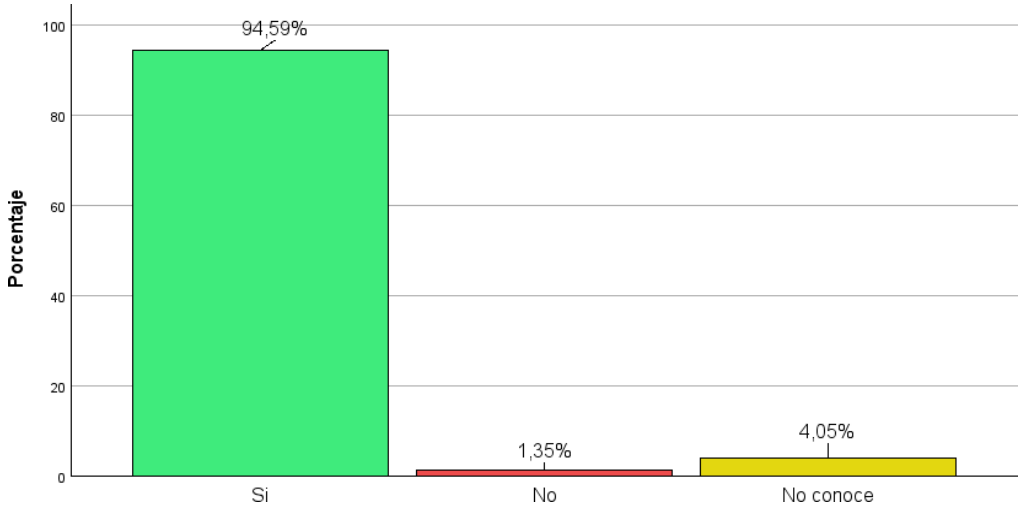


Figura 4.1. Porcentaje de respuestas Pregunta Nº1

En la figura 4.1 se evidencia que la gran mayoría de los empleados del GADMCE encuestados reconocen la importancia que las políticas de seguridad de la información tienen en la institución, sin embargo, se observa en la tabla 4.1 que algo más del 5%, o no tienen conocimiento o no coinciden en que sea algo importante; por lo tanto, se puede inferir que no tienen mayor grado de concientización del rol que juega le seguridad de la información en sus procesos internos. Esta pregunta guarda relación con la cláusula 5.2 de la ISO 270001.

Tabla 4.2
¿Se están aplicando las políticas de seguridad de la información en la institución?

Respuesta	N	%
Si	18	24,3%
No	21	28,4%
No conoce	5	47,3%

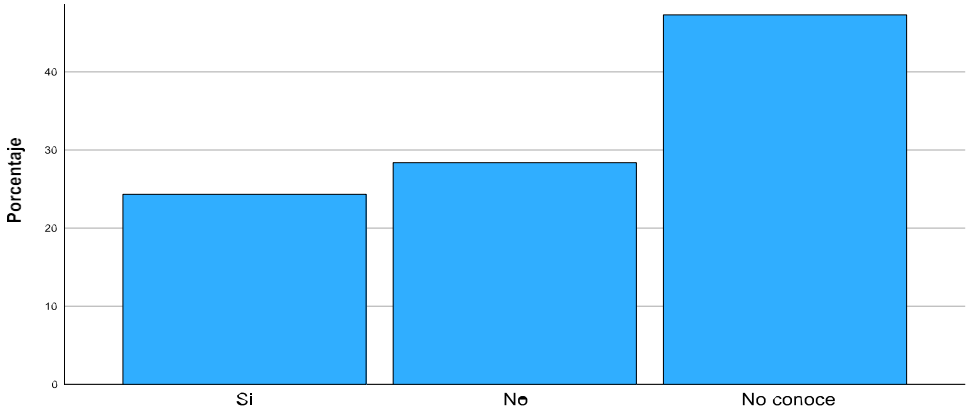


Figura 4.2. Porcentaje de respuestas Pregunta Nº2

En la figura 4.2 se evidencia un desconocimiento por parte de la gran mayoría de los empleados del GADMCE que fueron encuestados, así lo detalla la tabla 4.2, en donde solo el 24% afirmó que se están aplicando políticas de seguridad de la información en la institución. Siendo preocupante que casi la mitad de los empleados desconozca sobre su aplicación, y peor aún, que el 28% señalen que no se aplican. Esta pregunta esta basada en el control A.5.1 de la ISO 270001:2022.

Tabla 4.3

¿La institución ha elaborado y requerido a todo el personal el cumplimiento de las políticas de seguridad de la información?

Respuesta	N	%
Si	19	25,7%
No	27	36,5%
No conoce	28	37,8%

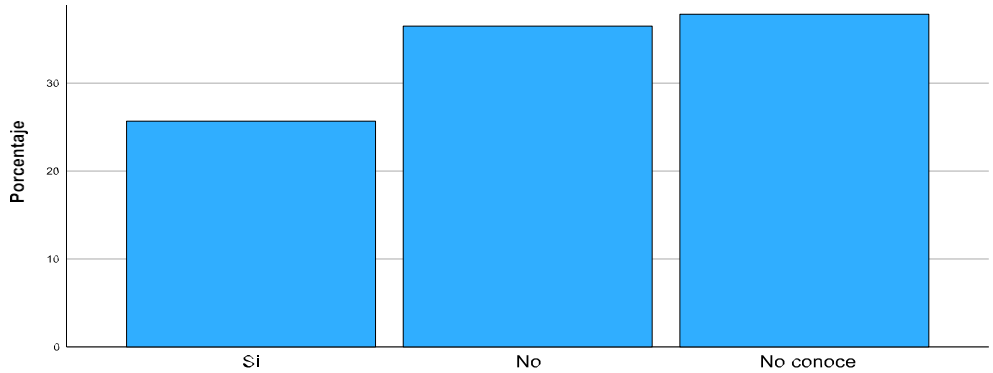


Figura 4.3. Porcentaje de respuestas Pregunta Nº3

En la figura 4.3 se visualiza que solo la cuarta parte de los empleados señala conocer que la institución ha elaborado y requerido a todo el personal del GADMCE el cumplimiento de las políticas de seguridad de la información. En la tabla 4.3 se evidencia que casi el 75% indicó: o no tener conocimiento, o que no se cumple la afirmación consultada basada en el control A.5.4 de la ISO 27001.

Tabla 4.4

¿Se establecen e implementan reglas para controlar el acceso físico y lógico a la información y otros activos informáticos asociados?

Respuesta	N	%
Si	52	70,3%
No	8	10,8%
No conoce	14	18,9%

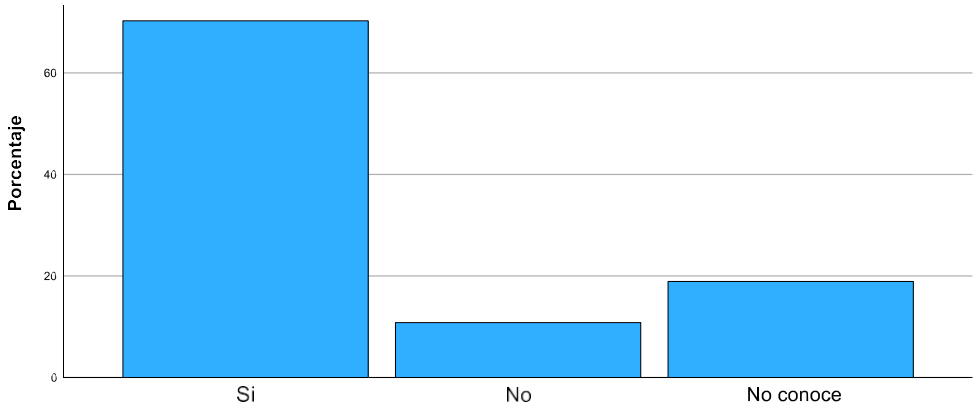


Figura 4.4. Porcentaje de respuestas Pregunta Nº4

En la figura 4.4 se puede evidenciar que la mayoría de los empleados señaló que, si se han establecido e implementado reglas para controlar el acceso físico (credenciales y biométricos) y lógico (usuarios y contraseñas) a la información y otros activos informáticos asociados a los requisitos de seguridad de la información de la institución, en concordancia con el control A.5.15 de la ISO 27001:2022. La tabla 4.4 demuestra que el 70% señalan el cumplimiento de este control.

Tabla 4.5

¿La institución identifica y cumple con los requisitos relacionados con la preservación de la privacidad y la protección de los datos personales (PII)?

Respuesta	N	%
Si	23	31,1%
No	11	14,9%
No conoce	40	54,1%

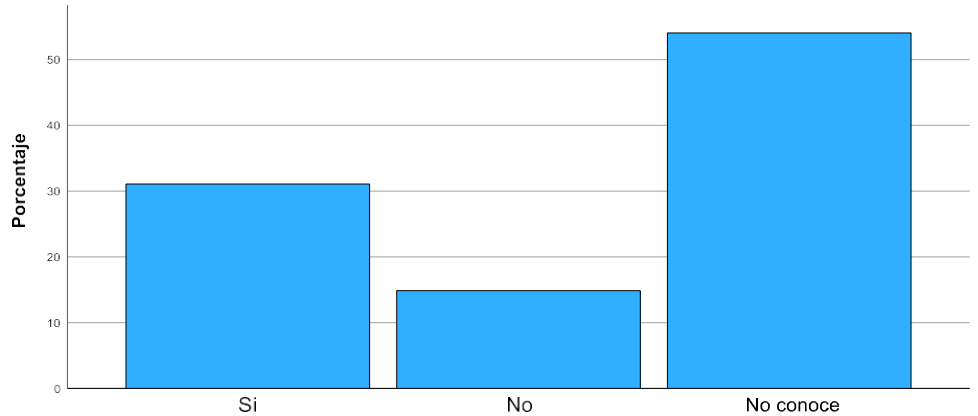


Figura 4.5. Porcentaje de respuestas Pregunta Nº5

En la figura 4.5 se puede visualizar que la mayoría de los empleados del GADMCE señalaron desconocer si institución identifica y cumple con los requisitos, leyes y regulaciones aplicables relacionados con la preservación de la privacidad y la protección de los datos personales. En la tabla 4.5 se aprecia que un 15% de los encuestados señaló que no se cumple, y el 31% que, si se está cumpliendo. Esta pregunta se realizó en función de la nueva ley orgánica de protección de datos personales y en base al control A.5.34 de la ISO 27001:2022.

4.1.2. Controles de personas

Tabla 4.6
¿El personal de la organización recibe concientización, educación y/o capacitación apropiadas sobre seguridad de la información?

Respuesta	N	%
Si	10	13,5%
No	51	68,9%
No conoce	13	17,6%

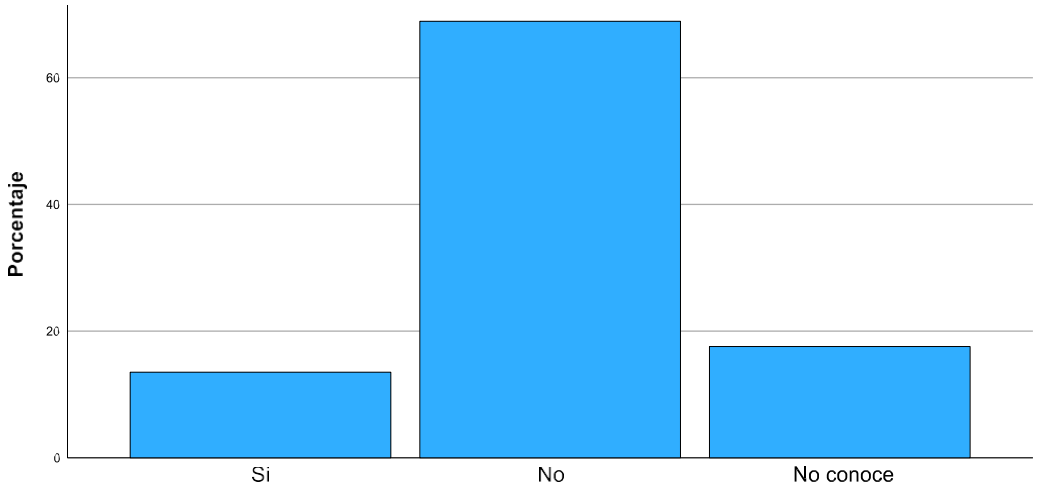


Figura 4.6. Porcentaje de respuestas Pregunta Nº6

En la figura 4.6 se evidencia que la mayoría de los empleados del GADMCE señalaron que no han participado en algún proceso de concientización, ni recibido educación y/o capacitación apropiadas sobre seguridad de la información, seguridad informática o ciberseguridad. En la tabla 4.6 se aprecia que son casi el 69% los empleados los que confirmaron este incumplimiento, sumado a que el 18% de los encuestados señalaron desconocer si se cumple o no con la pregunta planteada. Apenas el 13.5% contesto que si se realiza algún proceso relacionado con la concientización, educación y/o capacitación sobre seguridad de la información Esta pregunta se basa en el control A.6.3 de la ISO 270001:2022.

Tabla 4.7

¿La institución hace firmar a los funcionarios algún acuerdo sobre la confidencialidad de la información que maneja en el desempeño de sus actividades?

Respuesta	N	%
Si	15	20,3%
No	40	54,1%
No conoce	19	25,7%

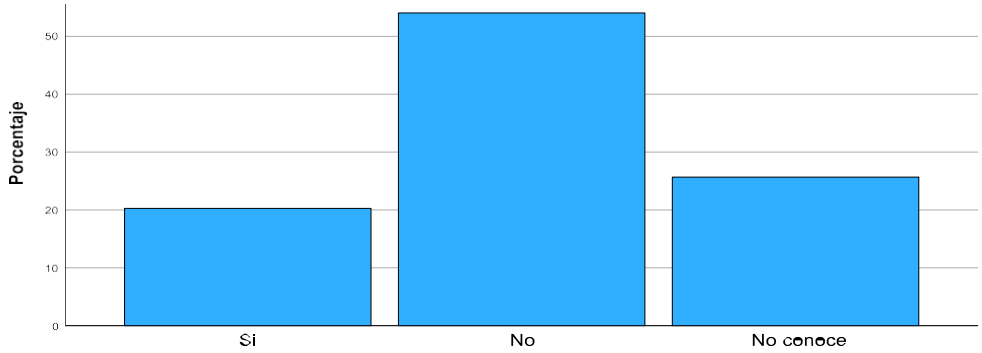


Figura 4.7. Porcentaje de respuestas Pregunta Nº7

En la figura 4.7 se presenta de manera gráfica las respuestas en donde los encuestados señalan que son pocos los empleados que conocen si la institución hace firmar a los funcionarios algún acuerdo sobre la confidencialidad o “no revelación” de la información que maneja o posee en el desempeño de sus actividades; peor aún si se identifican, documentan y revisan periódicamente. Observando el resultado en la tabla 4.7 se evidencia que el 20% señalaron que, si se cumple con este control. Muy por el contrario, la gran mayoría, el 54% señaló que no se cumple el mismo, y el 26% señaló no conocer sobre el tema. Esta pregunta se basa en el control A.6.6 de la ISO 270001:2022.

Tabla 4.8

¿Se implementan medidas de seguridad cuando el personal trabaja de forma remota para proteger la información?

Respuesta	N	%
Si	24	32,4%
No	21	28,4%
No conoce	29	39,2%

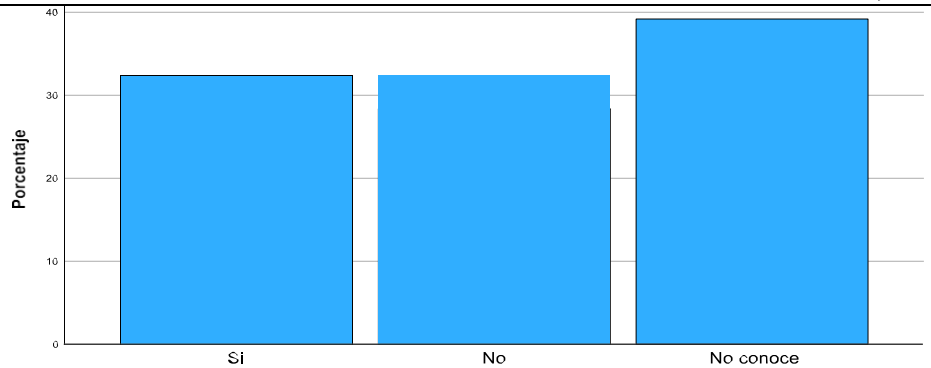


Figura 4.8. Porcentaje de respuestas Pregunta Nº8

En la figura 4.8 se grafica el desconocimiento que la mayoría de empleados tienen en cuanto a las medidas de seguridad implementadas por la Dirección de TIC cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización. Tal como se presenta en la tabla 4.8, solo el 32% manifiesta que, si se implementa algún tipo de medida o mecanismo de seguridad. Sin embargo, un 39% desconoce y un 28% señaló que no existen medidas. Esta pregunta está basada en el control A.6.7 de la ISO 27001:2022.

Tabla 4.9

¿Se utiliza algún sistema de registro de incidentes para que los funcionarios informen eventos de seguridad observados o sospechosos de manera oportuna?

Respuesta	N	%
Si	23	31,1%
No	22	29,7%
No conoce	29	39,2%

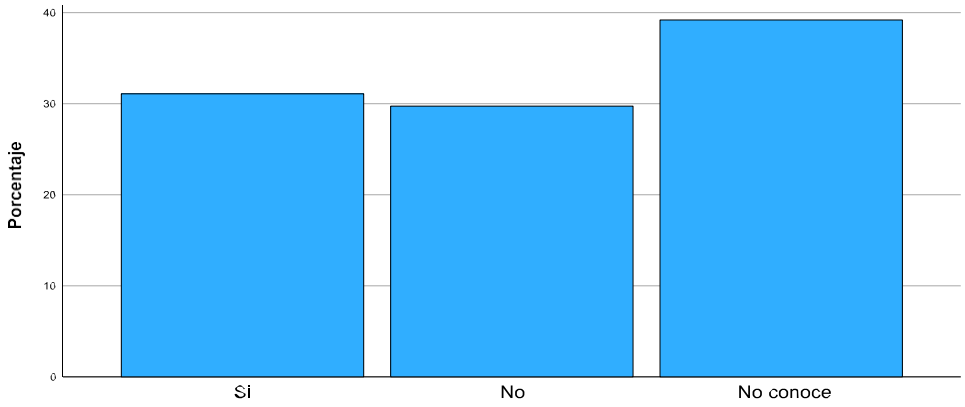


Figura 4.9. Porcentaje de respuestas Pregunta Nº9

En la figura 4.9 se grafica las respuestas de la mayoría de los empleados en donde señalaron que no conoce o no se utiliza algún sistema de registro de incidentes (mesa de ayuda - Helpdesk) u otro mecanismo para que el personal informe eventos de seguridad de la información, seguridad informática o ciberseguridad observados o sospechosos de manera oportuna. Esto se puede constatar cuantitativamente en la tabla 4.9, con casi el 69% de respuestas no positivas. Esta pregunta está basada en el control A.6.8 relacionado con los informes de eventos de seguridad de la información de la ISO 27001:2022.

Tabla 4.10

¿Está consciente de las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información?

Respuesta	N	%
Si	24	32,4%
No	15	20,3%
No conoce	35	47,3%

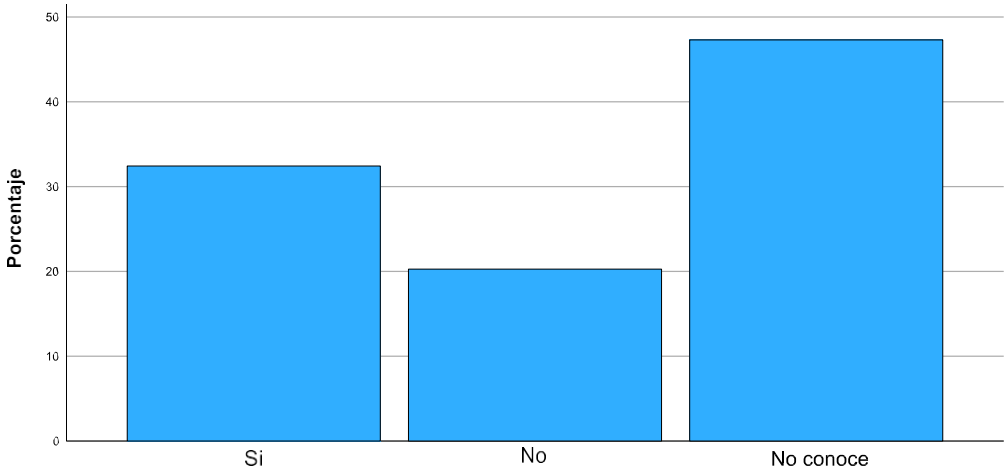


Figura 4.10. Porcentaje de respuestas Pregunta Nº10

En la figura 4.10 se evidencia que la mayoría de los empleados no están conscientes de las implicaciones que tiene el no cumplir con los requisitos del sistema de gestión de seguridad de la información. La tabla 4.10, precisa que solo el 32% contestó afirmativamente esta pregunta, y que la mayoría de encuestados, alrededor de un 68% manifestó que no estar consciente y no conocer de las repercusiones del citado incumplimiento. Esta pregunta está basada en la cláusula 7.3 de los requisitos obligatorios del SGSI titulada: Programa de concientización en seguridad, de la ISO 27001:2022.

4.1.3. Controles Físicos

Tabla 4.11

¿Las medidas de seguridad física que la institución tiene para salvaguardar los activos informáticos son las adecuadas?

Respuesta	N	%
Si	39	52,7%
No	18	24,3%
No conoce	17	23,0%

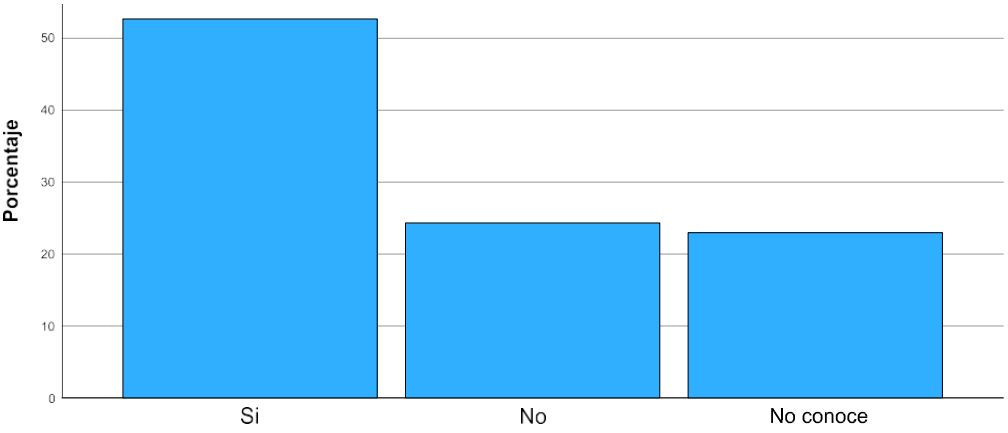


Figura 4.11. Porcentaje de respuestas Pregunta Nº11

En la figura 4.11 se visualiza que la mayoría de los empleados señalaron que las medidas de seguridad física que la institución tiene para salvaguardar los activos informáticos son las adecuadas, es decir se cuenta con guardianía en las entradas de las instalaciones, control de accesos a oficinas, cámaras de seguridad, y perímetros de seguridad en donde se encuentran los activos de información; esto se evidencia en la tabla 4.11, con casi el 53% de respuestas afirmativas. Un 24% señaló que no existen medidas de seguridad física, y un 23% manifestó desconocer del tema. Esta pregunta se basó en el control A.7.3 de la ISO 27001:2022.

Tabla 4.12

¿La institución cuenta con la protección contra amenazas físicas y ambientales a la infraestructura tecnológica o equipamiento informático?

Respuesta	N	%
Si	13	17,6%
No	25	33,8%
No conoce	36	48,6%

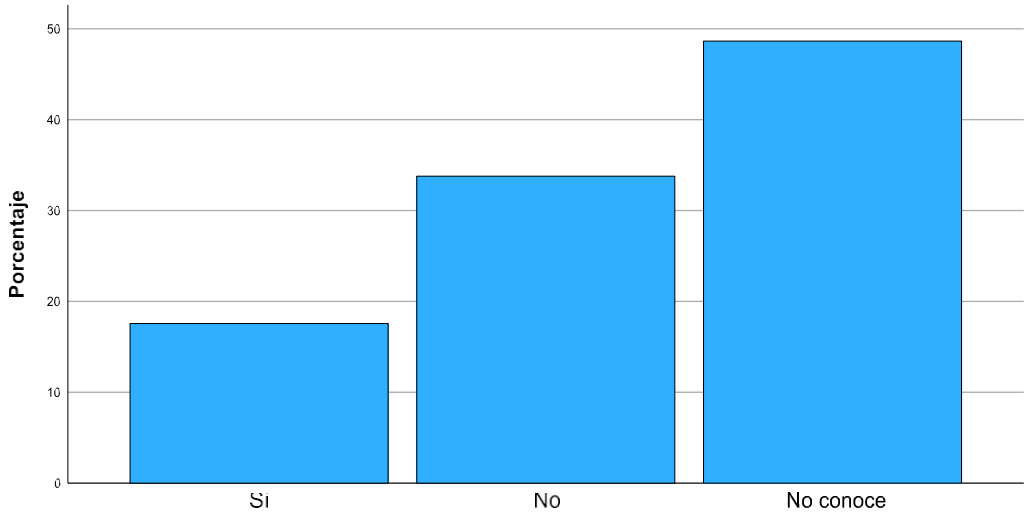


Figura 4.12. Porcentaje de respuestas Pregunta Nº12

En la figura 4.12 se evidencia uno de los puntos más débiles de la institución, pues tal como lo detalla la tabla 4.12 solo alrededor del 18% de los empleados encuestados manifestaron que la institución si cuenta con protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura tecnológica o equipamiento informático. Un 34% señaló que no se cuenta con protección, y un 49%, es decir casi la mitad de manifestaron que desconocen de las medidas o mecanismos de protección existentes en las oficinas, despachos o instalaciones del GAD municipal de Esmeraldas. Esta pregunta se basó en el control A.7.3 de la ISO 27001:2022.

Tabla 4.13

¿El activo informático a su cargo está ubicado de forma segura y protegida mediante el acceso restringido a su área de trabajo?

Respuesta	N	%
Si	25	33,8%
No	39	52,7%
No conoce	10	13,5%

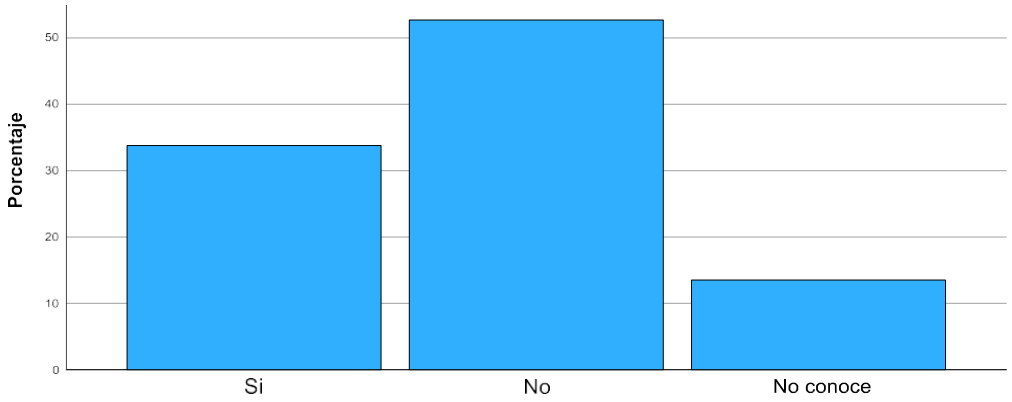


Figura 4.13. Porcentaje de respuestas Pregunta Nº13

En la figura 4.13 se visualiza que la mayoría de los empleados señalaron que el activo informático a su cargo (o equipos de cómputo con los que trabaja) no está ubicado en un lugar seguro (libre de inundación, humedad, polvo, o daño eléctrico) ni cuenta con protección (libre de robo, vandalismo o sabotaje) mediante el acceso restringido a su área de trabajo. En la tabla 4.13 se puede confirmar el dato que indica que con el 53% de respuestas negativas. Esta pregunta se basó en el control A.7.8 de la ISO 27001:2022.

Tabla 4.14

¿Los cables de energía, de red, internet o servicios de información donde se conectan sus equipos están protegidos contra interceptaciones o daños?

Respuesta	N	%
Si	20	27,0%
No	39	52,7%
No conoce	15	20,3%

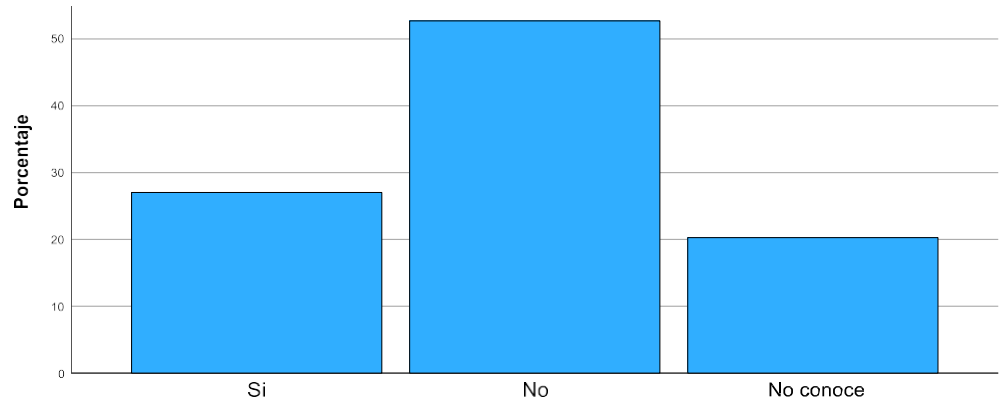


Figura 4.14. Porcentaje de respuestas Pregunta Nº14

En la figura 4.14 se presenta la opinión de los empleados sobre los cables de energía, datos, internet o los servicios de información de soporte donde se conectan los equipos que utilizan; evidenciando en la tabla 4.14 que para una mayoría conformada por el 53%, estos no se encuentran protegidos contra interceptaciones, interferencias o daños. El 20% señalaron desconocer del tema. Y solo el 27% de los encuestados contestaron positivamente esta pregunta, basada en el control A.7.12 de la ISO 27001:2022.

Tabla 4.15

¿Los equipos informáticos reciben periódicamente mantenimiento preventivo para garantizar la disponibilidad, integridad y confidencialidad de la información?

Respuesta	N	%
Si	26	35,1%
No	27	36,5%
No conoce	21	28,4%

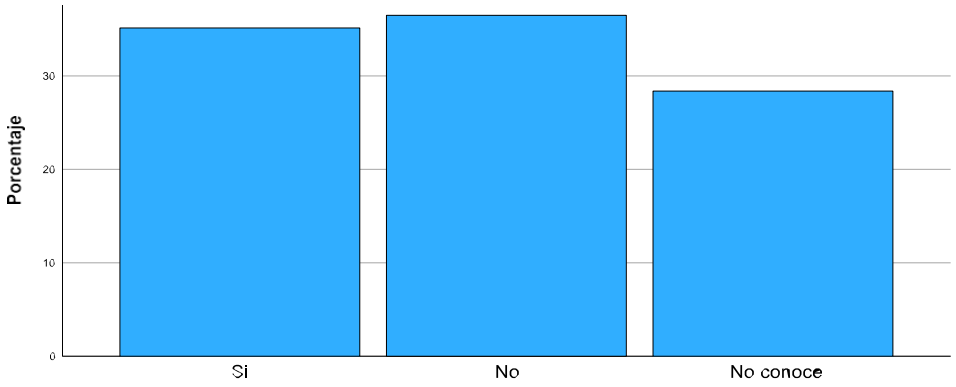


Figura 4.15. Porcentaje de respuestas Pregunta Nº15

En la figura 4.15 se presenta que la mayoría de los empleados, no reciben periódicamente mantenimiento preventivo o desconocen si se realiza ese proceso para garantizar la disponibilidad, integridad y confidencialidad de la información. En la tabla 4.15 se aprecia que solo el 35% señalaron que puede confirmar el dato que indica que con el 53% de respuestas negativas sobre el mantenimiento de equipos informáticos (Hardware y software) de la institución. El análisis de esta pregunta está basado en el control A.7.13 de la ISO 27001:2022.

4.1.4. Controles Tecnológicos

Tabla 4.16

¿La institución tiene instalado y actualizado algún antivirus para proteger la información almacenada, procesada o accesible a través del computador asignado

Respuesta	N	%
Si	35	47,3%
No	26	35,1%
No conoce	13	17,6%

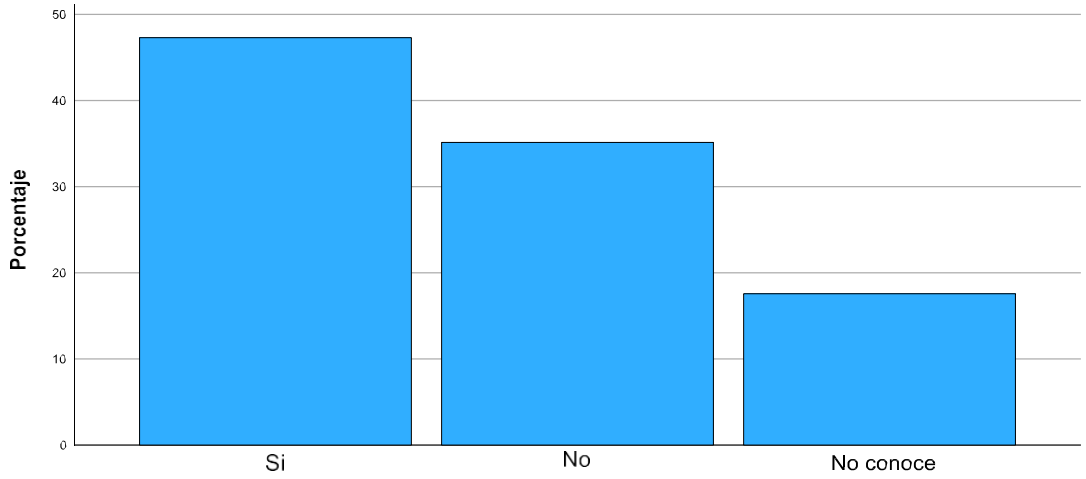


Figura 4.16. Porcentaje de respuestas Pregunta Nº16

En la figura 4.16 se visualiza que la mayoría de los empleados señalaron que la institución tiene instalado y actualizado un programa de antivirus para proteger la información almacenada en archivos y carpetas, procesada a través de sistemas o accesible por correo electrónico a través del activo informático (computador) asignado en calidad de usuario para el cumplimiento de sus funciones. En la tabla 4.16 se puede confirmar el dato que indica que con el 53% de respuestas negativas. Esta pregunta se basó en el control A.7.8 de la ISO 27001:2022.

Tabla 4.17

¿Se implementan tecnologías y procedimientos de autenticación segura para el control de acceso al sistema operativo, la red de datos o los sistemas?

Respuesta	N	%
Si	56	75,7%
No	10	13,5%
No conoce	8	10,8%

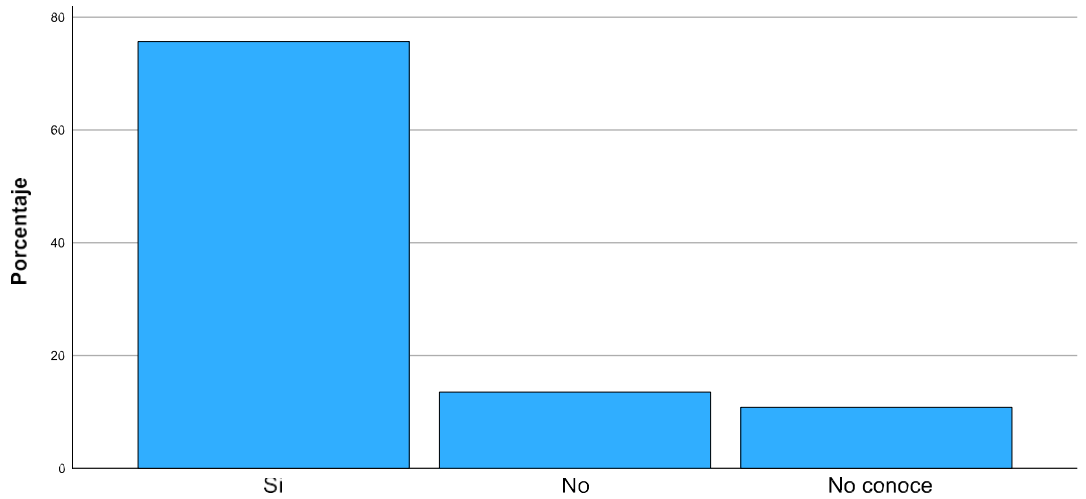


Figura 4.17. Porcentaje de respuestas Pregunta Nº17

En la figura 4.17 se puede apreciar que la mayoría de los empleados indicaron que, si se implementan tecnologías y procedimientos de autenticación segura para el control de acceso al sistema operativo, la red de datos o los sistemas informáticos existentes. En la tabla 4.17 se evidencia el punto más fuerte de la Dirección de TIC en lo referente a seguridad de la información con un 76% de valoraciones positivas. Esta pregunta se basó en el control A.8.12 de la ISO 27001:2022.

Tabla 4.18

¿Se aplican medidas de prevención de fuga de datos, filtración de información a través de la red y otros dispositivos que procesen, almacenen o transmitan información?

Respuesta	N	%
Si	13	17,6%
No	15	20,3%
No conoce	46	62,2%

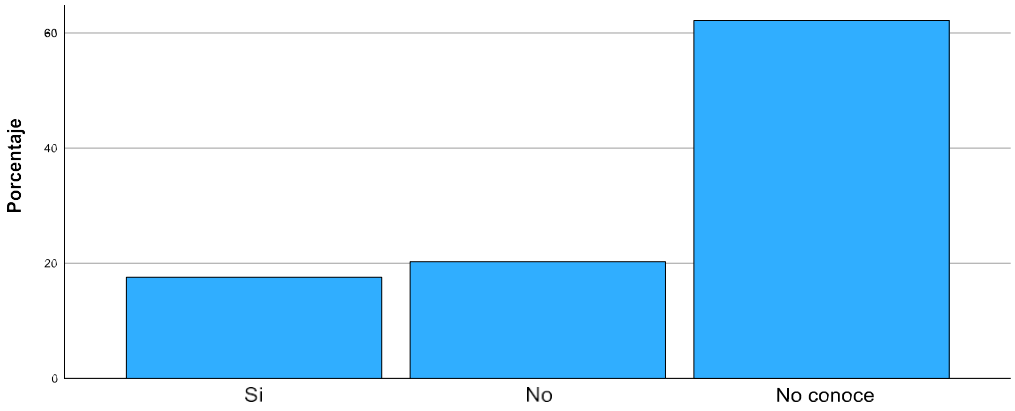


Figura 4.18. Porcentaje de respuestas Pregunta Nº18

En la figura 4.18 se puede apreciar que la mayoría de los empleados indicaron que, desconocen si en la institución se aplican medidas de prevención de fuga de datos, filtración de información a través de la red y otros dispositivos que procesen, almacenen o transmitan información. Un 20% de los encuestados indicaron que no existen medidas de prevención, y solo el 18% aproximadamente indicaron que, si se han tomados medidas a través de accesos restringidos a carpetas, la colocación de claves a los equipos y archivos. En la tabla 4.18 se puede apreciar mejor la diferencia entre los que señalan que si se cumple, y casi el 80% que señalan lo contrario o desconocen.

Tabla 4.19

¿Tiene asignado bienes o activos informáticos para el desarrollo de sus actividades como funcionario público?

Respuesta	N	%
Si	65	87,8%
No	7	9,5%
No conoce	2	2,7%

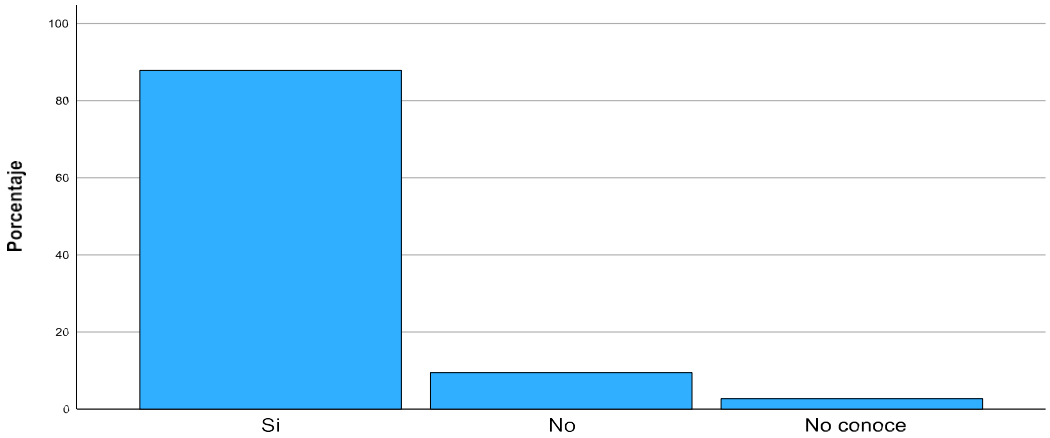


Figura 4.19. Porcentaje de respuestas Pregunta Nº19

En la figura 4.19 se ilustra que la gran mayoría de los encuestados tiene asignado un activo informático, es decir un computador personal para el cumplimiento de sus labores. Sin embargo, existe casi un 10% que manifestaron no tener el equipo o bien asignado o incluso prestado. Se pudo contrastar con el listado de bienes generado a través del sistema que existen funcionarios con una gran cantidad de equipos asignados, sobre todo del proyecto de ciudad inteligente, siendo los más costosos y de más alto riesgo. En la tabla 4.18 se puede evidenciar el detalle de las cantidades de empleados que contestaron negativamente esa pregunta, basada en el control A.7.8 de la ISO 27001:2022. relacionada al inventario de información.

Tabla 4.20

¿Las redes y los dispositivos de red se protegen, gestionan y controlan para proteger la información en los sistemas y aplicaciones?

Respuesta	N	%
Si	30	40,5%
No	7	9,5%
No conoce	37	50,0%

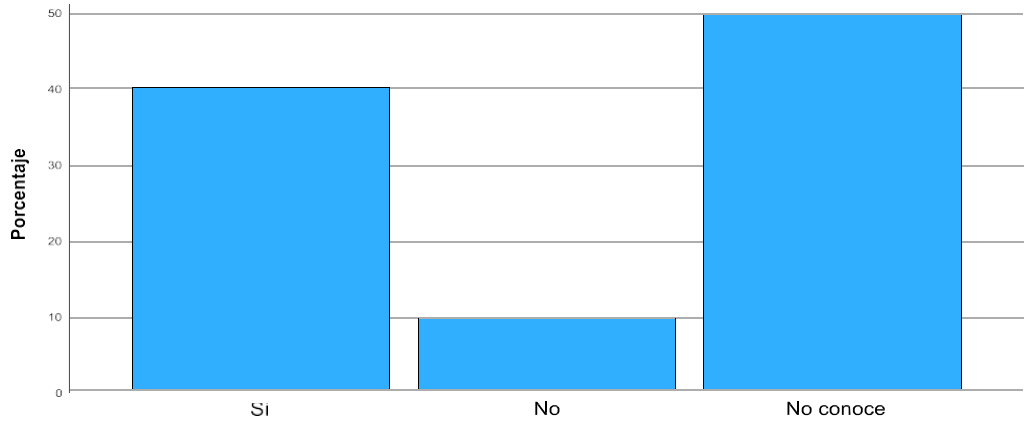


Figura 4.20. Porcentaje de respuestas Pregunta Nº17

En la tabla 4.20 se puede evidenciar que la mayoría de los empleados no se sienten protegidos ni seguros al estar conectados a la red de datos de la institución, o al utilizar sus equipos de cómputo en red. Un 40% de los funcionarios indicaron que los sistemas y aplicaciones que utilizan se gestionan de forma adecuada y no han tenido mayor inconveniente de seguridad al utilizarlos estas herramientas en sus actividades diarias. Sin embargo, en la figura 4.20 se puede visualizar que el 60% de los funcionarios que utilizan los activos informáticos no se sienten seguros con la seguridad en la red de datos.

4.2. Información obtenida mediante entrevista al Director

4.2.1. Requisitos obligatorios del SGSI

Tabla 4.21
Resultado de evaluación del estado de las cláusulas obligatorias del SGSI del GADMCE

Sección (cláusula)	Requisito ISO/IEC 27001	Grado de cumplimiento	Estado
4	Contexto de la organización	20,00%	Inicial
5	Liderazgo	60,00%	Definido
6	Planificación	33,33%	Limitado
7	Soporte	32,00%	Limitado
8	Operación	13,33%	Inicial
9	Evaluación del desempeño	0,00%	Inexistente
10	Mejora	10,00%	Inicial
	Promedio general	24,10%	

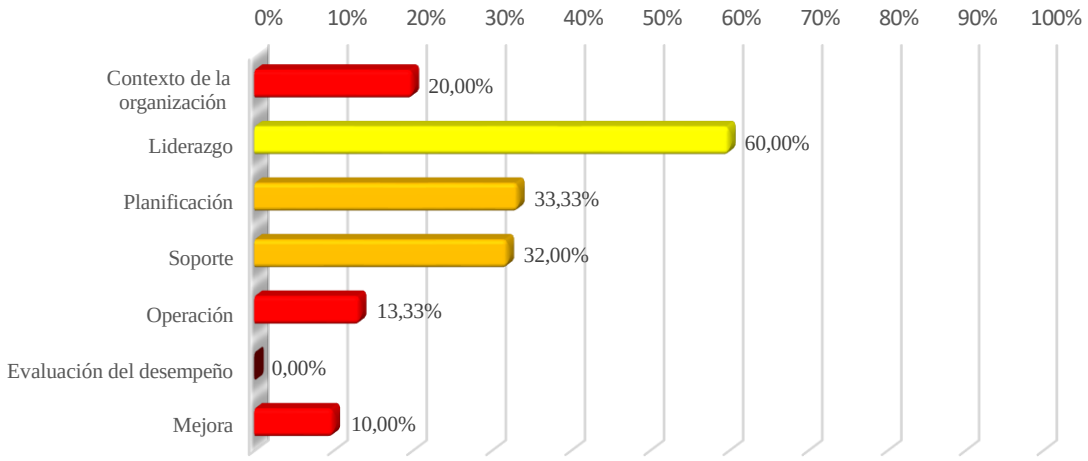


Figura 4.21. Grado de cumplimiento de los requisitos obligatorios ISO 27001:2022

La tabla 4.21 el estado de cada una de las cláusulas de los requisitos obligatorios que debe tener un SGSI, en el caso del GADMCE en la entrevista de evaluación realizada al director de TIC se obtuvo un promedio general de 24.10%. En la figura 4.21 se grafica el grado de cumplimiento de cada sección o clausula, en donde se evidenció el incumplimiento en sus secciones, a excepción de número cinco (liderazgo), siendo esta

la mejor evaluada con un estatus de “definida” debido a que su desarrollo parcialmente cumplido. y este SGSI no está aún implementado, ni ha sido avalado por la máxima autoridad; por lo tanto, el estado general de este parámetro es de “inicial”, es decir: su desarrollo apenas ha iniciado y requiere completar una serie de actividades para cumplir a satisfacción los requisitos establecidos por la normativa. En el anexo B se puede apreciar mejor la ponderación asignada a cada parámetro y el cálculo realizado para cuantificar en base al estado de cumplimiento de cada clausula, el nivel de madurez del SGSI de la institución.

4.2.2. Controles de seguridad de la información

Tabla 4.22
Resultado general por categorías del cumplimiento de los controles del SGSI del GADMCE

Controles	Cumplimiento			
	Frecuencia		Porcentaje	
	Si	No	Si %	No %
Organizacionales	7	30	18,92	81,08
Personales	3	5	37,50	62,50
Físicos	9	5	64,29	35,71
Tecnológicos	13	21	41,18	58,82
Total	32	61	34,41	65,59

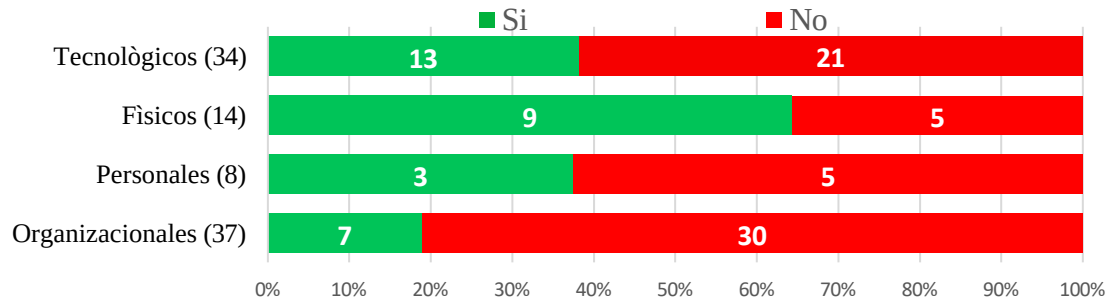


Figura 4.22. Cumplimiento de controles ISO 27001:2022 por categorías

En la tabla 4.22 se resume (por categorías) el resultado de la evaluación de cumplimiento de los 93 controles de seguridad establecidos en la norma ISO 27001 en sus anexos del 2022 en donde se evidencia que solo se cumplen 32 de los 93 controles definidos por la normativa, es decir el 34%. Existiendo un 66% de incumplimiento en este parámetro, observando la figura 4.22 este incumplimiento se da en los controles organizacionales, ya que apenas se cumple en un 19% de estos. De las cuatro categorías en que están clasificados lo controles por la norma, se observó que solo en el caso de los controles físicos se tiene un nivel de cumplimiento satisfactorio al cumplirse 9 de los 14 controles establecidos, es decir el 64%. A continuación, se presenta un resumen y análisis

general por cada categoría de controles y el detalle del estado de cumplimiento en base a las evidencias y soportes presentados por el Director de TIC, es decir su nivel de madurez.

Tabla 4.23
Resultado de la evaluación del estado de cumplimiento de los controles por categorías

Categoría	No existe	Inicial	Limitado	Definido	Gestionado	Optimizado	Total
Organizacional	9	14	7	1	4	2	37
Personales	1	2	2	1	1	1	8
Físicos	3	1	1	2	6	1	14
Tecnológicos	6	10	5	3	9	1	34
Total	20	26	15	6	21	5	93

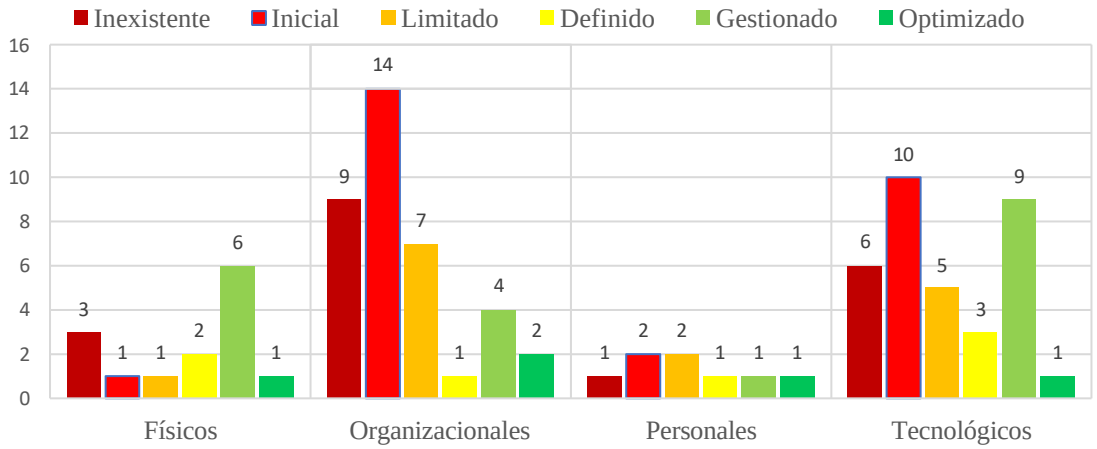


Figura 4.23. Grado de cumplimiento (estado) de controles ISO 27001:2022 por categorías

En la tabla 4.23 se presenta la distribución de los controles de seguridad clasificados por categoría y por estado o grado de cumplimiento. Se pudo constatar el elevado número de controles en estado “inexistente”, “inicial” o limitado, es decir que no se cumplen de manera satisfactoria en la institución. Eso se aprecia de mejor manera en la figura 4.23 en donde al estar presentadas sus distribuciones de manera porcentual se observó que solo en la categoría de controles físicos se cumple en más de la mitad de los controles, y por el contrario se visualiza que, en las tres categorías restantes, sobre todo en los controles organizacionales se encuentran la mayoría de no conformidades.

En el anexo B, se presentan el detalle de todos los parámetros analizados para cada uno de los 93 controles y el grado de cumplimiento asignado en función de la evaluación realizada, es decir su nivel de madurez. En dicho anexo consta la evidencia presentada por el Director de TIC, el cuestionario utilizado en la entrevista con la pregunta evaluatoria de cada control, y la respuesta con la información sistematizada.

4.2.3. Sistema de Gestión de Seguridad de Información

Tabla 4.24
Nivel de madurez Grado de cumplimiento Controles Organizacionales

Estado	Significado del estado	Requisitos obligatorios	Controles Anexo A
Inexistente	Ausencia completa o legible de una política, procedimiento, normativa, proceso, control, etc.	26,09%	20,43%
Inicial	Apenas ha comenzado su desarrollo, y requerirá de un trabajo considerable para satisfacer los requisitos requeridos	39,13%	29,03%
Limitado	Evidencia avance, progresando bien pero no se evidencia se esté completado aún, o que falte poco para terminar	17,39%	16,13%
Definido	El desarrollo está más o menos completo aunque con ausencia de detalles y/o no está aún implementado, en cumplimiento, vigente, ni activamente avalado por la alta dirección	17,39%	7,53%
Gestionado	El desarrollo está completo, el proceso / control ha sido implementado y recientemente comenzó a operar	0,00%	21,51%
Optimizado	El requisito está plenamente conforme y terminado, está plenamente operativo como se espera, está siendo activamente supervisado y mejorado, y hay evidencia sustancial para demostrar todo lo antedicho a los auditores	0,00%	5,38%
	Total	100,00%	100,00%

Nota: Tomado de ISO27001security (2022)

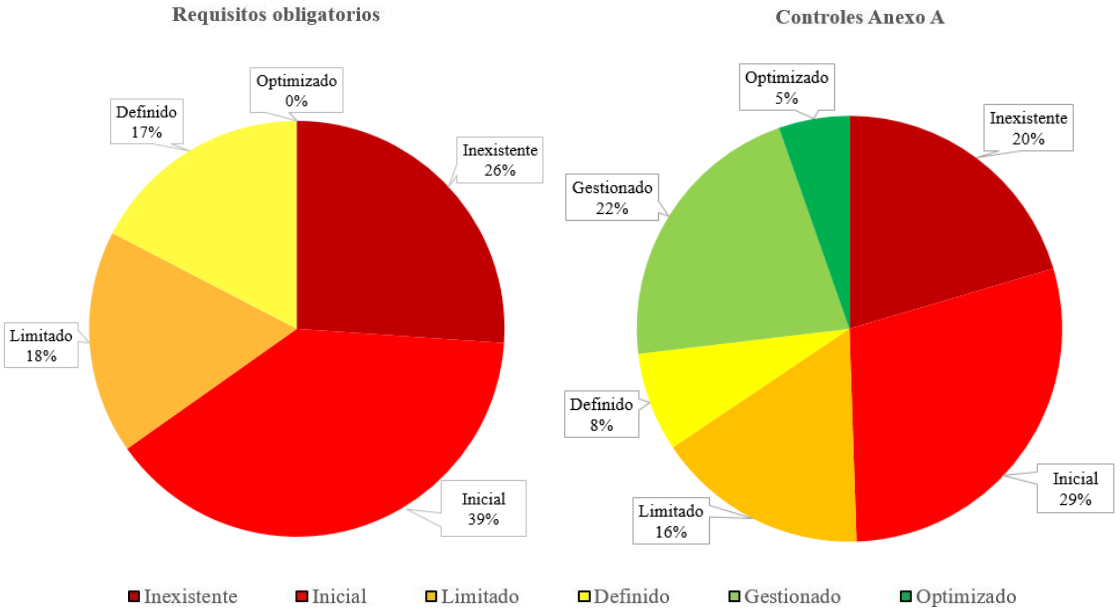


Figura 4.24. Comparativo de cumplimiento SGSI: Requisitos obligatorios VS Controles

La tabla 4.23 presenta un resumen comparativo del resultado de la evaluación de los cada una de las clausulas consideradas como requisitos obligatorios del SGSI versus los controles (mecanismos) de seguridad establecidos en la ISO 27001:2022. Siendo el nivel de madurez o estados de la medición mucho más baja en el primer caso con 19 de 23 cláusulas de incumplimiento representando el 82,61% del total de requisitos

obligatorios evaluados, e incluso sin ningún parámetro en estado de cumplimiento gestionado u óptimo, la única cláusula en donde se cumple con un estado de "definido" es el número 5, correspondiente a liderazgo. En el segundo pastel, se representa el nivel de cumplimiento de los controles establecidos en el anexo de la norma, como se puede apreciar la cantidad de controles que sí cumplen son 32 del total de 93, y constituye un 34,41% del total de controles evaluados. En la figura 4.24 se puede apreciar mejor la proporción de cumplimiento (optimo, gestionado o definido) y de incumplimiento (inexistente, inicial o limitado) para cada uno de los dos aspectos evaluados, sin embargo, para comprender de mejor forma el detalle de los resultados es necesario revisar el instrumento de evaluación de las clausulas obligatorias del SGSI y la matriz de levantamiento de información de los controles del SGSI, ambos se encuentran al final de este documento como anexo A y anexo B respectivamente.

4.3. Información obtenida mediante entrevistas a funcionarios de TI

4.3.1. Matriz de valoración del riesgo informático

Tabla 4.25
Evaluación del riesgo informático

	Impacto				Probabilidad		Riesgo	
Activo	C	I	D	CID	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación	Nivel
C01	3	3	3	3,00	2	2	12,00	Alto
C02	3	3	3	3,00	3	1	9,00	Medio
C03	3	3	3	3,00	2	1	6,00	Medio
C04	1	1	3	1,67	2	2	6,67	Medio
C05	1	1	3	1,67	2	3	10,00	Alto
C06	1	1	3	1,67	2	2	6,67	Medio
C07	1	1	3	1,67	2	2	6,67	Medio
C08	1	1	3	1,67	2	2	6,67	Medio
C09	1	1	3	1,67	1	3	5,00	Medio
C10	1	1	3	1,67	2	2	6,67	Medio
C11	1	1	3	1,67	2	3	10,00	Alto
C12	1	1	3	1,67	2	2	6,67	Medio
C13	3	3	3	3,00	1	3	9,00	Medio
C14	2	3	3	2,67	2	3	16,00	Alto
C15	3	3	2	2,67	3	2	16,00	Alto
C16	3	2	2	2,33	2	2	9,33	Alto
C17	2	3	2	2,33	3	2	14,00	Alto
C18	2	3	2	2,33	2	2	9,33	Alto
C19	2	1	3	2,00	2	2	8,00	Medio
C20	3	3	2	2,67	2	2	10,67	Alto
C21	1	1	3	1,67	2	1	3,33	Bajo
C22	1	1	3	1,67	2	2	6,67	Medio
C23	1	1	3	1,67	3	2	10,00	Alto
C24	2	3	1	2,00	3	2	12,00	Alto
C25	1	2	3	2,00	2	3	12,00	Alto
C26	1	1	1	1,00	2	3	6,00	Medio

C27	2	3	3	2,67	2	2	10,67	Alto
C28	1	1	2	1,33	2	2	5,33	Medio
C29	2	3	3	2,67	3	2	16,00	Alto
C30	1	1	2	1,33	3	2	8,00	Medio
C31	2	3	3	2,67	2	2	10,67	Alto
C32	2	2	2	2,00	2	2	8,00	Medio
C33	1	1	2	1,33	2	2	5,33	Medio
C34	1	1	3	1,67	3	3	15,00	Alto
C35	1	1	2	1,33	2	1	2,67	Bajo
C36	1	1	2	1,33	2	2	5,33	Medio
C37	2	1	3	2,00	1	2	4,00	Medio
C38	1	1	2	1,33	1	2	2,67	Bajo
C39	1	2	3	2,00	1	3	6,00	Medio
C40	2	3	2	2,33	2	2	9,33	Alto
C41	1	1	3	1,67	2	2	6,67	Medio
C42	1	1	3	1,67	3	3	15,00	Alto
C43	2	2	3	2,33	2	2	9,33	Alto
C44	1	1	1	1,00	3	3	9,00	Medio
C45	3	3	3	3,00	3	1	9,00	Medio
C46	2	2	1	1,67	2	1	3,33	Bajo
C47	3	1	1	1,67	2	2	6,67	Medio
C48	2	2	1	1,67	2	2	6,67	Medio
C49	1	1	1	1,00	2	2	4,00	Medio
C50	3	3	3	3,00	1	2	6,00	Medio

Nota. En el anexo B se detalla la matriz de valoración más completa, pero por temas de seguridad se han omitido algunos parámetros que contenían información considerada confidencial y la valoración monetaria, que fueron parte del análisis y evaluación del riesgo informático, pero no pueden ser incluidos en este informe. También se incluye en el anexo E, el modelo de entrevista que se aplicó a los funcionarios de la Dirección de TIC.

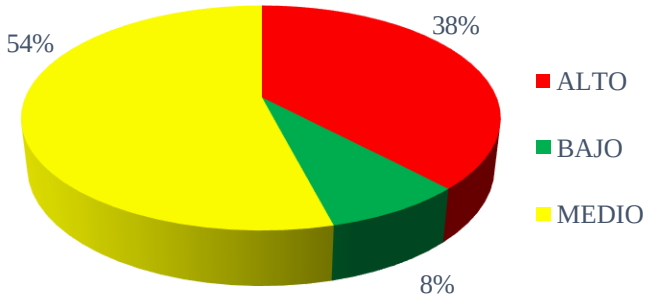


Figura 4.25. Nivel de riesgo de los activos informáticos del GADMCE

En la tabla 4.25 se evidencia en resumen los 50 activos informáticos considerados como críticos, en donde se concentra el 90% del valor monetario, y de los cuales se evidencia en la figura 4.25 que el 38% presenta un alto riesgo de seguridad. En el anexo E se puede corroborar que los equipos con alto riesgo representan monetariamente el 59% del total del inventario de activo informático de la institución por lo que se hace imperiosa la aplicación de controles como medidas de tratamiento para los riesgos determinado en la evaluación. De esa muestra con la que se desarrollaron los análisis de riesgo informático los activos que presentan bajo riesgo apenas representan el 8 del total y equivalen el 2% del valor monetario total. Lo que significa que los mecanismos implementados por la Dirección de TIC, no están incidiendo en la seguridad de tecnólogas de información del GADMCE.

4.3.2. Normas de Control Interno 410

Tabla 4.26
Nivel de confianza y nivel de riesgo del control interno institucional

Norma	Descripción	Nivel de Confianza	Nivel de riesgo
410-01	Organización de la unidad de TIC	80,00%	BAJO
410-02	Comité de Tecnologías de la Información y Comunicación	20,00%	ALTO
410-03	Segregación de funciones	56,00%	MEDIO
410-04	Plan estratégico y operativo de TIC	40,00%	ALTO
410-05	Políticas y procedimientos	37,14%	ALTO
410-06	Clasificación y arquitectura de la información	25,00%	ALTO
410-07	Administración de proyectos tecnológicos	32,50%	ALTO
410-08	Desarrollo, mantenimiento y adquisición de software	30,67%	ALTO
410-09	Adquisiciones de infraestructura tecnológica	32,50%	ALTO
410-10	Mantenimiento, actualización y control infraestructura Tec.	33,33%	ALTO
410-11	Seguridad de tecnología de información	37,14%	ALTO
410-12	Plan de contingencias	22,50%	ALTO
410-13	Administración de soporte de tecnología de información	33,85%	ALTO
410-14	Monitoreo y evaluación de los procesos y servicios	24,00%	ALTO
410-15	Portal web, servicios telemáticos e intranet	65,00%	MEDIO
410-16	Capacitación relacionada a las TIC	35,00%	ALTO
410-17	Firmas electrónicas	64,00%	MEDIO
	Promedio nivel de confianza	39,33%	ALTO

Fuente: GADMCE - Instrumento de evaluación de la CGE

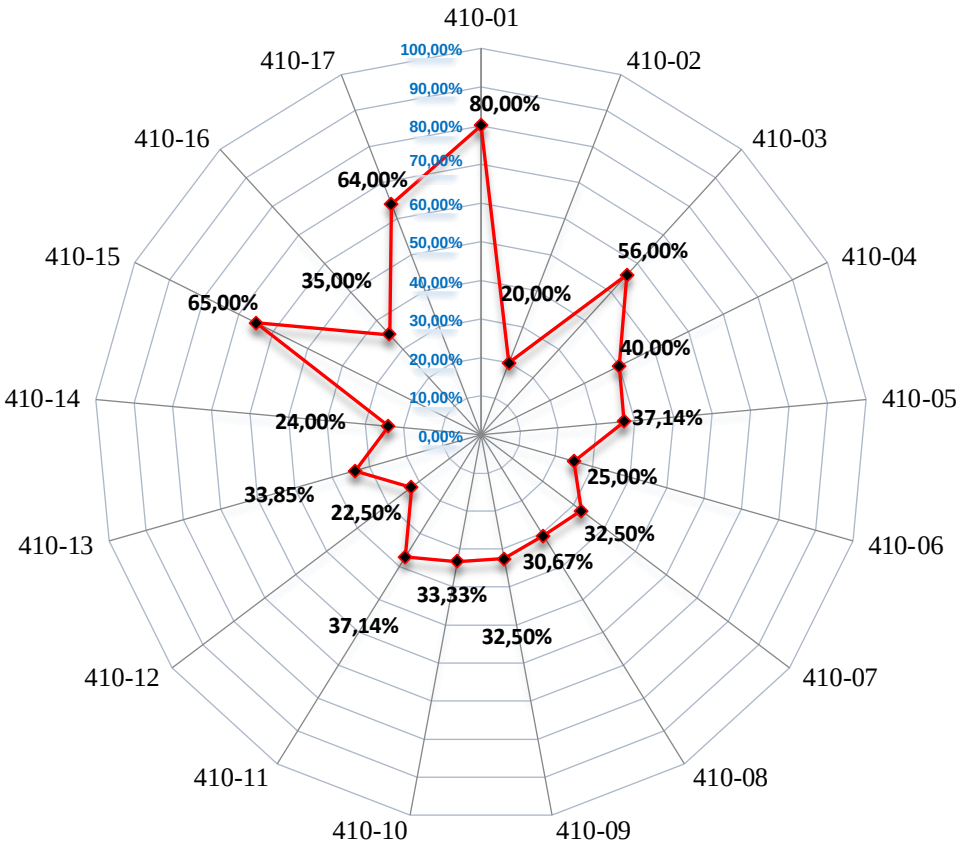


Figura 4.26. Nivel de confianza del ambiente de control - norma 410
Fuente: GADMCE 2024 – Elaboración propia

La tabla 4.26 contiene el resumen cuantificado de la entrevista de evaluación de cada una de las normas de tecnología de información realizada al Director y funcionarios responsables de cada proceso de TI. Como se puede notar, la única norma valorada con un nivel de confianza alto es la 410-01, lo que implica un nivel de riesgo bajo en lo relacionado con la organización de la unidad de TIC en el GADMCE. Así mismo, se pudo identificar que solo 3 normas (410-03, 410-15 y 410-17) tienen un nivel de riesgo medio; y, por el contrario, se pudo establecer que 13 de las 17 normas evaluadas tienen un nivel de riesgo alto, es decir el (76,47%).

A partir de la figura 4.26 representada en el gráfico radial, se deducen los niveles de confianza determinados para cada una de las variables, es decir las 17 normas (presentados en detalle en el informe de auditoría del siguiente capítulo), obteniendo un nivel de confianza (grado de cumplimiento) de 39.33 lo que implica un riesgo informático alto. El detalle de cada cuantificación se puede revisar en el anexo F, en él también se detalla para cada control evaluado, el medio de verificación que se utilizó o que se presentó como evidencia por parte de la Dirección de TIC y que se contrasto con las respuestas de las encuestas de los funcionarios.

4.4. Información obtenida mediante Observación

4.4.1. Activos informáticos

Se extrajo del sistema de control de bienes los registros de todos los activos informáticos (computadoras, periféricos, software, programas, equipo de redes, aplicaciones, servidores, equipos de seguridad, entre otros). En los casos de activos en bodega se pudo constatar información adicional del activo, como son: el valor nominal registrado, fecha de adquisición, custodio administrativo, fecha de asignación, y, según el caso, el valor invertido en el mismo. En el anexo E se presenta parte del listado de las informaciones extraídas del programa SIGAME.

Se pudo revisar el software y los programas instalados en los equipos de cómputo, con sus respectivas licencias en el caso del antivirus, sistema CABILDO y otras aplicaciones de los servidores y equipo de redes que se utilizan. Se visitó el área de bodega en donde se almacenan los repuestos de partes y piezas utilizadas para el mantenimiento correctivo. Se constató la existencia del plan de mantenimiento preventivo con su cronograma, pero no se pudo evidenciar el seguimiento o cumplimiento del mismo.

4.4.2. Instalaciones y dependencias

Se puedo observar la inexistencia de procedimientos formales de seguridad relacionada con la infraestructura tecnológica en las instalaciones y dependencias de la institución, sobre todo por parte del personal que trabaja en la institución fuera de los horarios laborales, significando un alto riesgo de seguridad. A pesar que existe un servidor de dominio no existe un control de las pantallas y escritorios de cada uno de los equipos que son parte de la red, en la mayoría de casos los computadores tenían contraseñas y bloqueado las pantallas con contraseñas, pero a nivel de usuario administrativo. La licencia del antivirus que se utiliza estaba por fenecer y todavía no se había realizado el proceso de contratación lo que supone un alto riesgo de seguridad en caso de algún retraso en la adquisidor o activación de la licencia.

No Existe una bitácora de control de acceso al área de los servidores (datacenter), si bien existe un sistema de monitoreo por medio de video, no existe un funcionario formalmente responsable del registro de incidentes y la bitácora a cargo de los guardias de seguridad física no tienen una supervisión periódica, ni procedimiento de evaluación de dichos registros. La mitad de los edificios se encuentran conectados a través de fibra óptica y poseen una topología bus estrella. En el caso de los demás edificios presentan problemas en la red y solo el 50% de las instalaciones tienen cableado estructurado, ninguno de los puntos de red cuenta con algún tipo de certificación y la mayoría del cableado es categoría 5e. No se evidenciar la existencia de planos con el inventario de los puntos de red. Si bien existía una bitácora con el inventario de las direcciones IP, extensiones telefónicas, parque informático, parque de impresión, e inventario de aplicaciones, los registros se manejan de manera aislada del sistema informático principal. No se lleva una bitácora de la limpieza del área de servidores y su frecuencia. En el anexo G se adjunta evidencia fotográfica de las visitas.

4.4.3. Datacenter institucional

Existe un datacenter portable que integra energía limpia (UPS), climatización, monitoreo y video vigilancia, además de la seguridad física de los servidores. La climatización del cuarto en donde se encuentra instalado del Datacenter cuenta con protección eléctrica y cableado estructurado. El acceso a estas instalaciones es restringido a personal específico de la Unidad de Infraestructura Tecnológica además de cerraduras

en el rack para limitar el acceso físico a los servidores y los equipos de red. Sin embargo, el Data Center no ha recibido mantenimiento especializados desde hace más de un año lo que supone un riesgo ya que ahí residen siete servidores virtuales y cuatro servidores físicos para los sistemas de aplicaciones como son: Cabildo ERP, SIGAME, Intranet, Base de Datos, SISCAL, Sistema de hoja de ruta, Antivirus, firewall, Monitoreo CCTV, entre los principales. En el anexo G se presenta evidencia fotográfica de la visita técnica realizada.

4.4.3. Infraestructura tecnológica de la ciudad

Se visitó las instalaciones del proyecto de adquisición de infraestructura tecnológica para la ciudad, denominado Esmeraldas Ciudad Inteligente, con interoperabilidad al ECU 911; evidenciando la operación y funcionamiento de los diversos sistemas como son cámaras IP, redes públicas de conectividad inalámbrica, sensores medioambientales, sistemas de botones de pánico y perifoneo que se encuentran integrados a una sala denominada Centro Integrado de Operación y Control Esmeraldas (CIOCE), el cual concentra a través de una red de fibra óptica de aproximadamente 100 kilómetros desplegada en toda la ciudad, alrededor de 80 puntos, constituyendo un sistema para la gestión y monitoreo de las competencias municipales, de sus unidades adscritas y empresas públicas concebido originalmente para de mejorar la seguridad, movilidad, y servicios públicos (sobre todo la recolección de la basura). Pero que en la actulidad se encuentra sub utilizado debido a la falta de recursos: personal, presupuesto, instalaciones físicas y mantenimiento. Los activos informáticos se encuentran agrupados en los componentes resumidos en la tabla 1.1 que se presentó en el capítulo 1. En el anexo G se puede constatar la visita tanto al CIOCE como a uno de los 80 puntos de la ciudad.

4.5. Resultados

Como se ha evidenciado a lo largo de este capítulo, con la evaluación realizada al SGSI del GADMCE, se ha podido analizar la infraestructura tecnológica existente y verificar si los mecanismos implementados por la Dirección de TIC aseguran el cumplimiento de la normativa legal vigente. A través de la norma ISO 27001:2022 se pudo determinar que, en términos generales de seguridad, la institución se encuentra en un nivel de madurez inicial, del análisis cuantitativo que se ha realizado a través de las encuestas y entrevistas, se desprende que en el caso de los requisitos obligatorios se

cumple 1 de 7 cláusulas, y en el caso de los controles de seguridad se cumplen 32 de 93 controles, promediando entres estos dos parámetros alrededor del 20% de cumplimiento. Esto se debe a que la institución no tiene implementado formalmente un SGSI, ya sea a través de algún estándar de la industria o utilizando el esquema gubernamental que desde el MINTEL se ha expedido.

La institución cuenta con un activo informático considerable que en su mayor parte es patrimonio de la ciudad (infraestructura del proyecto de Ciudad Inteligente), eso se pudo evidenciar al evaluar la seguridad de la institución a nivel de parque informático, software, almacenamiento, redes y comunicaciones a través de la matriz de valoración del riesgo informático que se elaboró y estableció con los mismos servidores públicos que laboran en la Dirección de TIC, constituyéndose en el punto de partida para poder implementar controles para el SGSI institucional que aseguren el cumplimiento de las NCI 410 relacionadas con las TIC. Por lo tanto la realización de auditorías internas y evaluaciones periódicas de las políticas de seguridad y del propio SGSI mitigan los riesgos de que las distintas amenazas a las que la institución se encuentra expuesta y sus vulnerabilidades materialicen una daño irreversible, irreparable o grave en sus activos de información; y por el contrario sea a través del informe de auditoría la oportunidad de mejora para proponer e implementar políticas de seguridad de la información que permitan implementar los controles necesarios para gestionar de los recursos de TI, garantizar la continuidad de los servicios instituciones y salvaguardar los activos de información existentes.

Al realizar la evaluación del sistema de control interno institucional a través del instrumento de la CGE de se obtuvo un nivel de confianza de alrededor del 39%, asociado a un nivel de riesgo “alto” según lo establecido por esa metodología, la cual se encuentra a detalle en el anexo F. Este resultado guarda similitud con el bajo nivel de cumplimiento obtenido en la evaluación de los requisitos obligatorios del SGSI que fue de 30.48%, y de los controles de seguridad de la información establecidos en el anexo de la norma ISO 27001:2022, que también significó un bajo grado de cumplimiento del 35%, el detalle de la cuantificación de cada uno de estos resultados se encuentra al final de este documento en el anexo A y anexo B respectivamente.

En un análisis adicional, si consideramos que la ponderación utilizada por la CGE para cuantificar cada factor, asigna un valor al mínimo estado posible (incipiente), al no

estar normalizado con las métricas utilizadas en los instrumentos de la norma ISO 27001:2022, genera una diferencia significativa que incide en aproximadamente un 10%, es decir en base el criterio de los niveles de madurez antes calculados el resultado sería de un 29%, coincidiendo con el resultado de evaluación para el SGSI, es decir: estado inicial o básico.

El GADMCE, carece de procedimientos y metodologías para evaluar o auditar su SGSI, y a pesar que no existe una receta o fórmula sobre las tareas, el tiempo y los recursos que se deben asignar para solventar cada una de las limitaciones que se han podido diagnosticar en esta fase; lo que sí existe, y son de cumplimiento obligatorio, son las normas de control de la CGE, sobre todo la norma 410 que engloba a 17 normas que abarcan la gestión de TIC. Es por ello que al realizar la evaluación del SGSI y la auditoría del sistema de control interno institucional se podrá validar una de las hipótesis planteadas en esta investigación, y entregar dos productos que serán de mucha utilidad para la Dirección de TIC y por ende la institución: el informe de auditoría y un plan de mejora, que incluyan los hallazgos, conclusiones y recomendaciones en el caso del informe de auditoría, y las políticas de seguridad de la información en el caso del plan de mejora.

Por todo lo descrito anteriormente, se ratifica lo expuesto siendo necesario la elaboración de un informe de auditoría del GADMCE basado en las normas de control interno de la Contraloría, en donde a través de instrumentos de sistematización de la información obtenida, se incluyan los hallazgos, con sus respectivas conclusiones y recomendaciones de las no conformidades e incumplimientos detectados, de manera que se proponga a la Dirección de TIC un plan de mejora a través de la implementación de políticas de seguridad de la información en la institución.

A continuación, se presenta el informe final, en donde solo se incluyen los hallazgos más relevantes y las recomendaciones para subsanar los incumplimientos. En el anexo I que se incluye al final se ha elaborado un acta con el resumen de las no conformidades en donde se ha codificado en función del número de norma y el número de recomendación establecida para esa norma; de manera que dicho documento pueda ser presentado la máxima autoridad y al consejo en pleno para su aprobación y ejecución, pues incluye también el responsable del tratamiento y el tiempo de cumplimiento sugerido por el auditor. Esa información ha sido consensuada con el Director de TIC, y la firma como delegado de la máxima autoridad el Coordinador General de la institución.

CAPITULO V
INFORME DE AUDITORIA Y PLAN DE MEJORA

5.1. Informe de auditoría del sistema de control interno institucional

5.1.1. Organización de la unidad de TIC (Norma 410-01)

Tabla 5.1
Evaluación Control Interno - Norma técnica aplicada: 410-01

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01					X	25,00	Estructura Orgánica
02					X	25,00	Estructura Orgánica
03					X	25,00	Estructura Orgánica
04	X					5,00	Ninguna
Total	1	0	0	0	3	80,00	

Conclusiones

La estructura organizacional del GADMCE tiene una unidad de TIC formalmente establecida en el estatuto orgánico por procesos al más alto nivel que le permite asesorar a la máxima autoridad y apoyar a las demás direcciones usuarias. La facultad establecida para la unidad de TIC contempla los temas tecnológicos, y su estructura refleja las necesidades institucionales, a través de los cuatro subprocesos definidos: proyectos, infraestructura, soporte, y aplicaciones; sin embargo, el Alcalde al no haber incorporado o designado un funcionario como oficial de seguridad de la información incumplió lo establecido en el artículo 48 de la ley de protección de datos personales, comprometiendo la seguridad de los datos personales que maneja la institución. Tampoco existe un área independiente de la unidad de TIC para que este oficial de seguridad este a cargo, como lo exige la normativa legal vigente.

Recomendaciones

El Alcalde, en calidad de máxima autoridad deberá designar un funcionario como Oficial de Seguridad de la Información (OSI) de un área independiente de la unidad de TIC. Esta designación deberá ser comunicada a la Subsecretaria de Gobierno Electrónico y Registro Civil del MINTEL.

5.1.2. Comité de TIC (Norma 410-02)

Tabla 5.2
Evaluación Control Interno - Norma técnica aplicada: 410-02

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01	X					4,00	Ninguna
02	X					4,00	Ninguna
03	X					4,00	Ninguna
04	X					4,00	Ninguna
05	X					4,00	Ninguna
Total	5	0	0	0	0	20,00	

Conclusiones

No se ha creado el Comité de TIC en función del tamaño y la necesidad institucional del GADMCE con la finalidad de coordinar los objetivos, alcance, y normativa para el desarrollo de los proyectos relacionados con el uso de las TIC y la implementación del Esquema Gubernamental de Seguridad de la Información. Por lo tanto, la máxima autoridad incumple la norma de control interno 410-02, el artículo 6 del acuerdo ministerial Nro. MINTEL-MINTEL-2024-0003, y el resto de criterios establecidos en esta norma relacionados a las funciones, enfoque e integración de este comité, agravando los riesgos de seguridad de la información en la institución.

Recomendaciones

El Alcalde deberá articular la creación del Comité de TIC, tal como lo establece la CGE (2023), es decir bajo un criterio unificado para la ejecución de uno o varios de los procesos institucionales, considerando lo establecido en la norma 410-02 y el acuerdo ministerial Nro. MINTEL-MINTEL-2024-0003, incluyendo las entidades adscritas y otras instituciones que la conforman.

El comité deberá estar conformado por los Directores de las siguientes áreas: planificación, talento humano, comunicación social, administrativa, TIC, y jurídica; además del delegado de protección de datos. Este comité tendrá como objetivo principal el garantizar la implementación de seguridad de la información en la institución, y será el responsable del control y seguimiento de su aplicación institucional (CGE, 2023).

5.1.3. Segregación de funciones (Norma 410-03)

Tabla 5.3
Evaluación Control Interno - Norma técnica aplicada: 410-03

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01				X		16,00	Estatuto Orgánico
02				X		16,00	Manual de puestos
03		X				8,00	Informe de necesidad de nuevo personal
04			X			12,00	Evaluación de desempeño anual
05	X					4,00	Ninguna
Total	1	1	1	2	0	56,00	

Conclusiones

Las responsabilidades y funciones de los empleados de la Dirección de TIC están definidas en el estatuto orgánico por procesos, pero de forma parcial, debido a que en algunos casos no fueron comunicadas formalmente. El Director de Talento Humano al inobservar lo dispuesto por la norma 410-03 ocasionó que en la evaluación de desempeño no se incluya todo el personal de la Dirección de TIC y que algunos funcionarios no consten en el estatuto orgánico funcional por procesos. Los usuarios de los sistemas informáticos como CABILDO, SIGAME o SISCAL no han sido formalmente establecidos por lo que El Director de TIC a inobservado la norma 410-02 ocasionando que no existan responsable formales de esos sistemas.

Recomendaciones

El Director de TIC deberá formalizar la asignación de todos los usuarios de los sistemas en base a los perfiles de cada funcionario, a través de actas de entrega/recepción de alta que deberán ser firmadas por las partes, y garantizar el ciclo de vida de las identidades.

El Director de Talento Humano deberá actualizar el estatuto orgánico por procesos de manera que se regularice la situación de los trabajadores bajo el código de trabajo que tienen funciones administrativas en la Dirección. Además, deberá crear el cargo de Oficial de Seguridad para cumplir las funciones establecidas en el Acuerdo Ministerial Nro. MINTEL-MINTEL-2024-0003.

5.1.4. Plan estratégico y operativo de TIC (Norma 410-04)

Tabla 5.4
Evaluación Control Interno - Norma técnica aplicada: 410-04

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01	X					2,86	Ninguna
02	X					2,86	Ninguna
03	X					2,86	Ninguna
04			X			8,57	POA 2024
05			X			8,57	POA 2024
06		X				8,57	POA 2024, No existe plan estratégico
07			X			8,57	Reforma POA 2024
Total	3	1	3	0	0	40,00	

Conclusiones

El Director de TIC al no haber elaborado e implementado un plan estratégico informático incumple la norma 410-04, ocasionando que la institución no cuente con una planificación que organicen los recursos existentes. No existe un plan estratégico institucional, pero se han elaborado planes operativos anuales en donde se incluye los proyectos, servicios, arquitectura con su respectivo presupuesto. Las modificaciones del POA han sido autorizadas por el Alcalde, y han sido sometidas al trámite de reforma pertinente, pero la mayoría de estos trámites tienen demora.

Recomendaciones

El Director de TIC debe elaborar un plan estratégico informático, alineado a la planificación estratégica de la institución y a la planificación de desarrollo del Gobierno Nacional. Se deberá incluir un análisis FODA y las propuestas de mejora en coordinación con las otras direcciones del GADMCE, El plan informático deberá cumplir lo que establece la Contraloría, y "considerar la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, análisis de riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario" (CGE, 2023).

El Director de TIC deberá presentar el plan informático para su aprobación por parte de la máxima autoridad, y una vez sea aprobado deberá ser socializado a lo interno de la institución y monitoreado de manera periódica por el Director.

5.1.5. Políticas y procedimientos (Norma 410-05)

Tabla 5.5
Evaluación Control Interno - Norma técnica aplicada: 410-05

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01	X					2,86	políticas de Seguridad sin aprobación
02			X			8,57	políticas de Seguridad
03	X					2,86	políticas de Seguridad actualizadas
04			X			8,57	políticas de Seguridad revisadas
05	X					2,86	Ninguna
06	X					2,86	Ninguna
07			X			8,57	Convenios: ECU 911, PUCESE DINARDAT, UTLV
Total	4	0	3	0	0	37,14	

Conclusiones

Las políticas y procedimientos de tecnología de información no han sido aprobadas formalmente por la máxima autoridad. Tampoco estableció algún procedimiento de difusión o comunicación, que permitan conocer a los funcionarios y usuarios de los sistemas. El Director de TIC incumplió la norma 410-05, ocasionando que los funcionarios desconozcan las políticas, normas y procedimientos de seguridades de los sistemas y tecnologías.

El Director de TIC presentó un documento con las Políticas de Seguridad, pero solo se evidencio el cumplimiento a nivel de la dirección, y no del resto de direcciones del GADMCE, es decir no se encuentren incorporadas formalmente en los procesos de la institución ocasionando que no existan controles, ni seguimiento al cumplimiento por parte de los usuarios de los sistemas y recursos tecnológicos.

Recomendaciones

El Alcalde debe establecer y aprobar las políticas de seguridad de la Información demostrando liderazgo y compromiso en el cumplimiento de los establecido en la misma, para lo cual deberá solicitar al Director de TIC la presentación de una propuesta.

El Director de TIC debe actualizar y difundir permanentemente las políticas y procedimientos de seguridad de los sistemas y tecnologías de información, incluyendo las tareas, los responsables, las excepciones y las sanciones en caso de incumplimiento.

5.1.6. Clasificación y arquitectura de la información (Norma 410-06)

Tabla 5.6
Evaluación Control Interno - Norma técnica aplicada: 410-06

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01	X					5,00	Ninguna
02	X					5,00	Ninguna
03		X				10,00	Elaboración de Diccionario de datos
04	X					5,00	Ninguna
Total	3	1	0	0	0	25,00	

Conclusiones

A pesar de constar en los productos de la Dirección de TIC, El Director de TIC no ha definido un proceso de clasificación y arquitectura de la información de manera que se puedan aplicar niveles de seguridad y propiedad para asegurar una eficiente organización de los datos. Esta función se encuentra establecida en el estatuto orgánico por procesos y en el perfil de puestos correspondiente al Analista Junior de Aplicaciones y Sistemas. Por lo que el Analista Junior de Aplicaciones y Sistemas inobservo la norma 410-06, ocasionando que la Dirección de TIC no tenga un modelo de información y tampoco adopte los controles necesarios para dar cumplimiento a la normativa legal vigente.

Recomendaciones

El Director debe supervisar que funcionario responsable de la arquitectura y clasificación de la información de la institución: defina, documente y actualice el diccionario de datos de los sistemas y aplicaciones desarrollados o adquiridos por el GADMCE.

El Analista Junior de Aplicaciones y Sistemas debe incluir en el diseño de la arquitectura de la información las reglas de validación y los controles de integridad y consistencia; con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente (CGE,2023).

5.1.7. Administración de proyectos tecnológicos (Norma 410-07)

Tabla 5.7
Evaluación Control Interno - Norma técnica aplicada: 410-07

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01	X					2,50	Ninguna
02		X				5,00	Contrato BDE
03	X					2,50	Ninguna
04			X			7,50	Contrato BDE
05	X					2,50	Ninguna
06	X					2,50	Ninguna
07	X					2,50	Ninguna
08			X			7,50	Informe BDE
Total	5	1	2	0	0	32,50	

Conclusiones

El Director de TIC no definió una metodología para administrar los proyectos de tecnología que ejecuten los subprocesos o unidades técnicas que conforman la dirección. No se consideró el costo total de propiedad de los proyectos, Por lo tanto, incumplió la norma 410-07 ocasionando que no exista una adecuada gestión de riesgos que permitan implementar mecanismos de seguridad de la información.

A pesar que se evidencio que en el caso del proyecto de Ciudad Inteligente se asignó formalmente un servidor público con la descripción de sus responsabilidades y funciones, el Director de TIC no supervisó que existan políticas de seguridad en la administración de los proyectos tecnológicos, lo que ocasionó que todos los activos informáticos del proyecto no sean considerados en los planes de seguridad y de contingencias.

Recomendaciones

El Director de TIC debe definir una metodología para la administración de proyectos de manera que cumpla la normativa vigente. Deberá evaluar permanentemente los riesgos identificados en cada proyecto para considerarlos en la planificación de los nuevos, considerando los planes de aseguramiento de la calidad y de control de cambios.

El Administrador del Proyecto o los que funjan con esa calidad, deberán identificar, aprobar y comunicar las etapas del proyecto, y los compromisos formales entre las partes interesadas, a través de la utilización de actas físicas o documentos electrónicos debidamente validados.

5.1.8. Desarrollo, mantenimiento y adquisición software de aplicación (Norma 410-08)

Tabla 5.8
Evaluación Control Interno - Norma técnica aplicada: 410-08

Pregunta	Estado del factor					Total	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo	% factor	
01	X					1,33	Ninguna
02			X			4,00	Contrato BDE
03		X				2,67	Informe técnico
04		X				2,67	Informe BDE
05	X					1,33	Ninguna
06	X					1,33	Ninguna
07		X				2,67	Contrato catastro
08	X					1,33	Ninguna
09	X					1,33	Ninguna
10		X				2,67	Manuales
11	X					1,33	Ninguna
12		X				2,67	Actas de reuniones
13	X					1,33	Ninguna
14	X					1,33	Ninguna
15		X				2,67	Manuales
Total	8	7	0	0	0	30,67	

Conclusiones

El Jefe de Sistemas y Aplicaciones no reguló los procesos de adquisición, desarrollo, y mantenimiento de los sistemas y aplicaciones; elaborando, documentando y aprobando procedimientos. Por tanto, incumplió la norma 410-08 ocasionando que no existan acuerdos formales de los requerimientos se identifique, priorice y especifique: la seguridad, los roles y perfiles de usuarios, el ciclo de vida de desarrollo de software, el plan o procedimiento de pruebas, y las pistas de auditoría (logs transaccionales).

Recomendaciones

El analista Junior de Aplicaciones y Sistemas deberá considerar en los procesos de adquisición, desarrollo, mantenimiento o implementación de software el establecimiento de procedimientos para: la validación, el plan de pruebas, la programación, la interfaz de usuario, la interoperabilidad y la escalabilidad.

El Director de TIC deberá gestionar ante el órgano competente los derechos de autor del software como de propiedad del GADMCE conforme a la ley, en el caso de desarrollos externos y contratos realizados con terceros los derechos de autor serán del GADMCE. En ambos casos se deberá entregar el código fuente de manera formal.

5.1.9. Adquisiciones de infraestructura tecnológica (Norma 410-09)

Tabla 5.9
Evaluación Control Interno - Norma técnica aplicada: 410-09

Pregunta	Estado del factor					Total	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo	% factor	
01		X				5,00	POA 2024
02		X				5,00	Informe de gestión
03	X					2,50	Contrato catastral
04			X			7,50	Informe técnico
05		X				5,00	Actas de Entrega/R
06	X					2,50	Ninguna
07	X					2,50	Ninguna
08	X					2,50	Ninguna
Total	4	3	1	0	0	32,50	

Conclusiones

El Director de TIC al no considerar algunas adquisiciones tecnológicas necesarias en plan anual de contrataciones tuvo que reformar el presupuesto, plan operativo y plan de contratación. Si bien algunos contratos de adquisición de infraestructura y soporte técnico tienen el detalle suficiente y las características técnicas (interfaces, número de serie, marca, modelo, etc.), el Director de TIC en el caso de los contratos de consultoría inobservo algunos aspectos de la norma 410-09, como fue el caso del Sistema Catastral ocasionando que no tengan: análisis de costo/beneficio, la evolución de riesgos, respaldos, la planificación de la capacidad, y la previsión de su vida útil.

Recomendaciones

El Director de TIC debe solicitar que los contratos con proveedores, sobre todo en el caso de consultorías, incluyan las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando los aspectos relacionados con la seguridad, propiedad y confidencialidad de la información.

El Jefe de Sistemas en el caso de almacenamiento en la “nube”, deberá tomar las previsiones necesarias en caso de alguna contingencia del proveedor mediante el análisis de los riesgos y el análisis costo/beneficio.

El Especialista de Soporte deberá respaldar la información almacenada antes de formatear bajo algún formato (borrado seguro de la información) y deberá considerar la normativa ambiental de gestión de residuos en el caso de baja de equipos o suministros.

5.1.10. Mantenimiento, actualización y control de la infraestructura tecnológica (Norma 410-10)

Tabla 5.10
Evaluación Control Interno - Norma técnica aplicada: 410-10

Pregunta	Estado del factor					Total	Acciones
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo	% factor	tomadas por la Entidad
01			X			6,67	Seguimiento Plan
02	X					2,22	Ninguna
03	X					2,22	Ninguna
04	X					2,22	Ninguna
05	X					2,22	Ninguna
06	X					2,22	Ninguna
07		X				4,44	Plan Mto
08		X				4,44	Inventario
09			X			6,67	Control de bienes
Total	5	2	2	0	0	33,33	

Conclusiones

El Jefe de Sistemas no llevó registro de las versiones del software que pasa a producción. No ha actualizó, publicó o difundió manuales con los mantenimientos o cambios realizados. Tampoco implementó ambientes de pruebas separados, para validar la seguridad; incumpliendo la norma 410-10, lo que ocasionó que la infraestructura tecnológica sea susceptible de fallas, comprometiendo la integridad de la información.

El Director de TIC al no supervisar que el Jefe de Sistemas documente el mantenimiento periódico que se realiza a la infraestructura tecnológica ocasionó que no exista evidencia documental sobre los trabajos realizados en los diversos componentes tecnológicos sobre todo el desplegado en toda la ciudad.

Recomendaciones

El Jefe de Sistemas debe documentar todos los mantenimientos a la infraestructura tecnológica que realizar en base al Plan anual de mantenimiento preventivo y correctivo. Y deberá mantener una bitácora con los cambios que se realicen en los sistemas y aplicaciones.

El Director de TIC deberá realizar el seguimiento y control de la planificación anual del mantenimiento preventivo y correctivo de la infraestructura tecnológica del GADMCE., registrando y evidenciando las actividades diarias que se efectúan.

5.1.11. Seguridad de tecnología de información (Norma 410-11)

Tabla 5.11
Evaluación Control Interno - Norma técnica aplicada: 410-11

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01		X				5,71	Existe un responsable
02	X					2,86	Ninguna
03		X				5,71	Plan de seguridad sin aprobar
04	X					2,86	Ninguna
05			X			8,57	Plataforma AME
06		X				5,71	Política de seguridad sin aprobar
07		X				5,71	POA 2024
Total	2	4	1	0	0	37,14	

Conclusiones

El Director de TIC no implemento el uso de estándares para determinar la eficiencia y eficacia de los mecanismos de seguridad de TI existentes en el GADMCE, no se evidencia el cumplimiento de la normativa vigente, sino que existen acciones aisladas, Por lo tanto, no cumple la norma 410-11, ocasionando el incumplimiento de la ley protección de datos personales y de las normas de control interno.

El Director de TIC no ha establecido una política de seguridad aprobada el Alcalde en calidad de la máxima autoridad, ocasionando que los funcionarios del GADMCE desconozcan los procedimientos y normativa interna establecida para precautelar los activos informáticos y generar un nivel de confianza en la infraestructura tecnológica que utilizan.

Recomendaciones

El Director de TIC debe gestionar ante la máxima autoridad, la aprobación de la política de seguridad de la información, para una vez aprobada, el contenido de esta se pueda socializar, difundir y publicar de manera que los funcionarios de la institución estén conscientes del riesgo de seguridad a los que se encuentran expuestos, de las sanciones y sobre todo tengan el compromiso de cumplirla en beneficio de tener un ambiente seguro.

El Jefe de Sistemas deberá ejecutar el plan de seguridad y hacer seguimiento de manera que se implementen los controles necesarios para mitigar los riesgos existentes.

5.1.12. Plan de contingencias (Norma 410-12)

Tabla 5.12
Evaluación Control Interno - Norma técnica aplicada: 410-12

Pregunta / Estado del factor							
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo	Total % factor	Acciones tomadas por la Entidad
01		X				2,50	Plan de contingencias para aprobación
02	X					5,00	Ninguna
03	X					2,50	Ninguna
04	X					7,50	Ninguna
05	X					2,50	Ninguna
06	X					2,50	Ninguna
07	X					2,50	Ninguna
08	X					2,50	Ninguna
Total	7	1	0	0	0	22,50	

Conclusiones

El Jefe de Sistemas ha elaborado un plan de contingencias, pero este no se ejecuta en la práctica, ni cubre toda la infraestructura tecnológica existente en la institución, ocasionando un alto riesgo de afectación a los activos de información en el caso de que las amenazas se materialicen. Sobre todo, en el caso del sistema CABILDO ERP, SIGAME, el portal ciudadano y la intranet.

No existe un comité que ejecute el plan en caso de una contingencia, No se ha realizado algún simulacro, en donde se ponga a prueba el plan por problemas en la infraestructura, sistemas o incluso el personal relacionado. Por lo tanto, el Director de TIC incumple la norma 410-12, ocasionando que no se evalúen las acciones establecidas en el caso de presentarse una emergencia, y por tanto se desconozca la eficacia y eficiencia del mismo.

Recomendaciones

Director de TIC debe evaluar si el plan de contingencias cumple con los objetivos ahí establecidos para asegurar la continuidad de los servicios de TI.

El Jefe de Sistemas deberá implementar un plan de continuidad de operaciones que contemple la puesta en marcha de la infraestructura necesaria mientras dure una contingencia; y deberá elaborar un plan de recuperación de desastres que establezca las actividades que se deben ejecutar antes, durante y después del desastre.

5.1.13. Administración de soporte de tecnología de información (Norma 410-13)

Tabla 5.13
Evaluación Control Interno - Norma técnica aplicada: 410-13

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01		X				3,08	Manual de procesos
02	X					1,54	Ninguna
03		X				3,08	Control de usuarios
04		X				3,08	Control de usuarios
05	X					1,54	Ninguna
06	X					1,54	Ninguna
07	X					1,54	Ninguna
08	X					1,54	Ninguna
09			X			4,62	Help desk de TI
10			X			6,15	Sistema hoja de ruta
11	X					1,54	Ninguna
12			X			4,62	Servidor de Backup
13	X					1,54	Ninguna
Total	7	3	3	0	0	33,85	

Conclusiones

El Director de TIC implementó una mesa de ayuda para gestionar los incidentes de seguridad y el soporte técnico, sin embargo, al no ser difundido o socializado con los empleados, ocasionando la subutilización de los recursos existentes y la falta de control.

El Especialista de Soporte no ha establecido mecanismos preventivos para salvaguardar los activos de información a nivel del parque informático, ocasionando que los equipos sean vulnerables a virus y software malicioso.

El Director de TIC no ha incorporado mecanismos de gestión documental y archivo, que proteja y conserve la información, ocasionando demora en los procesos.

Recomendaciones

El Director de TIC deberá definir niveles de servicio y operación para todos los procesos críticos de TI, en base a los requerimientos de los usuarios internos y externos.

El Jefe de Sistemas deberá revisar regularmente todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de procesos y administradores de SI.

El Director de TIC deberá implementar un archivo digital y un sistema de gestión documental que agilite de forma segura la gestión de la información municipal.

5.1.14. Monitoreo y evaluación de los procesos y servicios (Norma 410-14)

Tabla 5.14
Evaluación Control Interno - Norma técnica aplicada: 410-14

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01	X					4,00	Ninguna
02	X					4,00	Ninguna
03	X					4,00	Ninguna
04		X				8,00	Informe de gestión
05	X					4,00	Ninguna
Total	4	1	0	0	0	24,00	

Conclusiones

El Director de TIC no ha definido formalmente un procedimiento que permita evidenciar las acciones de evaluación y monitores realizadas por cada subproceso de la Dirección de TIC, ocasionando insatisfacción en los usuarios internos y externos por servicios tecnológicos recibidos, incumpliendo lo establecido en la norma 410-14.

El Director de TIC no presentó informes periódicos al Alcalde o su cuerpo de ediles, con los resultados del monitoreo realizado a través del CIOCE al proceso de recolección de basura, alzado y rutas de la flota vehicular para que se identifiquen e implanten acciones correctivas. Sin embargo, las acciones correctivas que se han dispuesto por las autoridades no han sido ejecutadas.

Recomendaciones

El Coordinador institucional deberá definir una metodología legalmente establecida que permita monitorear la contribución y el impacto de las acciones realizadas por la unidad de TIC.

El Director de TIC debe definir indicadores y métricas para los subprocesos que permitan la toma de decisiones y permita realizar los correctivos necesarios. En el caso del monitoreo a través de CIOCE, los reportes deben ser diarios en el caso de la recolección de basura y el control vehicular de las rutas.

El Director de TIC deberá evaluar al menos una vez al año, el nivel de satisfacción de los funcionarios y ciudadanos, sobre todo en el uso del portal web, la aplicación móvil de los ciudadanos, y la intranet institucional de empleados.

5.1.15. Portal web, servicios telemáticos e intranet (Norma 410-15)

Tabla 5.15
Evaluación Control Interno - Norma técnica aplicada: 410-15

Pregunta	Estado del factor					Total	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo	% factor	
01			X			15,00	Manual servicio web Manual de uso correo electrónico
02		X				10,00	Informe técnico
03				X		20,00	Sistema de hoja de ruta Intranet institucional Portal ciudadano
04				X		20,00	Sistema de hoja de ruta Munidigital Intranet institucional Portal ciudadano
Total	0	1	1	2	0	65,00	

Conclusiones

El Asistente de Aplicaciones y Sistemas a disponer de normas, procedimientos y ha elaborado instructivos de los servicios de internet, intranet, correo electrónico y sitio web de la entidad. Sin embargo, no ha socializado con todo el personal, ocasionando que no todos los funcionarios utilicen su correo electrónico o acceden al internet de manera adecuada, incumpliendo la norma 410-15.

El responsable de la Unidad de Aplicaciones y Sistemas ha desarrollado aplicaciones web para la automatización de procesos y seguimiento de trámites, tanto para el uso de información entre instituciones como para los ciudadanos, sin embargo, no se evidencia socialización sobre esas herramientas, ocasionando la subutilización de las mismas. Así mismo ha implementado aplicaciones web y móviles tanto propias como en comodato, sin considerar el tratamiento y seguridad de la protección de datos personales.

Recomendaciones

Director de TIC deberá desarrollar esquemas normativos de conformidad con las disposiciones y normativa legal vigente, considerando los requerimientos de los usuarios externos e internos, y sobre todo la ley de protección de datos personales.

EL Director de TIC, debe gestionar la socialización de todos productos y servicios tecnológicos tanto con los usuarios internos (funcionarios), como con los externos (ciudadanos),

5.1.16. Portal web, servicios telemáticos e intranet (Norma 410-16)

Tabla 5.16
Evaluación Control Interno - Norma técnica aplicada: 410-16

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01			X			15,00	Capacitaciones de la CGE en temas TIC
02	X					5,00	Ninguna
03	X					5,00	Ninguna
04		X				10,00	Plan de capacitación
Total	2	1	1	0	0	35,00	

Conclusiones

El Director de TIC no ha elaborado una planificación de capacitación especializada dirigida a personal de TIC, debido a la falta de presupuesto, ocasionando que no exista un eficiente plan de capacitación de TIC para el personal que utilizan los sistemas CABILDO, SIGAME, SISCAL; portal ciudadano; y correo electrónico.

El Director de TIC, no ha coordinado con la Dirección de Talento Humano la elaboración del plan de capacitación para todos los funcionarios relacionado a las TIC, incumpliendo la norma 410-16 y ocasionando que los funcionarios no se capaciten.

Recomendaciones

El Director de TIC deberá solicitar a la Dirección de Talento Humano que a través de la CGE, se capacite en temas especializados de tecnologías a todo el personal de la Dirección, para que estos a su vez repliquen los conocimientos adquiridos al resto de funcionarios en donde sea pertinente.

El Director de TIC en coordinación con la Dirección de Talento Humano deberá elaborar un plan de capacitación de TIC identificado y documentando las necesidades de todo el personal.

El Director Financiero deberá considerar incluir una partida en el presupuesto destinada a la capacitación especializada por parte de funcionarios de TIC, siempre y cuando esos cursos sean replicados y de utilidad para la institución y sus procesos.

5.1.17. Firmas electrónicas (Norma 410-17)

Tabla 5.17
Evaluación Control Interno - Norma técnica aplicada: 410-17

Pregunta	Estado del factor					Total % factor	Acciones tomadas por la Entidad
No.	Incipiente	Básico	Confiable	Muy confiable	Optimo		
01					X	20,00	Instalación de firma EC, Reglamento CP
02			X			12,00	Soporte en sitio y virtual
03		X				8,00	Intranet sin firma electrónica
04				X		16,00	Firma .EC
05		X				8,00	Carpetas compartidas
Total	0	2	1	1	1	64,00	

Conclusiones

Existe un instructivo de Compras Públicas para el uso obligatorio de la firma electrónica. El Director de TIC ha incorporado uso de la firma electrónica de manera automática en la intranet, pero todavía no se utiliza a nivel de las demás direcciones del GADMCE, cumpliendo de manera parcial la norma 410-17.

El Director de TIC a través de su equipo técnico, capacitó a los servidores de la institución sobre las medidas de seguridad, y responsabilidades que deben tener en cuenta al usar la firma electrónica. Pero no se cuenta con un registro de la periodicidad, fecha, contenido y personal que entrego el soporte. Existe un instructivo que no ha sido socializado difundido con la mayoría de funcionarios de la institución, ocasionando que el cumpliendo de esta norma sea parcial.

Recomendaciones

El Director de TIC debe desarrollar e implementar aplicativos que incluyan el uso de la firma electrónica al resto del personal, incorporando mecanismos y reportes que faciliten una auditoría de los mensajes firmados electrónicamente.

El Director de TIC deberá elaborar procedimientos que permitan respaldar y almacenar bajo su responsabilidad en su estado original, los archivos electrónicos o mensajes de datos firmados electrónicamente, a través de medios electrónicos seguros. Permitiendo la optimización de recursos y el ahorro de papel y suministros de impresión.

5.2. Plan de mejora

IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN - GADMCE

1. Introducción

1.1. Antecedentes (C.4.1, C.4.2)

Con la trasformación digital y los nuevos modelos de gestión que muchos municipios quieren implementar, la utilización de un estándar de la industria de la seguridad de la información como las normas ISO 27001:2022 constituye un marco de referencia confiable, completo, flexible y actualizado para garantizar el cumpliendo de las normas de control interno de la CGE, la LOPDP y demás normativa vigente en el Ecuador.

6.1.6. Como conclusión general de esta investigación, con base en las normas de control interno de la CGE, podemos establecer que los mecanismos de tecnologías de información aplicados en del GADMCE, inciden en el sistema de gestión de la seguridad de la información de la institución con un bajo nivel de cumplimiento (29%); esto coincide y se evidencia en el cumplimiento de 29 de los 93 controles que establecen las normas ISO 27001:2022, así como el bajo grado de cumplimiento de los requisitos obligatorios para mantener un adecuado sistema de gestión de seguridad de información (SGSI).

Como se mencionó anteriormente, se ha comprobado que los mecanismos aplicados basados en las normas de control interno de la CGE inciden en la seguridad de la información de la institución, pero en un bajo nivel (31%); es decir se ha evidenciado el cumplimiento de 29 de los 93 controles que establece la metodología utilizada, sin embargo referente a los requisitos obligatorios para un SGSI en un sentido estricto, el nivel de cumplimiento es muy bajo, al no estar aún implementado, y evidenciar que el desarrollo apenas ha comenzado (29%) y requerirá un trabajo significativo para satisfacer los requisitos establecidos por la norma ISO 27001:2022. Por lo tanto, se establece como punto de partida para la mejora de la institución: la implementación de la política de seguridad de la información, en base a la EGSI.

1.2. Objetivo de la Política (C.5.2)

Establecer los principios y lineamientos que permitan al GADMCE asegurando la adecuada protección de todos sus activos de información y previniendo que la materialización de los riesgos pueda afectar la confidencialidad, integridad y disponibilidad de la información.

1.3. Declaración de los objetivos de seguridad de la información (C.6.2)

- **Objetivo 1:** Fortalecer el ambiente de control con base en el sistema de seguridad de la información, para que desde el compromiso de la máxima autoridad se convierta en un hábito de buenas prácticas, promoviendo el cumplimiento de las políticas, por parte de todo el personal de la institución.
- **Objetivo 2:** Gestionar eficientemente los riesgos de seguridad de la información para mantener un entorno controlado y a niveles aceptables, a través del despliegue de medidas de seguridad para prevenir o reducir los efectos indeseados en el tratamiento de los riesgos.
- **Objetivo 3:** Garantizar una eficiente gestión de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad que permitan el establecimiento de medidas de protección, detección y recuperación, proporcional a la criticidad del evento, valor de la información y de los servicios afectados.

2. Compromiso de la alta dirección (C.5.1)

Basado en el EGSI(2023), el Alcalde de Esmeraldas, en su calidad de máxima autoridad del cantón en conjunto con su equipo directivo, entendiendo la importancia de una adecuada gestión de la seguridad de información, demostrando liderazgo y compromiso, se ha comprometido con la implementación de un SGSI; buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, en estricto cumplimiento de la normativa legal vigente y en concordancia con la misión y visión institucional.

Basandose en el EGSI (2023), el GADMCE estable que la protección de la información busca la disminución del impacto generado sobre sus activos de información, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de

exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la información, acorde con las necesidades de los funcionarios, los ciudadanos, y los demás actores de la sociedad. De acuerdo a lo expuesto, esta política aplica a todo el su funcionario, proveedores, usuarios y la ciudadanía en general.

3. Roles y Responsabilidades (C.5.3, A.5.2)

Basados en el EGSI (2023), se establece que:

- La máxima autoridad a través del Comité de Seguridad de la Información (CSI - equipo directivo) es el responsable de asegurar que la seguridad de la información se gestiona adecuadamente en toda la institución.
- Cada funcionario Director departamental (NJS), es responsable de garantizar que los funcionarios que trabajan bajo su control protegen la información de acuerdo con las normas establecidas por la institución.
- El Oficial de Seguridad de la Información (OSI) asesora al equipo directivo, proporciona apoyo especializado al personal de la institución y garantiza que los informes sobre la situación de la seguridad de la información están disponibles.
- Cada uno de los funcionarios de la institución tiene la responsabilidad de mantener la seguridad de información dentro de las actividades relacionadas con su trabajo.

4. Alcance y usuarios (C.4.3)

Esta Política se aplica a todo lo que contempla el EGSI, los usuarios internos de este documento son todos los funcionarios del GADMCE, como también todos los usuarios externos a la institución lo conforman los ciudadanos y demás actores locales. Esta política de Seguridad, deberá estar disponible en la página web institucional www.esmeraldas.gob.ec, y en un repositorio digital de manera que sea de libre acceso para todos los funcionarios.

Nota: Junto a cada componente de esta política se encuentra codificada la cláusula y/o control del SGSI con la que guarda relación, y cuyo grado de cumplimiento en las matrices de evaluación que se adjuntan tuvieron el más bajo nivel de cumplimiento. Además, y guardan relación directa con las recomendaciones incluidas en informe final entregado a la Dirección de TIC.

5. Comunicación de la Política (C.7.3, C.7.4)

La Política de Seguridad de la Información será comunicada con todos los funcionarios de la institución, mediante talleres de inducciones, campañas de socialización, y las plataformas tecnológicas existentes en la institución: correo electrónico, pagina web, intranet y redes sociales.

El Director de Comunicación determinará la necesidad para las comunicaciones internas y externas relevantes al SGSI, y establecerá un programa de concientización en seguridad.

6. Políticas de Seguridad de la Información (A.5.1)

***6.1. Seguridad de los Recursos Humanos* (A.5.3, A.5.4, A.6.2)**

Toda persona aspirante o empleado de la institución deberá cumplir y hacer cumplir lo establecido en la presente Política en todas las fases, incluyendo en la fase previa a la contratación, fase de contratación, y fase de desvinculación de los funcionarios.

La Dirección de Talento Humano establecerá en los acuerdos contractuales de trabajo se las responsabilidades del personal y de la organización en materia de seguridad de la información

6.2. Seguridad de Activos de información (A.5.9, A7.8)

La Dirección de TIC deberá mantener un el inventario actualizado de activos de información del GADMCE. En cada Dirección del GADMCE existirá un custodio, el cual tendrá la responsabilidad de asegurar que el activo esté inventariado y protegido. Deberá informar a la Dirección Administrativa cualquier novedad presentada con el activo.

La Dirección Administrativa deberá asignar un responsable de la gestión de activos de información a lo largo de su ciclo de vida. Este funcionario deberá mantener un registro documentado de todos los usuarios con acceso autorizado a dicho activo.

6.3. Clasificación y arquitectura de la información (A.5.12)

La Dirección de TIC Se deberá definir un modelo de arquitectura y clasificación que incluya de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por el GADMCE.

El responsable del modelo de arquitectura y clasificación de los datos será un funcionario de la Dirección de TIC, y será el Administrador de la Base de Datos institucional.

Administrador de la Base de Datos institucional deberá definir un esquema de clasificación y los requisitos de manipulación de medios de almacenamiento a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de información.

6.4. Prevención de fugas de información (A.8.12)

La Dirección de Talento Humano y Desarrollo Organizacional, en coordinación con el Director de TIC capacitara a todos los funcionarios de la institución sobre mejores prácticas de prevención de fugas de información.

6.5. Seguridad de control de acceso (A.5.17)

Los usuarios de cualquier sistema, aplicación o programa requerirán de un usuario y contraseña, que deberán ser únicos y no podrá ser compartida. La Dirección de TIC será la responsable de la creación de estos usuarios en función del registro que haga talento humano en el sistema.

Se prohíbe el uso de usuarios genéricos, se utilizarán cuentas de usuario asociadas al perfil del cargo que desempeñe en según el estatuto orgánico por procesos vigente. La Dirección de Talento Humano será la responsable de incluir esto en el contrato y en el sistema.

6.6. Trabajo Remoto (A.6.7, A.7.9)

Los servicios de conexión para trabajo remoto estarán destinados exclusivamente a los funcionarios del GADMCE. Su uso por parte de cualquier otro tipo de colaborador requerirá autorización del Director de TIC.

Laborar desde un equipo fuera del lugar de trabajo del trabajador requerirá de medidas de seguridad para que el teletrabajo no suponga una amenaza para la seguridad de la información.

El servicio de teletrabajo se monitorizará y controlará, registrándose tanto la conexión como la actividad de acuerdo con los protocolos de seguridad, y el equipo utilizado para la conexión en la modalidad de teletrabajo podrá ser de propiedad del funcionario.

6.7. Seguridad Física y ambiental (A.7.1, A.7.2, A.7.3, A.7.4, A7.5, A.7.6)

Los espacios físicos donde residan los sistemas de información del GADMCE deberán estar protegidos adecuadamente mediante controles de acceso perimetrales, sistemas de vigilancia y medidas preventivas de manera que puedan evitarse o mitigar el impacto de incidentes de Seguridad (accesos no autorizados, vandalismo, robo o sabotaje) y accidentes ambientales (terremoto, incendio, inundación, corte de energía eléctrica, etc.) (Grupo ACS, 2022, p. 13).

Al Dirección Administrativa deberá controlar el acceso de los funcionarios mediante dispositivos biométricos y en caso excepcional a través de una bitácora digital o en papel.

6.8. Seguridad en el ciclo de vida del desarrollo de sistemas (A.8.25)

El Jefe de Sistemas ser responsable de la adquisición, desarrollo y mantenimiento de los sistemas de información deberá cumplir con requisitos mínimos de seguridad acorde con las ISO 27001:2022.

Las pruebas de seguridad se deberán definir e implementar en el ciclo de vida del desarrollo, los entornos de desarrollo, prueba y producción deberán ser independientes.

Se deberá realizar una gestión de validación y pruebas, seguimiento de los cambios, y mantener un inventario del software en donde se especifique el número de versión.

6.9. Gestión de incidentes (A.5.7, A.5.24)

La Dirección de TIC deberá definir, establecer y comunicar el proceso, los roles y las responsabilidades de gestión de incidentes de seguridad de la información categorizando los incidentes, y analizando sus impactos.

Todos los funcionarios del GADMCE tienen la obligación de informar al responsable de seguridad de cualquier incidente o delito que pudiera comprometer la seguridad de los activos de información de la institución.

La Dirección de TIC deberá elaborar plan de contingencias categorizado como confidencial, que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

6.10. Seguridad en los Proveedores (A.5.19, A.5.20)

La Dirección de TIC deberá definir e implementan procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.

El director de TIC deberá establecer y acordar con cada proveedor los requisitos de seguridad de la información pertinentes en función del tipo de relación que se tenga.

La Dirección de TIC establecerá los niveles de servicio y medidas de seguridad, que deberán ser equivalentes a las establecidas en la presente Política.

6.11. Auditorías de Seguridad y gestión de vulnerabilidades (C.9.2, A.8.34)

En base a los establecido por el Grupo ACS(2022)

Se deberá realizar una identificación periódica de vulnerabilidades técnicas de los sistemas de información y aplicaciones empleadas en la organización, de acuerdo a su exposición a dichas vulnerabilidades y adoptando las medidas adecuadas para mitigar el riesgo asociado.

Se deberá aplicar las medidas correctoras necesarias tan pronto como sea posible. La identificación, gestión y corrección de las vulnerabilidades debe hacerse conforme a un enfoque basado en riesgos, teniendo en cuenta la criticidad y la exposición de los activos (Grupo ACS, 2022, p. 15).

6.12. Gestión de cambios (A.8.30)

El Director de TIC deberá revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información de los proveedores y en la prestación de servicios.

Los cambios en las instalaciones de procesamiento de información y los sistemas de información deberán estar sujetos a procedimientos de gestión de cambios. En caso que la institución determine la necesidad de cambios en el SGSI estos deberán ser realizados de planificadamente.

6.13. Filtrado web y uso de criptografía (A.8.23, A.8.24)

El Jefe de Sistemas deberá gestionar el acceso a sitios web externos para reducir la exposición a contenidos maliciosos y definir e implementar para el uso eficaz de la criptografía, incluida la gestión de claves criptográficas.

6.14. Revisión de la Política (C.10.1)

La aprobación de esta Política implica que su implantación contará con el apoyo de la máxima autoridad para lograr todos los objetivos establecidos en la misma, como también para cumplir con todos sus requisitos. (Grupo ACS, 2022, p. 16)

La presente Política será revisada y aprobada anualmente por el Comité Informático. Sin embargo, si se presentan cambios el entorno, amenazas y riesgos de cualquier tipo, se revisará, asegurando así que la Política permanezca adaptada la realidad del GADMCE.

7. Gestión de Excepciones (C.10.2)

Cualquier excepción a la presente Política de Seguridad de la Información deberá ser registrada e informada al Director de TIC, y este a su vez comunicará a la máxima autoridad. Estas excepciones serán analizadas por el Comité de Seguridad para evaluar el riesgo, y en base a la resolución técnica elaborada por la Dirección de TIC, estos deberán ser asumidos por el solicitante, en conjunto con la máxima autoridad de la institución.

8. Sanciones disciplinarias (A.6.2, A.6.4)

La Dirección de Talento Humano tomará de las acciones disciplinarias correspondientes de acuerdo con el reglamento interno del GADMCE ante el de incumplimiento de alguna de las disposiciones establecidas.

Es responsabilidad de todos los funcionarios notificar al responsable de Seguridad de la Información, infirmar cualquier evento o situación que pudiera suponer el incumplimiento de alguna de las directrices definidas por la presente Política. (Grupo ACS, 2022, p. 16)

La Dirección de Talento Humano deberá formalizar y comunicar un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.

9. Glosario de términos

Término	Definición
Activo de información	Algo que una organización valora (sistemas, soportes, edificios, personas, etc.) y por lo tanto debe proteger
Ataque	Intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo
Aplicación	solución de TI diseñada para ayudar a los usuarios de las organizaciones a realizar tareas o automatizar un proceso
Confidencialidad	Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados
Control	Salvaguarda o contramedida que modifica el riesgo de seguridad de la información
Cloud	Conjunto de servicios de computación en la nube (internet)
Cortafuego	Herramienta informática diseñada para bloquear el acceso no autorizado dentro de una red
Criptografía	Protocolos utilizados para proteger la información y dotar de seguridad a las comunicaciones
CSI	Comité de Seguridad de la Información
Disponibilidad	Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada
Firma electrónica	Protocolo criptográfico utilizado para verificar la autenticidad e integridad de los mensajes o documentos digitales
EGSI	Esquema Gubernamental de Seguridad de la Información
Impacto	El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos financieros
Ignífugos	Que no se inflama ni propaga la llama o el fuego
Información	Conjunto de datos procesados con significado para la institución
Integridad	Propiedad de proteger la precisión y completitud de los activos
Malware	programas malintencionados que se insertan e instalan en los sistemas y servidores de los usuarios finales
NJS	Nivel jerárquico superior
No repudio	Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje y que un receptor niegue su recepción
Proceso	Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
OSI	Oficial de Seguridad de la Información
Riesgo	Posibilidad de que una amenaza pueda explotar una vulnerabilidad para causar pérdida o daño a un activo de información
Trazabilidad	Cualidad que permite que todas las acciones realizadas sobren la información sean asociadas de modo inequívoco a un individuo o entidad
Virus	programas que se instalan en el ordenador, normalmente de forma oculta al propietario, con fines maliciosos
VPN	Red privada virtual
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Nota: Tomado de ISO/IEC27001(2022) y MINTEL(2024)

10. Documentos de referencia

- Ley Orgánica de Protección de Datos Personales
- Acuerdo Ministerial Nro. MINTEL-MINTEL-0003-2024
- Esquema Gubernamental de Seguridad de la Información (EGSI v3.0)
- Familia de Normas Técnicas ISO/IEC 27000:2022
- NCI 410 de la CGE
- Alcance del EGSI
- Plan de Ordenamiento y Desarrollo Territorial de Esmeraldas
- Plan Operativo Anual 2024

11. Firmas de responsabilidad

	Nombre/Cargo	Firma
Elaborado por:	David Rodríguez Portes **Consultor Externo**	
Revisado por:	Damián Meza Anchundia **Presidente del Comité**	
Aprobado por:	Vicko Villacis Tenorio **Alcalde de Esmeraldas**	

Control de versiones del formato referencial

Versión:	1.0
Fecha de la versión:	05-06-2024
Creado por:	Dirección de Tecnología de Información y Comunicación
Aprobado por:	Subsecretaría de Gobierno Electrónico y Registro Civil
Nivel de confidencialidad:	Bajo

Historial de cambios del formato referencial

Versión	Fecha	Detalle del cambio
1.0	05/06/2024	Emisión inicial del documento

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

6.1.1. El análisis y evaluación de riesgo informático es el punto de partida para que una institución implemente mecanismos de seguridad de TI, de allí que las normas ISO 27001:2022 especifican los controles y los requisitos obligatorios que una institución debe cumplir con el objeto de que un SGSI sea eficiente, todos los requisitos obligatorios son relativos al SGSI que se evalúa, más que a los riesgos de seguridad que tiene la infraestructura tecnológica; si bien la norma no obliga a emplear controles de seguridad específicos, y es la organización la que los determina, con la finalidad de establecer una línea base que le permita a la institución el mantenimiento y mejora continua de su SGSI.

6.1.2. La evaluación de las tecnologías de información a nivel de parque informático, software, almacenamiento, redes y comunicaciones basado en las normas de control interno de la CGE, constituye en la práctica una auditoria al SGSI institucional, a través de la cual se determina si los mecanismos de seguridad informática implementados garantizan el cumplimiento de la normativa legal vigente, la continuidad de los servicios y salvaguardan los activos de información.

6.1.3. En todo informe de auditoría es necesario que las observaciones o hallazgos contengan el criterio, la condición, la causa y el impacto que tiene en la seguridad de la información de manera que se garantice un ambiente de control adecuado, la continuidad de los servicios, la operatividad de la infraestructura tecnológica y salvaguarde los activos de información de la institución, sobre todo de la información sensible, en donde las protecciones de los datos personales tienen un papel preponderante.

6.1.4. La implementación de políticas de seguridad de la información en una institución como el GADMCE además de asegurar el cumplimiento de las normas de control interno, o de las normas ISO 27001, representa en realidad la mejor estrategia que una autoridad puede establecer para convertir la implementación de marco seguridad y confianza, en un legado institucional que no solo salvaguarde los activos de información, sino que a largo plazo salvaguarde los recursos públicos.

6.1.5. Ninguno de los mecanismos de seguridad informática implementados por las organizaciones para proteger su infraestructura tecnológica, por costoso o complejos que sean, son suficientes o eficientes, si no se cumplen las normas de control interno, y por lo tanto, no se cuenta con un adecuado ambiente de control interno que genere confianza entre los usuarios (internos y externos), y asegure la disponibilidad, integridad y confidencialidad del activo más importante que tienen las organizaciones en la actualidad: la información.

6.1.6. Una vez analizado el ambiente de control, los activos informáticos, y el SGSI de la institución, bajo el marco de referencia de la norma ISO 27001:2022 y las NCI 410, se concluye que la falta de políticas de seguridad de la información ocasionó que los mecanismos implementados tengan un bajo grado de cumplimiento de los controles que establecen ambas normativas; por lo tanto, inciden negativamente en la seguridad de las tecnologías de información del GADMCE.

6.2. RECOMENDACIONES

6.2.1. El GADMCE deberá contar con un Sistema de Gestión de la Seguridad de Información (SGSI) formalmente definido, de manera que en base a las políticas propuestas se establezcan mecanismos para todos los casos en que el estado del control o clausura fue inexistente o inicial.

6.2.2. Los responsables de las unidades de TIC deberán evaluar continuamente los riesgos de seguridad de la información de la institución, para decidir con que controles serán tratados dichos riesgos, utilizando las políticas y procedimientos definidos en el SGSI, sin embargo, se debe tener claro que la norma ISO27001:2022 no obliga a emplear controles de seguridad específicos: es la institución la que los determina.

6.2.3. Los funcionarios de las unidades de TIC de las instituciones públicas, con su director a la cabeza, deberán cumplir de forma obligatoria con todas las disposiciones establecidas en las NCI 410 con la finalidad de mantener un adecuado ambiente de control interno que asegure la integridad, disponibilidad, y confidencialidad del activo más valioso de la institución: la información.

6.2.4. La máxima autoridad y su equipo directivo deberán demostrar liderazgo y compromiso con el SGSI cumpliendo y haciendo cumplir de la política de seguridad de la información aprobada en la institución.

6.2.5. Considerando que la CGE, en las NCI 410, establece la utilización de estándares de seguridad, como la ISO 27001:2022, y el MINTEL, en su EGSI la establece como su marco de referencia; se recomienda a instituciones del sector público y los responsables de las unidades de TI, la utilización de este estándar internacional, no solo para mejorar y asegurar la seguridad de la información de su organización, sino del propio sistema de control interno institucional.

.

REFERENCIAS

Abril, A., Pulido, J., y Bohada, J. (2013). *Análisis de riesgos en seguridad de la información*. Revista Ciencia, Innovación y Tecnología, I, 40-53. Fundación Universitaria Juan de Castellanos. Boyaca. Colombia. https://revista.jdc.edu.co/index.php/rciyt/article/view/121

Acurio, S. A., (2023). *Propuesta de un plan de seguridad informático para la empresa EP -EMAPA-A*. Tesis de grado. Maestría en Gerencia Informática. Pontificia Universidad Católica del Ecuador Sede Ambato. https://repositorio.pucesa.edu.ec/bi xtstream/123456789/4088/1/79247.pdf

AEPD. (2021). *Gestión del riesgo y evaluación de impacto en tratamiento de datos personales*. Guía de la Agencia Española de Protección de Datos. https://www.aepd.es/guias/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

Aguilar, F., (2019). *Los ataques informáticos y su incidencia en la Seguridad de servidores con sistema operativo Linux de Entidades de gobierno local*. Tesis de Maestría en Gerencia de Sistemas de Información. Facultad de Ingeniería en Sistemas. Universidad Técnica de Ambato. Ambato, Ecuador. https://repositorio.uta.edu.ec/bitstream/123456789/30474/1/Tesis_t1645msi.pdf

Alcaldía de Esmeraldas. (02 de diciembre de 2021). Inauguración Proyecto Esmeraldas Ciudad Inteligente. Ecuador. [Video]. YouTube. Obtenido en https://www.youtube.com/watch?v=p40KTXiTHLI

Alvarado, N., (2018), *Tecnología contra el crimen: Entusiasmo con cautela y criterio*. Sin Miedos. Revista Digital BID. https://blogs.iadb.org/seguridad-ciudadana/es/tecnologia-contra-el-crimen-entusiasmo-con-criterio/

Aponte, G., y Cuenca, J. P. (2021). *Modelo de gestión de TI para el Gobierno Autónomo Descentralizado Municipal del Cantón Huaquillas*. Dominio de las Ciencias. https://dominiodelasciencias.com/ojs/index.php/es/article/view/2383

Arief, A., y Wahab, I. H. A. (2017*). Information technology audit for management evaluation using COBIT and IT security (Case study on Dishubkominfo of North Maluku Provincial Government, Indonesia).* Proceedings - 2016 3rd International

Conference on Information Technology, Computer, and Electrical Engineering, ICITACEE 2016, 388–392. https://doi.org/10.1109/ICITACEE.2016.7892477

Baca, G., (2016). *Introducción a la Seguridad Informática. Ciudad de México,* México: Grupo Editorial Patria. Recuperado de: https://books.google.com.ec/books?id=IhUhDgAAQBAJ&lpg=PP1&ots=0XQv2zscFs&dq=plan%20de%20seguridad%20inform%C3%A1tica.

Ballester, M. (2010). *Gobierno de las TIC.* ISO/IEC 38500. ISACA Journal. https://docplayer.es/816237-Gobierno-corporativo-tic.html

BID y OEA. (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe*. Reporte 2020. Observatorio de Ciberseguridad. Banco Interamericano de Desarrollo. http://dx.doi.org/10.18235/0002513

Bouskela, M., Casseb, M., Bassi, S. y Facchina, M. (2016). *La ruta hacia las Smart Cities*. Banco Interamericano de Desarrollo. https://publications.iadb.org/es/la-ruta-hacia-las-smart-cities-migrando-de-una-gestion-tradicional-la-ciudad-inteligente

Calle, A., Mendoza, G., Ronquillo H., y Rivera, B. (2023). *Auditorìa de la gestión de Tecnologías de la Información en el sector público.* Revista Ciencia y Desarrollo. Universidad Alas Peruanas. https://revistas.uap.edu.pe/ojs/index.php/CYD/article/view/2575/2572

Caraguay, S. (2020). *Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú 2007-2019.* Estado y comunes: Revista de políticas y problemas públicos. N.° 11, vol. 2, julio-diciembre 2020, pp. 135-153. Instituto de Altos Estudios Nacionales (IAEN). Quito-Ecuador. Obtenido en https://revistas.iaen.edu.ec/index.php/estado_comunes/article/view/178/340

Cartuche, J., Hernández, D., Morocho, R., y Radicelli, C. (2020). *Seguridad IoT: Principales amenazas en una taxonomía de activos*. Hamut´ay, 7 (1), 51-59. Universidad Alas Peruanas. Lima. Perú. http://dx.doi.org/10.21503/hamu.v7i3.2192

Castillo, L., (2022). *Evaluación de la seguridad informática bajo las normas ISO/IEC 27001 en la infraestructura tecnológica de la Universidad Estatal de Milagro.*

Tesis. Maestría en Tecnologías de Información. UNEMI. Milagro, Ecuador. https://repositorio.unemi.edu.ec/xmlui/handle/123456789/7000

Centro Criptológico Nacional de España. (2012*). Guía de seguridad de las Tic* (CCN-STIC-817), agosto 2012. https://www.ccncert.cni.es/publico/seriesCCN-STIC/series/800- Esquema_Nacional_de_Seguridad/817-Gestion_incidentes_seguridad/817- Gestion_incidentes_seguridad-ago12.pdf

CEPAL. (2016). *Horizontes 2030*. Trigésimo sexto periodo de sesiones de la Comisión Económica para América Latina y el Caribe.

Codolà, S., Garre, S., y Cruz, D. (2018). *Seguridad y auditoria de la información*. Recurso de aprendizaje de la Universidad Abierta de Cataluña (UOC). Barcelona. http://creativecommons.org/licenses/by-nc-nd/3.0/es/

Condori, P. (2020). *Universo, población y muestra*. Curso Taller. Universidad Nacional de Juliaca. Perú. Obtenido en https://www.aacademica.org/cporfirio/18.pdf

Contraloría General del Estado. (2023). *Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de recursos públicos.* Acuerdo No. 004-CG-2023. Registro Oficial. Suplemento 257, 1-102, https://www.contraloria.gob.ec/WFDescarga.aspx?id=1487&tipo=mul

COOTAD. (2010). Código Orgánico de Organización Territorial, Autonomía y Descentralización. *Ley 0 Registro Oficial Suplemento* 303 de 19-oct.-2010 Ultima modificación: 31-dic.-2019 Estado: Reformado

Chica, A. (2020). *Estudio de la planeación de auditoría enfocado en análisis de seguridad de la información*. Tecnológico de Antioquia. Colombia. https://dspace.tdea.edu.co/bitstream/handle/tdea/1397/Informe%20Planeaci%C3%B3n%20auditoria.pdf?sequence=1&isAllowed=y

Chóez Acosta, L. (2020). *Implementación de un plan de tratamiento de riesgos tecnológicos al centro de cómputo de una organización no gubernamental sin fines de lucro siguiendo la metodología MAGERIT*. Tesis de Maestría en Seguridad Informatice. ESPOL. FIEC. Guayaquil.http://www.dspace.espol.edu.ec/xmlui/handle/123456789/50402

Cruz Allende, D. (2018). *Análisis de riesgos*. Recurso de aprendizaje de la Universidad Abierta de Cataluña (UOC). Barcelona. https://openaccess.uoc.edu/bitstream/10609/142807/2/M%c3%b3dulo%202_An%c3%a1lisis%20de%20riesgos.pdf

Cusme, k., Zambrano, Y., Zambrano L., y Morales, J. (2020). *Procesos de Tecnologías de la Información: Norma 410 de la Contraloría General del Estado.* Ponencia Escuela Superior Politécnica Agropecuaria de Manabí. http://www.espam.edu.ec/recursos/sitio/informativo/archivos/ponencias/vinculacion/i/s2/CIV64CSDCS20.pdf

Decreto Ejecutivo No.681. Que declara el estado de excepción por grave conmoción interna en la provincia de Esmeraldas. con motivo de las actividades de grupos de delincuencia organizada, sucesos cuyo escalonamiento pone en riesgo la seguridad de los ciudadanos y de las fuerzas del orden, su integridad y su vida. Registro Oficial del Ecuador (Emitido el 03 de marzo de 2023). https://smart.fielweb.com/App_Themes/InformacionInteres/-signed.pdf

Díaz, A., Real, C. del, Gallardo, F., Solari, M., Jordán, J., Vázquez, R., y Maldonado, D. (2023). *Agenda de investigación: smart cities y seguridad en Andalucía*. Universidad de Cádiz. España. Obtenido en https://hdl.handle.net/1887/3618829

Domínguez, J., y Solís, G. (2009). *Análisis y aprovechamiento de los sistemas de información para una eficiente auditoria y control de gestión.* Escuela Superior Politécnica de Litoral. Guayaquil. Ecuador. http://www.dspace.espol.edu.ec/handle/123456789/1901

Enriquez, L. (2021). La protección de datos en América latina: influencia del RGPD. Observatorio de Ciberderechos y Tecnosociedad. Universidad Simón Bolívar, Ecuador. Obtenido en https://www.uasb.edu.ec/ciberderechos/2021/06/15/la-proteccion-de-datos-en-america-latina-influencia-del-rgpd/

Ernst & Young, *XV Encuesta Global de Seguridad de la Información de Ernst & Young*, 2018. Disponible en: http://www.ey.com. [Último acceso: 05 08 2020].

ESET. (2020). *Security Report Latinoamerica 2020*. https://www.Welivesecurity.Com/wp-content/uploads/2020/08/eset-security-reportlatam_2020.Pdf

Euroinnova. (2024). *Aplicación Práctica de la Ley de Protección de Datos Personales.* Curso práctico. Unidad Didáctica 4. La auditoría de protección de datos.

GADMCE. (2020), *Plan de Ordenamiento y Desarrollo Territorial del Cantón Esmeraldas*. Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas.

Gantz, S. D. (2013). *The Basics of IT Audit: Purposes, Processes, and Practical Information*. https://doi.org/10.1016/C2013-0-06954-X

García-Cervigón Hurtado, A., y Alegre Ramos, M. (2011). *Seguridad informática* Sistemas microinformáticos y redes: Informática y comunicaciones. Madrid: Paraninfo.

Garre, Silvia., Segovia, Antonio., Tortajada, Arsenio., y Cruz, Daniel. (2018). *Introducción a la seguridad de la información*. Recurso de aprendizaje de la Universidad Abierta de Cataluña (UOC). Módulo 1. Barcelona. Obtenida en https://openaccess.uoc.edu/bitstream/10609/142807/1/M%C3%B3dulo%201_Introducci%C3%B3n%20a%20la%20seguridad%20de%20la%20informaci%C3%B3n.pdf

Gómez, R., Pérez, D., Donoso, Y. y Herrera, A. (2012). *Metodología y gobierno de la gestión de riesgos de tecnologías de la información*. Revista de Ingeniería, 48. Facultad de Ingeniería. Universidad de los Andes. http://dx.doi.org/10.16924%2Friua.v0i31.217

González, L., y Permuy, C. (2020). *Software para estandarizar el proceso de auditoría de seguridad informática*. XVIII Convención y feria internación Informática 2020. La Habana. Cuba. Obtenido en https://es.scribd.com/document/492335911/GES15

González, P. (2023). *Ley de Protección de Datos establece multas para funcionarios.* Revista Primicias. Obtenido en: https://www.primicias.ec/noticias/economia/ley-proteccion-datos-multas-funcionarios/

Grupo ACS. (2022). *Política de Seguridad de la Información*. Grupo Actividades de Construcción y Servicios S.A. España. Obtenido en https://www.grupoacs.com/ficheros_editor/File/05_Compliance/Pol%C3%ADticas/31_Pol%C3%ADtica%20de%20Seguridad%20de%20la%20Informaci%C3%B3n.pdf

Humayun, M., Niazi, M., Jhanjhi, N., Alshayeb, M., y Mahmood, S. (2020). *Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study*. Arabian Journal For Science And Engineering, 45(4), 3171-3189. https://doi.org/10.1007/s13369-019-04319-2.

INEC. (2010). *Censo de Población y Vivienda* 2010. Instituto Nacional de Estadísticas y Censos. Ecuador. Obtenido en: https://www.ecuadorencifras.gob.ec/censo-de-poblacion-y-vivienda/

Imbaquingo, D. (2022). Método de auditoría informática basado en sistemas de procesamiento avanzado de datos que permita minimizar el riesgo de calidad de los resultados. Tesis Doctoral. Universidad Nacional de La Plata. Repositorio Institucional de la UNLP. https://sedici.unlp.edu.ar/handle/10915/157674

Imbaquingo, D., Jácome, J. y Pusdá, M. (2017). *Fundamentos de Auditoría Informática basada en riesgos*. Ibarra, Ecuador: Universidad Técnica del Norte.

ISACA. (2012). COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. Marco Entregador de COBIT 5.0. Estados Unidos.

ISO/IEC 27001:2022. (2022). *Seguridad de la información, ciberseguridad y protección de la privacidad - Controles de seguridad de la información.* [en línea], (sin fecha). Obtenido en https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:v2:en

ISO27001security [en línea], (2022). [Consultado el 13 de diciembre de 2023]. Disponible en: https://www.iso27001security.com/html/27001.html

León, J., Mora, J., Huilcapi, M., Tamayo, A., y Armijos C. (2018). *COBIT como modelo para auditorías y control de los sistemas de información*. Revista Polo del Conocimiento, 3(4), 17. Manta. Ecuador. https://doi.org/10.23857/pc.v3i4.439

Mallar, M. A. (2010): *La gestión por procesos: un enfoque de gestión eficiente*. Revista Científica "Visión de Futuro", vol. 13, núm. 1.

Management, T. I. (2015). *Asset Management An Anatomy*. Version 3. United. Obtenido de https://theiam.org/media/1781/iam_anatomy_ver3_web.pdf

Martin, Eliseo. (2023). *Mejora el nivel de seguridad y elimina o destruye tus vulnerabilidades*. Ebook de Ciberseguridad.

Martins, L. (2014). *Software asset management in an organization*. Instituto Universitario de Lisboa (ISCTE-IUL. Obtenido de http://hdl.handle.net/10071/11184

Martínez, A. (2021). *Claves y aspectos prácticos para la adaptación de las ICEX al nuevo marco de la protección de datos personales*. Revista Auditoria Publica, Tribunal Vasco de Cuentas Publicas. España. https://asocex.es/wp-content/uploads/2019/12/Revista-Auditoria-Publica-n%C2%BA-74.-pag-115-a-122.pdf

Mendoza, W., García, T., Delgado, M., y Barreiro, I. (2018). *El control interno y su influencia en la gestión administrativa del sector público*. Dominio de las Ciencias, 206-240. https://dialnet.unirioja.es/servlet/articulo?codigo=6656251

Ministerio de Hacienda y Administraciones Públicas. (2016). *MAGERIT versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Secretaria General Técnica. Gobierno de España. Madrid. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

MINTEL. (2024). *Esquema Gubernamental de Seguridad de la Información – EGSI.* Acuerdo Ministerial Nº MINTEL-2024-0003. Ministerio de Telecomunicaciones y de la Sociedad de la Información. Registro Oficial del Ecuador Nº509. (Emitido el 1 de marzo de 2024). https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2024/03/Registro-Oficial-Acuerdo-Ministerial-No.-0003-2024-EGSI-version-3.0.pdf

MINTEL. (2021). *Política de Ciberseguridad del Ecuador*. Acuerdo Ministerial 006-2021. Ministerio de Telecomunicaciones y de la Sociedad de la Información. Registro Oficial del Ecuador Nº479. (Emitido el 23 de junio de 2019).

https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Acuerdo-No.-006-2021-Politica-de-Ciberseguridad.pdf

MINTEL. (2019). *Guía para el tratamiento de datos personales en la Administración Pública.* Acuerdo Ministerial 12. Ministerio de Telecomunicaciones y de la Sociedad de la Información. Registro Oficial del Ecuador Nº18. (Emitido el 15 de agosto de 2019). https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2019/11/Gu%C3%ADa-de-protecci%C3%B3n-de-datos-personales.pdf

MINTEL. (2019). *Libro Blanco de Territorios Digitales*. Decreto Ejecutivo Nº633. Ministerio de Telecomunicaciones y de la Sociedad de la Información. (Emitido el 08 de enero de 2019). https://www.telecomunicaciones.gob.ec/wp-content/uploads/2019/11/LBTD_actualizado_25-11-2019_a.pdf

Molina, M. (2015). *Propuesta de un Plan de Gestión de Riesgos de Tecnología aplicado en la Escuela Superior Politécnica del Litoral*. Universidad Politécnica De Madrid. http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2014-2015/TFM_Maria_Fernanda_Molina_Miranda_2015.pdf

Nasir, A., Arshah, R. A., y Hamid, M. R. A. (2019). *A dimension-based information security culture model and its relationship with employees' security behavior: A case study in Malaysian higher educational institutions*. Information Security Journal: A Global Perspective. https://doi.org/10.1080/19393555.2019.1643956

Novoa, H. y Rodríguez, C. (2023). *Metodologías Para el Análisis de Riesgos en los SGSi.* Fundación Universitaria Juan de Castellanos. Facultad de Ingeniería. Tunja, Colombia. [Consultado 18-12-2023]. Obtenido en https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/view/1435/1874

Numpaque, E. (2018). *Análisis de riesgos: proceso, regulaciones y metodologías*. Universidad Piloto de Colombia. Bogotá. http://polux.unipiloto.edu.co:8080/00004802.pdf

Parlamento Europeo y del Consejo. (17 de abril de 2019). Reglamento (UE) sobre ENISA (Agencia de Ciberseguridad de la Unión Europea) y sobre la certificación de la

ciberseguridad de las tecnologías de la información y las comunicaciones. y por el que se deroga el Reglamento (UE) n.º 526/2013 (Ley de Ciberseguridad). [Reglamento 2019/881 de 2019]. https://eur-lex.europa.eu/eli/reg/2019/881/oj

Ponce, L., (2023). *Todo lo que debes conocer sobre la Protección de Datos Personales*. PwC Ecuador. Obtenido en https://www.pwc.ec/es/entrevistas-de-temas-de-interes/todo-lo-que-debes-conocer-sobre-la-proteccion-de-datos-personales.html

Ramírez, E., y Rincón, M. (2022). *La importancia de la seguridad de la información en el sector público en Colombia*. Revista Ibérica de Sistemas y Tecnologías de Información. RISTI Nº46. Universidad Popular del Cesar. https://scielo.pt/pdf/rist/n46/1646-9895-rist-46-97.pdf

Rodríguez, A., Sepúlveda, L. (2023). Cuadro comparativo sobre metodologías para la evaluación de riesgos laborales. Corporación Universitaria Minuto de Dios. Girardot. Colombia. https://es.scribd.com/document/634683596/ACTIVIDAD-2-MAPA-COMPARATIVO

Romero, A., Gasca, M., García, M., y Hernández, A. (2022). *Aplicación de buenas prácticas, un camino hacia la cultura de la seguridad informática en las instituciones públicas*. Revista Electrónica Sobre Tecnología, Educación y Sociedad, 9(18). https://www.ctes.org.mx/index.php/ctes/article/view/794

Sacoto, V., (2019). *Implementación de un esquema de seguridad informática para una entidad financiera con el propósito de mitigar los riesgos que podrían presentarse a causa de ataques cibernéticos, internos o externos y salvaguardar la integridad de la información, basados en el estándar ISO27001*. Tesis. ESPOL. FIEC, Guayaquil. http://www.dspace.espol.edu.ec/xmlui/handle/123456789/47048

Sánchez, V. (2019). *Planificación de la implementación de un esquema de seguridad basada en la norma ISO 27001:2013, para el proceso de administración del sistema de información geográfica en el gobierno autónomo descentralizado del cantón Samborondón*. Tesis de Grado. Maestría en Seguridad Informática. ESPOL, FIEC, Guayaquil. http://www.dspace.espol.edu.ec/xmlui/handle/123456789/47047

Sevilla Erazo, E., (2023). *Diseño de un plan de gestión de riesgos tecnológicos con la Metodología MAGERIT v3 basada en la norma ISO/IEC 31000, para fortalecer la*

gestión de amenazas y riesgos en los Laboratorios de informática de la facultad de ingeniería en Ciencias de la UTN. Tesis. Universidad Técnica del Norte. Ibarra. http://repositorio.utn.edu.ec/bitstream/123456789/13866/2/04%20ISC%20672%20TESIS%20GRADO.pdf

Solarte, F., Enríquez, E., y Benavides, M. (2015). *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001*. Revista Tecnológica - ESPOL, 28(5), 497–498. http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Soler González, R., Varela-Lorenzo, P., Oñate-Andino, A., & Naranjo-Silva, E. (2018). *La gestión de riesgo: el ausente recurrente de la administración de empresas // Risk management: the recurrent absence of business administration*. CIENCIA UNEMI, 11(26), 51-62. https://doi.org/10.29076/issn.2528-7737vol11iss26.2018pp51-62p

Solórzano, L., Rezabala J., y Aranda A., *Estudio sobre el estado del arte de la seguridad informática en el Ecuador y sus necesidades reales*. ESPOL. https://www.dspace.espol.edu.ec/handle/123456789/24298

SOPHOS. (2019). *El 90% de las empresas que ha sufrido un ciberataque contaba con soluciones tradicionales de seguridad*. Sophos News. https://news.sophos.com/es-es/2019/11/28/el-90-de-las-empresas-que-hasufrido-un-ciberataque-contaba-con-soluciones-tradicionales-de-seguridad/

Srinivas, K. (2019). *Process of Risk Management*. Perspectives on Risk, Assessment and Management Paradigms. https://doi.org/10.5772/intechopen.80804

Tamayo, M., González, D., De la Caridad, M., Fornet, J., y Cabrera, E. (2020*). La gestión de riesgos* (1st ed.). Universo Sur.

Trujillo, S, Carlos, J., Merlos, Gallegos, M., y Valero, L. (2020). *Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares*. Ideas en Ciencias de la Ingeniería ISSN en trámite. 49-70. Facultad de Ingeniería. Universidad Autónoma del Estado de México. México. https://hemeroteca.uaemex.mx/index.php/ideasingenieria/article/view/14591

Tusa, E. (2021). *Evaluación técnica informática al subsistema de matriculación vehicular de la mancomunidad de tránsito del norte con base en COBIT 2019.*

Tesis. Maestría en Gerencia de Sistemas. Universidad de las Fuerzas Armadas ESPE. Matriz Sangolquí. https://repositorio.espe.edu.ec/bitstream/21000/25461/1/T-ESPE-044667.pdf

UIT. (2019). N*uevos datos de la UIT indican que, pese a la mayor implantación de Internet la brecha de género digital sigue creciendo*. Comunicado de Prensa. Unión Internacional de Telecomunicaciones. (noviembre de 2019). https://www.Itu.Int/es/mediacentre/pages/2019-pr19.Aspx

Urbanovics, A. y Guajardo, R. (2022). *Estrategias de ciberseguridad en los países latinoamericanos – un análisis comparativo.* Revista Acta Hispánica Sumplementum 4. Núm. IV. Universidad Nacional de Servicio Público. Hungria. https://doi.org/10.14232/actahisp.2022.0.89-104

Vásquez, A., Chavez, G., y Gonzalez, J. (2023). *La auditoría interna en las entidades públicas y privados de Ecuador. Enfoques. Revista de Investigación en Ciencias de la Administración.* Volumen 7. Nº26. pp. 162 – 169. https://revistaenfoques.org/index.php/revistaenfoques/article/view/183

Villegas, J. A. (2019). *Evaluación técnica informática al sistema de gestión de seguridad de la información del GAD provincial de Imbabura en base de la norma ISO/IEC 27001:2013*. Maestría en Gerencia de Sistemas. ESPE. Matriz Sangolquí. https://repositorio.espe.edu.ec/handle/21000/21529

ANEXO A

Plantilla resumen de entrevista estructurada al Director de TIC para la evaluación del SGSI en base a los requisitos obligatorios ISO 270001:2022

Estado de la implementación de la Norma ISO/IEC 27001 Requisitos obligatorios SGSI GADMCE

Sección	Requisito ISO/IEC 27001	Preguntas realizadas	Estado	Si cumple	No cumple	Evidencia
4.0	**Contexto de la organización**					**20,00%**
4.1	Entender la organización y su contexto	¿La organización determina los problemas externos e internos que son relevantes para su propósito y que afecta su capacidad para lograr los resultados esperados de su SGSI?	**Limitado**	-	40%	PDOT
4.2	Comprender las necesidades y expectativas de las partes interesadas	¿Se identifican las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, requisitos relevantes al respecto de la seguridad de la información y sus obligaciones?	**Inicial**	-	20%	Política de segridad
4.3	Alcance del SGSI	¿Se determina y documenta el alcance del SGSI?	**Inexistente**	-	0%	NINGUNA
4.4	Sistema de gestión de seguridad de la información(SGSI)	¿Se establecer, implementar, mantener y mejorar continuamente el SGSI de conformidad con la norma?	**Inicial**	-	20%	Política de segridad
5	**Liderazgo**					**60,00%**
5.1	Liderazgo y compromiso	¿La alta dirección demuestra liderazgo y compromiso con respecto al SGSI?	**Definido**	60%	-	Disposiciones internas
5.2	Política	¿La alta dirección establece una política de seguridad de la información?	**Definido**	60%	-	Política de segridad
5.3	Funciones, responsabilidades y autoridades de la organización	¿La alta dirección se asegura de que las responsabilidades y autoridades de los roles relevantes para la seguridad de la información se asignen y comuniquen dentro de la organización?	**Definido**	60%	-	Orgánico funcional. Manual de puestos y funciones
6.0	**Planificación**					**33,33%**
6.1	Acciones para tratar con los riesgos y oportunidades	¿Al diseñar o planificar el SGSI se toman el contexto de la organización, los requisitos de las partes interesadas, se determinan los riesgos y oportunidades, se evalúan, y se aplica un proceso documentado de tratamiento de riesgos de seguridad de la información?	**Inicial**	-	20%	NINGUNA. Disposiciones informales.
6.2	Objetivos de seguridad de la información y planificación para alcanzarlos	¿Se establecen y documentan los objetivos y planes de seguridad de la información en las funciones y niveles pertinentes?	**Definido**	60%	-	Plan de seguridad de infraestructura tecnológica
6.3	Planificación de cambios	¿Cuando la organización determina la necesidad de cambios en el SGSI estos son llevados a cabo de manera planificada?	**Inicial**	-	20%	NINGUNA. Disposiciones informales.
7.0	**Soporte**					**40,00%**
7.1	Recursos	¿Se determina y proporcionan los recursos necesarios para el SGSI?	**Definido**	60%	-	Plan Operativo Annual
7.2	Competencias	¿Se determina, documenta y pone a disposición las competencias necesarias?	**Definido**	60%	-	Plan de capacitación
7.3	Concientización	¿Se establece un programa de concientización en seguridad?	**Limitado**	-	40%	NINGUNA. Disposiciones informales.
7.4	Comunicación	¿Se determinar la necesidad para las comunicaciones internas y externas relevantes al SGSI?	**Inicial**	-	20%	Comunicaciones internas
7.5	Información documentada	¿Se incluye la información documentada requerida por la norma, así como la requerida por la organización, garantizando: la identificación y descripción (títulos, autores, etc.), formato, revisión y aprobación de la idoneidad y adecuación.	**Inicial**	-	20%	NINGUNA. Disposiciones informales.
8.0	**Operación**					**20,00%**
8.1	Planificación y control operacional	¿Se planifica, implementa, controla y documenta el proceso del SGSI para gestionar los riesgos (plan de tratamiento de riesgos)?	**Limitado**	-	40%	POA 2023
8.2	Evaluación del riesgo de seguridad de la información	¿Se (Re)hace la evaluación y documentan los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones?	**Inicial**	-	20%	Plan de contingencias
8.3	Tratamiento del riesgo de seguridad de la información	¿Se implementa el plan de tratamiento de riesgos (tratar los riesgos?) y documentar los resultados?	**Inexistente**	-	0%	NINGUNA
9.0	**Evaluación del desempeño**					**20,00%**
9.1	Seguimiento, medición, análisis y evaluación	¿Se hace seguimiento, mide, analiza y evalua el SGSI y los controles?	**Limitado**	-	40%	Informe de gestion 2023
9.2	Auditoría interna	¿Se planifica y llevar a cabo auditorías internas del SGSI?	**Inicial**	-	20%	NINGUNA. Disposiciones informales.
9.3	Revisión por la dirección	Se emprenden revisiones por la dirección del SGSI regularmente	**Inexistente**	-	0%	NINGUNA
10.0	**Mejora**					**20,00%**
10.1	Mejora continua	¿Se mejora continuamente el SGSI?	**Limitado**	-	40%	Informe de gestion 2023
10.2	No conformidad y acciones correctivas	¿Se identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones?	**Inicial**	-	20%	NINGUNA. Disposiciones informales.
					30,48%	**Nivel de madurez SGSI**

ANEXO B

Plantilla resumen de entrevistas al Director y funcionarios de TIC para la evaluación de controles de seguridad según norma ISO 270001:2022

EVALUACIÓN DEL SGSI DEL GADMCE - Declaración de Aplicabilidad (SoA) y estado de los controles de la seguridad de la información NORMA ISO27001:2022 ANEXO

Control	Nombre	Tipo	Estado	Cumple	No cumple	Evidencia	Preguntas realizadas	Respuesta	Si	No	Area responsible
A.5.1	Políticas para la seguridad de la información	Organizacionales	Limitado	-	40%	Solo están aprobadas por la dirección de TI. No han sido socializadas	¿La política de seguridad de la información y las políticas específicas de cada tema son definidas, aprobadas por la dirección, publicadas y comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes y revisados a intervalos planificados si se producen cambios significativos.	NO EXISTE		X	Dirección
A.5.2	Funciones y responsabilidades de seguridad de la información	Organizacionales	Gestionado	80%	-	Orgánico funcional por procesos	¿Se definen y asignan funciones y responsabilidades de seguridad de la información según las necesidades de la organización.	Orgánico Funcional por procesos	X		Dirección
A.5.3	Segregación de tareas	Organizacionales	Gestionado	80%	-	Manual de procesos y procedimientos	¿Se separarán las tareas y áreas de responsabilidad en conflicto?	Manual de puestos y funciones	X		Dirección
A.5.4	Responsabilidades de gestión	Organizacionales	Inicial	-	20%	Existe memorando solo a nivel de la dirección de TI	¿La gerencia requiere a todo el personal aplicar la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y procedimientos temáticos específicos de la organización?	NO EXISTE		X	Dirección
A.5.5	Contacto con las autoridades	Organizacionales	Inicial	-	20%	Solo con la DINARDAT	¿La organización establece y mantiene contacto con las autoridades pertinentes?	NO EXISTE		X	Dirección
A.5.6	Contacto con grupos de interés especial	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿La organización establece y mantiene contacto con grupos de intereses especiales u otros foros especializados en seguridad y asociaciones profesionales?	NO EXISTE		X	Dirección
A.5.7	Inteligencia de amenazas	Organizacionales	Inicial	-	20%	Sistema de help desk. Solo se recopila	¿La información relacionada con las amenazas a la seguridad de la información se recopila y analiza para producir inteligencia sobre amenazas?	NO EXISTE		X	Dirección
A.5.8	Seguridad de la información en la gestión de proyectos	Organizacionales	Definido	60%	-	Consta definida en el TDR	¿La seguridad de la información se integra en la gestión de proyectos?	TDR	X		Proyectos
A.5.9	Inventario de información y otros activos asociados	Organizacionales	Inicial	-	20%	Solo existe inventario de activos bienes	¿Se desarrolla y mantien un inventario de información y otros activos asociados, incluidos los propietarios.	NO EXISTE		X	Dirección
A.5.10	Uso aceptable de la información y otros activos asociados	Organizacionales	Inicial	-	20%	No se presenta evidencia	¿Se identifican, documentan e implementan reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados?	NO EXISTE		X	Dirección
A.5.11	Devolución de activos	Organizacionales	Optimizado	100%	-	Proceso de bodega, actas de entrega. Paz y salvo	¿El personal y otras partes interesadas, según corresponda, devolvuelven todos los activos de la organización en su poder al cambiaro terminación de su empleo, contrato o acuerdo?	Acta de entrega Repepción / Paz y salvo	X		Dirección
A.5.12	Clasificación de información	Organizacionales	Inicial	-	20%	No se presenta evidencia	¿Se clasifica la información de acuerdo a las necesidades de seguridad de la información de la organización con base en confidencialidad, integridad, disponibilidad y requisitos relevantes de las partes interesada?	NO EXISTE		X	Dirección
A.5.13	Etiquetado de información	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿Se desarrolla e implementa un conjunto apropiado de procedimientos para el etiquetado de información de acuerdo con el esquema de clasificación de información adoptado por la organización?	NO EXISTE		X	Dirección
A.5.14	Transferencia de información	Organizacionales	Gestionado	80%	-	Convenio ECU911, Convenio DINARDAT	¿Existen reglas, procedimientos o acuerdos de transferencia de información para todo tipo de instalaciones de transferencia dentro de la organización y entre la organización y otras partes?	DINARDAT	X		Dirección
A.5.15	Control de Acceso	Organizacionales	Limitado	-	40%	Reglamento interno y normas de control interno	¿Se establecen e implementan reglas para controlar el acceso físico y lógico a la información y otros activos asociados con base en los requisitos de seguridad de la información y del negocio?	Informe Técnico	X		Dirección
A.5.16	Gestión de identidad	Organizacionales	Inicial	-	20%	No se presenta evidencia	¿Se gestiona el ciclo de vida completo de las identidades?	Se gestiona por pedido expreso, no esta formalizado		X	Dirección
A.5.17	Información de autenticación	Organizacionales	Limitado	-	40%	Actas de entrega de usuarios y contraseñas	¿La asignación y gestión de la información de autenticación se controla mediante un proceso de gestión, incluido el assoramiento al personal sobre el manejo adecuado de la información de autenticación?	NO EXISTE		X	Dirección
A.5.18	Derechos de acceso	Organizacionales	Inicial	-	20%	No se presenta evidencia	¿Los derechos de acceso a la información y otros activos asociados se proporcionan, revisan, modificar y eliminan de acuerdo con la política temática específica de la organización y las reglas para el control de acceso?	NO EXISTE		X	Dirección
A.5.19	Seguridad de la información en las relaciones con proveedores	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿Se definen e implementan procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor?	NO EXISTE		X	Dirección
A.5.20	Abordar la seguridad de la información en los acuerdos con proveedores	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿Los requisitos de seguridad de la información pertinentes se establecen y acuerdan con cada proveedor en función del tipo de relación con el proveedor?	NO EXISTE		X	Dirección
A.5.21	Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y las comunicaciones (TIC)	Organizacionales	Inicial	-	20%	No se presenta evidencia	¿Se definen e implementan procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC?	NO EXISTE		X	Dirección
A.5.22	Gestión del cambio, revisión y monitoreo de los servicios del proveedor o suministrador	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿La organización monitorea, revisa, evalua y gestiona periódicamente los cambios en las prácticas de seguridad de la información de los proveedores y en la prestación de servicios?	NO EXISTE		X	Infraestructura

Control	Nombre	Tipo	Estado	Cumple	No cumple	Evidencia	Preguntas realizadas	Respuesta	Si	No	Area responsible
A.5.23	Seguridad de la información para el uso de servicios en la nube (cloud)	Organizacionales	Optimizado	100%	-	TDR, Informe técnico	¿Los procesos de adquisición, uso, gestión y salida de servicios en la nube se establecen de acuerdo con los requisitos de seguridad de la información de la organización?	INFORME TECNICO	X		Infraestructura
A.5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	Organizacionales	Limitado	-	40%	No se presenta evidencia	¿La organización planifica y se prepara para gestionar incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información?	NO EXISTE		X	Infraestructura
A.5.25	Evaluación y decisión sobre eventos de seguridad de la información	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿La organización evalua los eventos de seguridad de la información y decide si deben clasificarse como incidentes de seguridad de la información?	NO EXISTE		X	Infraestructura
A.5.26	Respuesta a los incidentes de seguridad de la información	Organizacionales	Gestionado	80%	-	Mesa de ayuda Helpdesk	¿Los incidentes de seguridad de la información se responden de acuerdo con los procedimientos documentados?	NO EXISTE		X	Infraestructura
A.5.27	Aprender de los incidentes de seguridad de la información	Organizacionales	Inicial	-	20%	Informe técnico	¿El conocimiento adquirido a partir de incidentes de seguridad de la información se utiliza para fortalecer y mejorar los controles de seguridad de la información?	Informe Técnico	X		Infraestructura
A.5.28	Recopilación de pruebas	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿La organiación establece e implementa procedimientos para la identificación, recopilación, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información?	NO EXISTE		X	Infraestructura
A.5.29	Seguridad de la información durante interrupciones	Organizacionales	Limitado	-	40%	Plan de seguridad institucional	¿La organización planifica cómo mantener la seguridad de la información en un nivel apropiado durante la interrupción?	NO EXISTE		X	Infraestructura
A.5.30	Preparación de las TIC para la continuidad de negocio	Organizacionales	Limitado	-	40%	Plan de contingencias	La preparación de las TIC se planifica, implementa, mantiene y prueba en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC?	NO EXISTE		X	Dirección
A.5.31	Requisitos legales, estatutarios, regulatorios y contractuales	Organizacionales	Inicial	-	20%	Existen recomendaciones de auditoria con algunos informes de seguimiento	¿Se identifican, documentan y mantienen actualizados los requisitos legales, estatutarios, regulatorios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos?	NO EXISTE		X	Infraestructura
A.5.32	Derechos de propiedad intelectual	Organizacionales	Inicial	-	20%	Solo existe en los nuevos contratados	¿La organización implementa procedimientos apropiados para proteger los derechos de propiedad intelectual?	NO EXISTE		X	Aplicaciones
A.5.33	Protección de registros	Organizacionales	Limitado	-	40%	Existe un archivo en la mayoria de direcciones	¿Los registros están protegidos contra pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada?	NO EXISTE		X	Infraestructura
A.5.34	Privacidad y protección de la información de identificación personal (PII)	Organizacionales	Inicial	-	20%	No se presenta evidencia	¿La organización identifica y cumple con los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes, regulaciones y requisitos contractuales aplicables?	NO EXISTE		X	Infraestructura
A.5.35	Revisión independiente de la seguridad de la información	Organizacionales	Inexistente	-	0%	No se presenta evidencia	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisa de forma independiente a intervalos planificados o cuando se producen cambios significativos.	NO EXISTE		X	Infraestructura
A.5.36	Cumplimiento de políticas, reglas y estándares de seguridad de la información	Organizacionales	Inicial	-	20%	A nivel de normas de control en algunas normas	¿Se revisa periódicamente el cumplimiento de la política de seguridad de la información de la organización, las políticas, reglas y estándares específicos de cada ítem?	NO EXISTE		X	Infraestructura
A.5.37	Procedimientos operacionales documentados	Organizacionales	Inexistente	-	0%	No se presenta evidencia	¿Los procedimientos operativos de las instalaciones de procesamiento de información se documentan y ponen a disposición del personal que los necesite?	NO EXISTE		X	Soporte
A.6.1	Revisión de antecedentes	Personales	Optimizado	100%	-	Certificados	¿Se realizan verificaciones de antecedentes de todos los candidatos a convertirse en personal antes de unirse a la organización y de manera continua teniendo en cuenta las leyes, regulaciones y ética aplicables a los requisitos del negocio, la clasificación de la información a la que se accederá y los riesgos percibidos?	SI SE REALIZA		X	Dirección
A.6.2	Términos y condiciones de empleo	Personales	Inicial	-	20%	Solo en algunos casos	¿En los acuerdos contractuales de trabajo se establen las responsabilidades del personal y de la organización en materia de seguridad de la información?	NO EXISTE		X	Dirección
A.6.3	Concientización, educación y capacitación sobre seguridad de la información.	Personales	Limitado	-	40%	Solo en ciertos casos, en el area de software se les dan capacitacion sobre la seguridad de información	¿El personal de la organización y las partes interesadas relevantes reciben concientización, educación y capacitación apropiadas sobre seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, políticas y procedimientos específicos de temas, según sea relevante para su función laboral?	NO EXISTE		X	Proyectos
A.6.4	Proceso disciplinario	Personales	Inexistente	-	0%	No se presenta evidencia	¿Se formaliza y comunica un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información?	NO EXISTE		X	Dirección
A.6.5	Responsabilidades tras el despido o cambio de empleo	Personales	Definido	60%	-	Pas y salvo	¿Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o cambio de empleo se definen, aplican y comunican al personal relevante y otras partes interesadas?	NO EXISTE		X	Dirección
A.6.6	Acuerdos de confidencialidad o no revelación	Personales	Inicial	-	20%	Cosnta en el manual de puestos y reglamento interno	¿Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información se identifican, documentan y revisan periódicamente, y son firmados por el personal y otras partes interesadas relevantes?	NO EXISTE		X	Dirección
A.6.7	Trabajo remoto	Personales	Gestionado	80%	-	VPN, teletrabajo	¿Se implementan medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización?	VPN	X		Infraestructura

EVALUACIÒN DEL SGSI DEL GADMCE - Declaración de Aplicabilidad (SoA) y estado de los controles de la seguridad de la información NORMA ISO27001:2022 ANEXO											
Control	**Nombre**	**Tipo**	**Estado**	**Cumple**	**No cumple**	**Evidencia**	**Preguntas realizadas**	**Respuesta**	**Si**	**No**	**Area responsible**
A.6.8	Informes de eventos de seguridad de la información	Personales	Limitado	-	40%	Mesa de ayuda Helpdesk	¿La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de canales apropiados de manera oportuna?	MESA DE AYUDA	X		Soporte
A.7.1	Perímetros de seguridad física	Físicos	Definido	60%	-	Fotografías	¿Se definen y utilizan perímetros de seguridad para proteger áreas que contienen información y otros activos asociados?	FOTOGRAFIAS		X	Soporte
A.7.2	Entrada física	Físicos	Gestionado	80%	-	Fotografías	¿Las áreas seguras están protegidas por controles de entrada y puntos de acceso adecuados?	FOTOGRAFIAS	X		Soporte
A.7.3	Seguridad de oficinas, despachos e instalaciones	Físicos	Gestionado	80%	-	Fotografías	¿Se diseña e implementa la seguridad física para oficinas, salas e instalaciones?	Informe Técnico	X		Soporte
A.7.4	Supervisión de la seguridad física	Físicos	Gestionado	80%	-	Sistema de CCTV	¿Las instalaciones son monitoreadas continuamente para detectar accesos físicos no autorizados?	Sistema de DE CCTV	X		Soporte
A.7.5	Protección contra amenazas físicas y ambientales	Físicos	Inicial	-	20%	Sistema de enfriamiento, alarmas	¿Se diseña e implementa la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura?	NO EXISTE		X	Soporte
A.7.6	Trabajo en áreas seguras	Físicos	Gestionado	80%	-	Reglamento interno	¿Se diseña e implementan medidas de seguridad para trabajar en áreas seguras?	REGLAMENTO	X		Soporte
A.7.7	Escritorio y pantalla limpios	Físicos	Limitado	-	40%	Existe un servidor de domino para ese control	¿Se definen y hace cumplir adecuadamente reglas claras de escritorio para papeles y medios de almacenamiento extraíbles y reglas claras de pantalla para instalaciones de procesamiento de información?			X	Infraestructura
A.7.8	Ubicación y protección de equipos.	Físicos	Gestionado	80%	-	Fotografías	¿El equipo esta ubicado de forma segura y protegida?	Datacenter / Fotografías	X		Soporte
A.7.9	Seguridad de los activos fuera de las instalaciones	Físicos	Inexistente	-	0%	Segun cada empleado	¿Se protegen los activos fuera del sitio?	NO EXISTE		X	Soporte
A.7.10	Medios de almacenamiento	Físicos	Inexistente	-	0%	No se presenta evidencia	¿Los medios de almacenamiento se gestionan a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización?	NO EXISTE		X	Infraestructura
A.7.11	Servicios de suministro o Servicios públicos de apoyo	Físicos	Gestionado	80%	-	UPS, 1 data center	¿Las instalaciones de procesamiento de información están protegidas contra fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte?	UPS Datacenter / Fotografías	X		Infraestructura
A.7.12	Seguridad del cableado	Físicos	Definido	60%	-	Fotografías	¿Los cables que transporten energía, datos o servicios de información de soporte estarán protegidos contra interceptaciones, interferencias o daños?	NO EXISTE		X	Soporte
A.7.13	Mantenimiento de equipos	Físicos	Optimizado	100%	-	Plan annual de mantenimiento preventivo	¿Los equipos se mantienen correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información?	Plan anual de mantenimiento preventivo	X		Soporte
A.7.14	Eliminación o re utilización segura de equipos	Físicos	Inexistente	-	0%	No se presenta evidencia	¿Los elementos del equipo que contienen medios de almacenamiento se verifican para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización?	NO EXISTE		X	Soporte
A.8.1	Dispositivos terminales de usuario	Tecnológicos	Gestionado	80%	-	Consola de Antivirus	¿La información almacenada, procesada o accesible a través de dispositivos terminales de usuario está protegida?	Contrato de Antivirus	X		Soporte
A.8.2	Derechos de acceso privilegiado	Tecnológicos	Gestionado	80%	-	Log de auditoria	¿La asignación y el uso de derechos de acceso privilegiado están restringidos y gestionados?	Registro de accesos	X		Aplicaciones
A.8.3	Restricción de acceso a la información	Tecnológicos	Definido	60%	-	Politica de seguridad	¿El acceso a la información y otros activos asociados está restringido de acuerdo con la política temática establecida sobre control de acceso?	NO EXISTE		X	Aplicaciones
A.8.4	Acceso al código fuente	Tecnológicos	Limitado	-	40%	Carpeta compartida	¿El acceso de lectura y escritura al código fuente, herramientas de desarrollo y bibliotecas de software se gestiona adecuadamente?	NO EXISTE		X	Aplicaciones
A.8.5	Autenticación segura	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿Se implementan tecnologías y procedimientos de autenticación segura con base en las restricciones de acceso a la información y la política temática específica sobre control de acceso?	NO EXISTE		X	Aplicaciones
A.8.6	Gestión de la capacidad	Tecnológicos	Gestionado	80%	-	Informe técnico, TDR	¿El uso de los recursos se supervisa y ajusta en consonancia con los requisitos de capacidad actuales y previstos?	Consola de antivirus	X		Infraestructura
A.8.7	Protección contra código malicioso (malware)	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿La protección contra el malware se implementa y respalda mediante una adecuada concienciación del usuario?	NO EXISTE		X	Soporte
A.8.8	Gestión de vulnerabilidades técnicas	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿Se obtiene información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se evalua la exposición de la organización a dichas vulnerabilidades y se deben tomar las medidas apropiadas?	NO EXISTE		X	Infraestructura
A.8.9	Gestión de la configuración	Tecnológicos	Limitado	-	40%	Inventario informàtico	¿Existe un Inventario de información y otros activos asociados?	Inventario de activos / Informe Técnico		X	Infraestructura
A.8.10	Borrado de información	Tecnológicos	Inicial	-	20%	Solo en algunos casos	¿La información almacenada en sistemas, dispositivos o cualquier otro medio de almacenamiento de información se elimina cuando ya no sea necesaria?	NO EXISTE		X	Infraestructura

EVALUACIÒN DEL SGSI DEL GADMCE - Declaración de Aplicabilidad (SoA) y estado de los controles de la seguridad de la información NORMA ISO27001:2022 ANEXO

Control	Nombre	Tipo	Estado	Cumple	No cumple	Evidencia	Preguntas realizadas	Respuesta	Si	No	Area responsible
A.8.11	Enmascarado de datos	Tecnológicos	Inexistente	-	0%	No se presenta evidencia	¿El enmascaramiento de datos se utiliza de acuerdo con la política temática específica de la organización sobre control de acceso y otras políticas específicas relacionadas y requisitos comerciales, teniendo en cuenta la legislación aplicable?	NO EXISTE		X	Infraestructura
A.8.12	Prevención de filtración de datos	Tecnológicos	Limitado	-	40%	Reglamento interno, politicas de seguridad	¿Se aplican medidas de prevención de fuga de datos a los sistemas, redes y cualesquiera otros dispositivos que procesen, almacenen o transmitan información sensible?	NO EXISTE		X	Infraestructura
A.8.13	Respaldo de información / Copia de seguridad de la información	Tecnológicos	Gestionado	80%	-	Servidor de respaldos, copias de seguridad	¿Las copias de seguridad de la información, el software y los sistemas se mantienen y prueban periódicamente de acuerdo con la política temática específica acordada sobre copias de seguridad?	Informe / Copia de seguridad	X		Infraestructura
A.8.14	Redundancia de las instalaciones de procesamiento de información	Tecnológicos	Definido	60%	-	Fotografias de servidores back up	¿Las instalaciones de procesamiento de información se implementan con redundancia suficiente para cumplir con los requisitos de disponibilidad?	SERVIDORES BACK UP	X		Infraestructura
A.8.15	Registración / Inicio sesión	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿Se producen, almacenan, protegen y analizan registros que registren actividades, excepciones, fallas y otros eventos relevantes?	NO EXISTE		X	Infraestructura
A.8.16	Actividades de supervisión / seguimiento	Tecnológicos	Limitado	-	40%	Solo cuando se reportan se registran	¿Se monitorean las redes, sistemas y aplicaciones para detectar comportamientos anómalos y se toman las acciones apropiadas para evaluar posibles incidentes de seguridad de la información?	REPORTES	X		Infraestructura
A.8.17	Sincronización de reloj (clock)	Tecnológicos	Gestionado	80%	-	Fotografia	¿Los relojes de los sistemas de procesamiento de información utilizados por la organización están sincronizados con las fuentes horarias aprobadas?	INFORME TECNICO	X		Infraestructura
A.8.18	Uso de programas utilitarios privilegiados	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿El uso de programas de utilidad que puedan anular los controles del sistema y de las aplicaciones están restringido y estrictamente controlado?	NO EXISTE		X	Soporte
A.8.19	Instalación de software en sistemas operativos.	Tecnológicos	Gestionado	80%	-	Politica de seguridad	¿Se implementar procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos?	Informe Tècnico	X		Soporte
A.8.20	Seguridad en redes	Tecnológicos	Gestionado	80%	-	Informe Tècnico	¿Las redes y los dispositivos de red se protegen, gestionan y controlan para proteger la información en los sistemas y aplicaciones?	Informe Técnico / Equipo de seguridad periferica	X		Infraestructura
A.8.21	Seguridad de servicios de red	Tecnológicos	Optimizado	100%	-	Informe Tècnico	¿Se identifican, implementan y monitorean los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red?	Informe Tècnico	X		Infraestructura
A.8.22	Segregación de redes	Tecnológicos	Gestionado	80%	-	Inventaario de red	¿Los grupos de servicios de información, usuarios y sistemas de información están segregados en las redes de la organización?	Informe Tècnico	X		Infraestructura
A.8.23	Filtrado web	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿El acceso a sitios web externos se gestiona para reducir la exposición a contenidos maliciosos?	NO EXISTE		X	Infraestructura
A.8.24	Uso de criptografia	Tecnológicos	Inexistente	-	0%	No se presenta evidencia	¿Se definen e implementan reglas para el uso eficaz de la criptografia, incluida la gestión de claves criptográficas?	NO EXISTE		X	Infraestructura
A.8.25	Ciclo de vida de desarrollo seguro	Tecnológicos	Inexistente	-	0%	No se presenta evidencia	¿Se establecen y aplican reglas para el desarrollo seguro de software y sistemas?	NO EXISTE		X	Aplicaciones
A.8.26	Requerimientos de seguridad en aplicaciones	Tecnológicos	Inexistente	-	0%	No se presenta evidencia	¿Los requisitos de seguridad de la información se identifican, especifican y aprueban al desarrollar o adquirir aplicaciones?	NO EXISTE		X	Aplicaciones
A.8.27	Principios de ingeniería y arquitectura de sistemas seguros	Tecnológicos	Inexistente	-	0%	No se presenta evidencia	¿Se establecen, documentan, mantienen y aplican principios para la ingeniería de sistemas seguros a cualquier actividad de desarrollo de sistemas de información?	NO EXISTE		X	Aplicaciones
A.8.28	Codificación segura	Tecnológicos	Gestionado	80%	-	informe tècnico	¿Se aplican principios de codificación segura al desarrollo de software?	Informe Tècnico	X		Aplicaciones
A.8.29	Pruebas de seguridad en desarrollo y aceptación	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿Los procesos de prueba de seguridad se definen e implementan en el ciclo de vida del desarrollo?	NO EXISTE		X	Aplicaciones
A.8.30	Desarrollo tercerizado o Desarrollo subcontratado	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿La organización dirige, monitorea y revisa las actividades relacionadas con el desarrollo del sistema subcontratado?	NO EXISTE		X	Aplicaciones
A.8.31	Separación de los entornos de desarrollo, prueba y producción	Tecnológicos	Definido	60%	-	Ambientes de prueba, informe	¿Los entornos de desarrollo, prueba y producción estan separados y asegurados?	Informe Tècnico / Ambiente de pruebas	X		Aplicaciones
A.8.32	Gestión de cambios	Tecnológicos	Inexistente	-	0%	No se presenta evidencia	¿Los cambios en las instalaciones de procesamiento de información y los sistemas de información están sujetos a procedimientos de gestión de cambios?	NO EXISTE		X	Aplicaciones
A.8.33	Información de prueba	Tecnológicos	Limitado	-	40%	No se presenta evidencia	¿La información de prueba se selecciona, protege y gestiona adecuadamente?	NO EXISTE		X	Aplicaciones
A.8.34	Protección de los sistemas de información durante las pruebas de auditoría	Tecnológicos	Inicial	-	20%	No se presenta evidencia	¿Las pruebas de auditoría y otras actividades de aseguramiento que impliquen la evaluación de sistemas operativos se planifican y acuerdan entre el evaluador y la dirección correspondiente?	NO EXISTE		X	Aplicaciones
		Número de controles:	**93**	**32**	**61**	**39%**	**Grado de cumplimiento**				

ANEXO C

Modelo de encuesta cerrada dirigida a los empleados administrativos (usuarios) de TI del GADMCE en base a la norma ISO 270001:2022

EVALUACIÓN DE LA SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN DEL GAD MUNICIPAL DE ESMERALDAS BASADO EN LAS NORMAS DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO
PERIODO 2023 - 2024

Encuesta a empleados pùblicos administrativos (usuarios)

Estimado funcionario, en el siguiente conjunto de preguntas relacionadas a la Seguridad de Tecnologias de Información que en la Direcciòn de TIC se lleva adelante, marque con una "X" el casillero que mejor represente su respuesta. Gracias.

Grupo de preguntas N°1: Organizacionales - Políticas de seguridad de la información

Item	Pregunta	Si	No	No conoce
A	¿Las políticas de seguridad de la información son importantes para la institución?			
B	¿Se están aplicando las políticas de seguridad de la información en la institución?			
C	¿La institución ha elaborado y requerido a todo el personal el cumplimiento de las políticas de seguridad de la información?			
D	¿Se establecen e implementan reglas para controlar el acceso físico (credenciales y biométricos) y lógico (usuarios y contraseñas) a la información y otros activos informáticos asociados, con base en los requisitos de seguridad de la información de la institución?			
E	¿La institución identifica y cumple con los requisitos relacionados con la preservación de la privacidad y la protección de los datos personales (PII) de acuerdo con las leyes, regulaciones y requisitos contractuales aplicables?			

Grupo de preguntas N°2: De personas - Capacitación y consciencia del personal

Item	Pregunta	Si	No	No conoce
A	¿El personal de la organización recibe concientización, educación y/o capacitación apropiadas sobre seguridad de la información, seguridad informática o ciberseguridad, según sea relevante para su función laboral?			
B	¿La institución hace firmar a los funcionarios algún acuerdo sobre la confidencialidad de la información que maneja o posee en el desempeño de sus actividades laborales?			
C	¿Se implementan medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la organización?			
D	¿La institución implementa utiliza algún sistema de registro de incidentes (mesa de ayuda - Helpdesk) u otro mecanismo para que el personal informe eventos de seguridad de la información, seguridad informática o ciberseguridad observados o sospechosos de manera oportuna?			
E	¿Está consciente de las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información?			

Grupo de preguntas N°3: Físicos - Seguridad física y ambiental de la infraestructura tecnológica

Item	Pregunta	Si	No	No conoce
A	¿Las medidas de seguridad física que la institución tiene para salvaguardar los activos informáticos son las adecuadas, es decir se cuenta con guardianía en las entradas de las instalaciones, control de accesos a oficinas, cámaras de seguridad, y perímetros de seguridad en donde se encuentran los activos de información?			
B	¿La institución cuenta con la protección contra amenazas físicas y ambientales, como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura tecnológica o equipamiento informático?			
C	¿El activo informático a su cargo (o equipos de cómputo con los que trabaja) está ubicado de forma segura (libre de inundación, humedad, polvo, o daño eléctrico) y protegida (libre de robo, vandalismo o sabotaje) mediante el acceso restringido a su área de trabajo?			
D	¿Los cables que transporta energía, red de datos, internet o servicios de información de soporte donde se conectan sus equipos están protegidos contra interceptaciones, interferencias o daños?			
E	¿Los equipos informáticos (Hardware y software) de la institución reciben periódicamente (al menos una vez al año) mantenimiento preventivo para garantizar la disponibilidad, integridad y confidencialidad de la información?			

Grupo de preguntas N°4: Tecnológicos - Seguridad de activos informáticos

Item	Pregunta	Si	No	No conoce
A	¿La institución tiene instalado y actualizado algún programa de antivirus para proteger la información almacenada (archivos y carpetas), procesada (sistemas) o accesible (correo electrónico) a través del activo informático (computador) asignado para el cumplimiento de sus funciones en calidad de usuario?			
B	¿Se implementan tecnologías y procedimientos de autenticación segura (usuario y contraseña) para el control de acceso al sistema operativo, la red de datos o los sistemas y aplicaciones en el computador; con base en las restricciones de acceso a la información?			
C	¿Se aplican medidas de prevención de fuga de datos de los sistemas, filtración de información de la institución a través de la red y cualesquiera otros dispositivos que procesen, almacenen o transmitan información sensible o confidencial?			
D	¿Tiene asignado bienes o activos informáticos (computador, impresora, monitor, y otro equipo) para el desarrollo de sus actividades como funcionario público?			
E	¿Las redes y los dispositivos de red se protegen, gestionan y controlan para proteger la información en los sistemas y aplicaciones?			

ANEXO D

Modelo de entrevista estructurada con preguntas abiertas a los funcionarios de la Dirección de Tecnologías de Información del GADMCE

1. ¿Describa sus funciones y subproceso al que pertenece dentro de la Dirección de TIC en el municipio de Esmeraldas?

_____

_____

2. ¿Cuál es la situación actual de la seguridad de la infraestructura tecnológica a su cargo o con la que usted desarrolla sus actividades?

_____

_____

3. ¿Menciones los dos activos informáticos más relevantes o equipos informáticos críticos que estén asignados a usted?

_____

_____

4. ¿Cómo se han identificado los riesgos a los que están expuestos los principales activos informáticos que tiene a su cargo?

_____

_____

5. ¿Cuál es el valor monetario del bien informático que tiene asignado?

_____

_____

6. ¿Cuáles son las amenazas que tienen esos activos considerados como críticos?

_____

_____

7. ¿Cuáles son las vulnerabilidades que presentan esos equipos asignados ante las amenazas antes mencionadas?

_____

_____

8. ¿Qué mecanismo, medidas o controles se han implementado para mitigar los riesgos de los activos informáticos a su cargo?

_____

_____

ANEXO E

Plantilla resumen de entrevistas estructuradas y evaluación del riesgo informático de los activos de TI del GADMCE

ANÁLISIS DE RIESGOS						Análisis de Riesgos						Evaluación de Riesgos	
							Impacto			Probabilidad			
Item	Subprocesos	Responsable	Nombre Activo	Amenaza	Vulnerabilidad	Valor	C	I	D	CID	Nivel de amenaza	Nivel de vulnerabilidad	Controles (Procesos Actividades Tareas)	Cálculo de Evaluación Riesgo	Nivel de Riesgo
C01	DIFY SEG	[illegible]	[illegible]	Poco espacio de almacenamiento	Falta de redundancia	$ 40.000,00	3	3	3	3,00	2	2	A.5.23,34 A.7.7,10	12,00	ALTO
C02	DIFY SEG	[illegible]	[illegible]	Ataques externos	Caída de los servicios	$ 20.000,00	3	3	3	3,00	3	1	A.8.5,6,13,7,21	9,00	MEDIO
C03	DIFY SEG	[illegible]	[illegible]	Terremotos, desastres naturales	Daños de equipos	$ 40.000,00	3	3	3	3,00	2	1	A.5.26,29 A.7.5 A.8.14	6,00	MEDIO
C04	DIFY SEG	[illegible]	[illegible]	Ambiente Clima desgaste	Daño en bateria	$ 5.000,00	1	1	3	1,67	2	2	A.5.26,29 A.7.5 A.8.14	6,67	MEDIO
C05	DIFY SEG	[illegible]	[illegible]	Accidentes de transito en postes	Rompimiento de la fibra	$ 400.000,00	1	1	3	1,67	2	3	A.5.6,8 A.8.32	10,00	ALTO
C06	DIFY SEG	[illegible]	[illegible]	Vandalismo	Poca vigilancia	$ 6.000,00	1	1	3	1,67	2	2	A.7.9	6,67	MEDIO
C07	DIFY SEG	[illegible]	[illegible]	Variaciones de voltaje	Inhibicion en equipos	$ 10.000,00	1	1	3	1,67	2	2	A.8.11,15,16	6,67	MEDIO
C08	DIFY SEG	[illegible]	[illegible]	Variaciones de voltaje	Inhibicion en equipos	$ 1.000,00	1	1	3	1,67	2	2	A.8.11,15,16	6,67	MEDIO
C09	DIFY SEG	[illegible]	[illegible]	Demasiadas conexiones concurrentes	Inhibicion en equipos	$ 30.000,00	1	1	3	1,67	1	3	A.7.11 A.8.17,33	5,00	MEDIO
C10	DIFY SEG	[illegible]	[illegible]	Climas extremos	Inhibicion en equipos	$ 10.000,00	1	1	3	1,67	2	2	A.7.11 A.8.17,34	6,67	MEDIO
C11	DIFY SEG	[illegible]	[illegible]	Poca proteccion y cuidados	Daño en punto de red	$ 30.000,00	1	1	3	1,67	2	3	A.7.12 A.8.20 22	10,00	ALTO
C12	DIFY SEG	[illegible]	[illegible]	Vandalismo	Poca vigilancia	$ 5.000,00	1	1	3	1,67	2	2	A.7.9	6,67	MEDIO
C13	APLY SIS	[illegible]	[illegible]	Ciber delincuentes	Caída de los servicios	$ 2.000,00	3	3	3	3,00	1	3	A.8.23,24	9,00	MEDIO
C14	APLY SIS	[illegible]	[illegible]	spam ramsonware	Secuestro de informacion	$ 1.000,00	2	3	3	2,67	2	3	A.8.23,24	16,00	ALTO
C15	APLY SIS	[illegible]	[illegible]	Participacion de Transitadores	Cobro por tramites corrupcion	$ 12.000,00	3	3	2	2,67	3	2	A.5.16,17,28 A.8.25,27,28,29	16,00	ALTO
C16	APLY SIS	[illegible]	[illegible]	Manejo de contraseñas en usuario	Fuga de informacion	$ 5.000,00	3	2	2	2,33	2	2	A.5.16,17,28 A.8.25,27,28,29	9,33	ALTO
C17	APLY SIS	[illegible]	[illegible]	migracion de datos inconsistentes	Errores en las emisiones	$ 20.000,00	2	3	2	2,33	3	2	A.6.2,5 A.8.3,31,34	14,00	ALTO
C18	APLY SIS	[illegible]	[illegible]	Variacion de voltaje	Daño de fuente de poder	$ 1.000,00	2	3	2	2,33	2	2	A.6.2,5 A.8.3,31,34	9,33	ALTO
C19	APLY SIS	[illegible]	[illegible]	Integracion con base alfanumerica antiena	Incompatibilidad sw base con plataforma de desarrollo	$ 35.000,00	2	1	3	2,00	2	2	A.5.10,12,13,14,15,18,33 A.8.2	8,00	MEDIO
C20	APLY SIS	[illegible]	[illegible]	Version limitada y obsoleta	Falta de controles	$ 40.000,00	3	3	2	2,67	2	2	A.5.10,12,13,14,15A.8.3	10,67	ALTO
C21	APLY SIS	[illegible]	[illegible]	Uso masivo de ciudadanos	Saturacion del sistema	$ 5.000,00	1	1	3	1,67	2	1	A.8.4,26,30	3,33	BAJO
C22	APLY SIS	[illegible]	[illegible]	Vandalismo	Poca vigilancia	$ 1.000,00	1	1	3	1,67	2	2	A.7.9	6,67	MEDIO
C23	APLY SIS	[illegible]	[illegible]	Vandalismo y sabotaje	Daños en los dispositivos vehiculares	$ 3.000,00	1	1	3	1,67	3	2	A.5.19,22 A.6.6,8	10,00	ALTO
C24	APLY SIS	[illegible]	[illegible]	Falta de control de uso	Informacion desactualizada	$ 2.000,00	2	3	1	2,00	3	2	A.5.10,22 A.6.6,9	12,00	ALTO
C25	APLY SIS	[illegible]	[illegible]	Falta de servidores redundantes	Daños en los registros	$ 10.000,00	1	2	3	2,00	2	3	A.5.4,21 A.8.8, 9	12,00	ALTO
C26	APLY SIS	[illegible]	[illegible]	Falta de un almacen seguro	Robo de suministros	$ 2.000,00	1	1	1	1,00	2	3	A.5.4,21 A.8.8, 10	6,00	MEDIO
C27	SOPY SER	[illegible]	[illegible]	Variaciones electricas	Daño en equipos	$ 150.000,00	2	3	3	2,67	2	2	A.5.9,11 A.7.8,13,14	10,67	ALTO
C28	SOPY SER	[illegible]	[illegible]	Falta de mantenimiento especializado	Daño del equipo	$ 5.000,00	1	1	2	1,33	2	2	A.8.1,10,19	5,33	MEDIO
C29	SOPY SER	[illegible]	[illegible]	Acceso de personas no autorizadas	Existencia de áreas sin vigilancia	$ 10.000,00	2	3	3	2,67	3	2	A.5.7,25 A.7.2,3,4	16,00	ALTO
C30	SOPY SER	[illegible]	[illegible]	Variaciones de voltaje	Apagado del sistema	$ 5.000,00	1	1	2	1,33	3	2	A.5.7,25 A.7.2,5,5	8,00	MEDIO
C31	SOPY SER	[illegible]	[illegible]	Crisis economica institucional	Desactivacion	$ 4.000,00	2	3	3	2,67	2	2	A.5.20, 32	10,67	ALTO
C32	SOPY SER	[illegible]	[illegible]	Crisis economica institucional	Desactivacion	$ 5.000,00	2	2	2	2,00	2	2	A.5.20, 32	8,00	MEDIO
C33	SOPY SER	[illegible]	[illegible]	Mal uso de equipo	Trabas en el papel	$ 10.000,00	1	1	2	1,33	2	2	A.5.30	5,33	MEDIO
C34	SOPY SER	[illegible]	[illegible]	Exceso de impresiones diarias	Daño de cabezales	$ 5.000,00	1	1	3	1,67	3	3	A.5.30	15,00	ALTO
C35	SOPY SER	[illegible]	[illegible]	Mal manejo del PC	Daño en el equipo	$ 10.000,00	1	1	2	1,33	2	1	A.5.27 A.6.3 A.8.18	2,67	BAJO
C36	SOPY SER	[illegible]	[illegible]	Mal manejo del PC	Daño en el equipo	$ 4.000,00	1	1	2	1,33	2	2	A.5.27 A.6.3 A.8.19	5,33	MEDIO
C37	PRY Y PRC	[illegible]	[illegible]	Daño en equipo AC	Sobre calentamiento	$ 80.000,00	2	1	3	2,00	1	2	A.5.24	4,00	MEDIO
C38	PRY Y PRC	[illegible]	[illegible]	Mal uso de equipos	Daño en operacion	$ 8.000,00	1	1	2	1,33	1	2	A.5.25	2,67	BAJO
C39	DIR G TIC	[illegible]	[illegible]	Inundacion por lluvia	Daños en el techo	$ 40.000,00	1	2	3	2,00	1	3	A.5.37, A.8.12	6,00	MEDIO
C40	DIR G TIC	[illegible]	[illegible]	Variacion de voltaje	Daño de fuente de poder	$ 1.000,00	1	2	2	2,33	2	2	A.5.37, A.8.13	9,33	ALTO
C41	PRY Y PRC	[illegible]	[illegible]	Vandalismo	Poca vigilancia	$ 180.000,00	1	1	3	1,67	2	2	A.7.9	6,67	MEDIO
C42	PRY Y PRC	[illegible]	[illegible]	Desgaste de baterias	Perdida de energia	$ 30.000,00	1	1	3	1,67	3	3	A.7.10	15,00	ALTO
C43	DIR G TIC	[illegible]	[illegible]	Robo delincuencia	Falta de seguridad	$ 1.500,00	2	2	3	2,33	2	2	A.5.1,2,3,5,25,31,35,36	9,33	ALTO
C44	DIR G TIC	[illegible]	[illegible]	Robo delincuencia	Falta de seguridad	$ 6.000,00	1	1	1	1,00	3	3	A.6.1,4,7 A.7.1,6	9,00	MEDIO
C45	ALCALDIA	[illegible]	[illegible]	Robo delincuencia	Acceso no autorizado	$ 1.500,00	3	3	3	3,00	3	1	A.5.1,2,3,5,25,31,35,36	9,00	MEDIO
C46	ALCALDIA	[illegible]	[illegible]	Ciber delincuencia - fraude	Accedo no autorizado	$ 30,00	2	2	1	1,67	2	1	A.6.1,4,7 A.7.1,6	3,33	BAJO
C47	ALCALDIA	[illegible]	[illegible]	Acceso de muchas personas	Espionaje	$ 10.000,00	3	1	1	1,67	2	2	A.6.1,4,7 A.7.1,6	6,67	MEDIO
C48	FINANCIERO	[illegible]	[illegible]	Ciber delincuencia - fraude	Acceso no autorizado	$ 30,00	2	2	1	1,67	2	2	A.6.1,4,7 A.7.1,6	6,67	MEDIO
C49	FINANCIERO	[illegible]	[illegible]	Robo delincuencia	Falta de seguridad	$ 1.500,00	1	1	1	1,00	2	2	A.6.1,4,7 A.7.1,6	4,00	MEDIO
C50	FINANCIERO	[illegible]	[illegible]	Acceso de muchas personas	Fuga de informacion	$ 1.000,00	3	3	3	3,00	1	2	A.6.1,4,7 A.7.1,6	6,00	MEDIO

ANEXO F

Matriz de evaluación normas de control interno 410

Entidad: GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTON ESMERALDAS

Area o rubro evaluado: Evaluación Integral del Sistema de Control Interno Institucional

Período : 2023 - 2024 — DEL 4 de febrero de 2024 AL 5 de abril de 2024

	Organización de la unidad deTIC	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-01**
No.	Preguntas de evaluaciòn y diagnòstico		1	2	3	4	5	**80,00**	Acciones Tomadas por la Entidad
			5,0	10,0	15,0	20,0	25,0		
1	¿La estructura organizacional de la entidad contiene una unidad de tecnología de información establecida formalmente dentro de los niveles de asesoría y apoyo a la alta direcciòn y unidades usuarias?						X	✓25,00	Estructura Orgànica por procesos
2	¿Las facultades establecidas para la unidad de Tecnología de Información de la institución contempla la rectoría, regulación y seguimiento de los temas tecnológicos de la institución?						X	✓25,00	Estructura Orgànica por procesos
3	¿La estructura organizacional de tecnología de información y comunicación refleja las necesidades institucionales, a través de un esquema mínimo de áreas que cubran proyectos tecnológicos, infraestructura tecnológica, soporte interno y externo de ser el caso, así como, de seguridad de tecnologías de la información y comunicación?						X	✓25,00	Estructura Orgànica por procesos
4	¿Se ha incorporado un oficial de seguridad de la información que estará a cargo de un área independiente de la unidad de tecnologías de la información y comunicaciones?		X					✗5,00	Ninguna

	Comité de Tecnologías de la Información y Comunicaciones	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-02**
No.	Preguntas de evaluaciòn y diagnòstico		1	2	3	4	5	**20,00**	Acciones Tomadas por la Entidad
			4,0	8,0	12,0	16,0	20,0		
1	¿La máxima autoridad de la entidad instrumentò la creación de un Comité de Tecnologías de la Información y Comunicaciones?		X					✓4,00	Ninguna
2	¿El Comité de Tecnologías de la Información y Comunicaciones està definido en función del tamaño y complejidad de la entidad?		X					✓4,00	Ninguna
3	¿El comitè se encarga de coordinar los lineamientos, objetivos y alcance, para el desarrollo de proyectos relacionados con el uso de las tecnologías de la información y comunicaciones?		X					✓4,00	Ninguna
4	¿El enfoque del comitè responde a un criterio unificado para la ejecución de uno o varios de los procesos institucionales (de la cadena de valor), incluyendo las entidades adscritas y otras instituciones que la conforman?		x					✓4,00	Ninguna
5	¿La integraciòn del comite se realizò con las siguentes àreas: talento humano, administrativa, planificación, comunicación social, tecnologías de la información, y jurídica?		X					✓4,00	Ninguna

	Segregación de funciones	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-03**
No.	Preguntas de evaluaciòn y diagnòstico		1	2	3	4	5	**56,00**	Acciones Tomadas por la Entidad
			4,0	8,0	12,0	16,0	20,0		
1	¿Las funciones y responsabilidades del personal de tecnología de información y comunicaciones y de los usuarios de los sistemas de información están claramente definidos en el estatuto orgánico de la entidad y fueron formalmente comunicadas?					X		✓16,00	Estatuto Organico
2	¿La asignación de funciones y sus respectivas responsabilidades garantizan una adecuada segregación, evitando funciones incompatibles?					X		✓16,00	Manual de puestos
3	¿Se ha realizado supervisiones del adecuado rendimiento del recurso humano de tecnología, en función del cual se ha determinado la necesidad de reubicación o incorporación de nuevo personal?			X				!8,00	Informe de necesidad de nuevo personal
4	¿La evaluación de desempeño del recurso humano de la unidad de tecnología se estableció en función de las atribuciones, responsabilidades, actividades, procedimientos, productos, habilidades, experiencia y otras condiciones determinadas en el estatuto orgánico de la entidad?				X			!12,00	Evaluación de desempeño anual
5	¿El Oficial de Seguridad de la Información cumple las funciones establecidas en la normativa vigente?		X					✗4,00	Ninguna

	Plan estratégico y operativo de TIC	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-04**
No.	Preguntas de evaluaciòn y diagnòstico		1	2	3	4	5	**40,00**	Acciones Tomadas por la Entidad
			2,9	5,7	8,6	11,4	14,3		
1	¿La unidad de tecnologías de la información y comunicaciones ha elaborado e implementado un plan estratégico para administrar y dirigir todos los recursos tecnológicos y de comunicación?		X					✗2,86	Ninguna
2	¿El Plan informático estratégico de tecnología está alineado con el Plan Estratégico Institucional, con las políticas públcias sectoriales y con el Plan Nacional de Desarrollo ?		X					✗2,86	Ninguna
3	¿El Plan informático estratégico de tecnología incluye uincluirá un análisis de la situación actual y las propuestas de mejora con la participación de todas las unidades de la organización, considerando la estructura interna, procesos, infraestructura, comunicaciones, aplicaciones y servicios a brindar, así como la definición de estrategias, análisis de riesgos, cronogramas, presupuesto de la inversión y operativo, fuentes de financiamiento y los requerimientos legales y regulatorios de ser necesario?		X					✗2,86	Ninguna
4	¿La unidad de tecnologías de la información y comunicacion ha elaborado planes operativos alineados con el plan estratégico de tecnologías de la información y comunicación y los objetivos estratégicos de la institución?				X			✓8,57	POA 2024
5	¿El Plan Anual Operativo de tecnología de información incluye los portafolios de proyectos y servicios, la arquitectura y dirección de tecnologías, las estrategias de migración, planes de contingencia y la incorporación de nuevas tecnologías de información?				X			✓8,57	POA 2024
6	¿El Plan informático estratégico y los planes operativos de tecnología están debidamente presupuestados y están incorporados al presupuesto anual de la organización?			X				!5,71	POA 2024, No existe plan estratègico
7	¿Las situaciones de excepción han sido autorizadas por la máxima autoridad de la entidad o por la instancia que corresponda; y, se someten al trámite de reforma pertinente?				X			✓8,57	Reforma POA 2024

	Políticas y procedimientos	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-05**
No.	Preguntas de evaluaciòn y diagnòstico		1	2	3	4	5	**37,14**	Acciones Tomadas por la Entidad
			2,9	5,7	8,6	11,4	14,3		
1	¿Las políticas y procedimientos que permiten organizar apropiadamente el área de tecnología de información y asignar el talento humano calificado e infraestructura tecnológica necesaria, fueron aprobados formalmente por la máxima autoridad?		X					✗2,86	Politicas de Seguridad sin aprobacion
2	¿La Unidad de Tecnología de Información definió, documentó y difundió las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones en la organización?				X			✓8,57	Politicas de Seguridad
3	¿Las políticas, estándares y procedimientos de tecnología fueron actualizados permanentemente e incluyen las tareas, los responsables de su ejecución, los procesos de excepción, el enfoque de cumplimiento y el control de los procesos que están normando, así como, las sanciones administrativas a que hubiere lugar si no se cumplieran?		X					✗2,86	Politicas de Seguridad actualizadas
4	¿Las políticas y procedimientos de tecnología de información contienen los temas de calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas, mensajería de datos, legalidad del softw are, entre otros, y mantienen consistencia con leyes conexas emitidas por los organismos competentes y estándares de tecnología de la información?				X			✓8,57	Politicas de Seguridad revisadas
5	¿Se han establecido procedimientos de comunicación, difusión y coordinación que permitan relacionar adecuadamente las atribuciones, competencias, procesos técnicos, actividades y productos desarrollados por tecnología de información y los de la organización?		X					✗2,86	Ninguna
6	¿Se encuentran incorporados en los procesos organizacionales relacionados con las tecnologías de información, controles, sistemas de aseguramiento de calidad, de gestión riesgo y estándares tecnológicos?		X					✗2,86	Ninguna
7	¿La unidad de tecnología de información ha promovido y establecido convenios con otras organizaciones o terceros a fin de promover y viabilizar el intercambio de información interinstitucional, así como programas de aplicación desarrollados al interior de las instituciones o prestación de servicios relacionados con la tecnología de información?				X			✓8,57	Convenios: ECU 911 DINARDAT PUCESE/UTLV

Entidad: GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTON ESMERALDAS

Area o rubro evaluado: Evaluación Integral del Sistema de Control Interno Institucional

Período : 2023 - 2024 | DEL 4 de febrero de 2024 AL 5 de abril de 2024

Clasificación y arquitectura de la información	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-06**
No.	Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**25,00**	Acciones Tomadas por la Entidad
		5,0	10,0	15,0	20,0	25,0		
1	¿La unidad de tecnologías de la información y comunicaciones definiò un proceso de clasificación de los datos para especificar y aplicar niveles de seguridad y propiedad, orientado a asegurar que los datos se encuentren organizados eficientemente?	X					✗ 5,00	Ninguna
2	¿La unidad de tecnologías de la información y comunicacionen adoptò las medidas para garantizar su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes, en concordancia con las necesidades operativas de las diferentes unidades usuarias?	X					✗ 5,00	Ninguna
3	¿El diseño de la arquitectura de la información que se define, se documenta y consta en un diccionario de datos corporativo que será actualizado de forma permanente		X				✓ 10,00	Elaboración de Diccionario de datos
4	¿El diseño de la arquitectura de la información que se define incluye las reglas de validación y los controles de integridad y consistencia, con la identificación de los sistemas o módulos que lo conforman, sus relaciones y los objetivos estratégicos a los que apoyan a fin de facilitar la incorporación de las aplicaciones y procesos institucionales de manera transparente?	X					✗ 5,00	Ninguna

Administración de proyectos tecnológicos	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-07**
No.	Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**32,50**	Acciones Tomadas por la Entidad
		2,5	5,0	7,5	10,0	12,5		
1	¿El Departamento de Tecnología de Información definió una metodologìa que faciliten la administración de todos los proyectos informáticos que ejecuten las áreas ténicas que conforman dicha unidad?	X					✗ 2,50	Ninguna
2	¿Los proyectos de tecnología de información contienen docuemntación y aprobación de la justificación que da origen al proyecto, asi como la naturaleza, objetivos y alcance del proyecto y su relación con otros proyectos institucionales, cronograma de actividades, recurso humano, tecnológico y financiero requerido y los planes de pruebas y capacitación correspondientes?		X				! 5,00	Contrato e informe BDE
3	¿En la formulación de los proyectos se consideró el costo Total de Propiedad, que incluya no solo el costo de compra, sino costos directos e indirectos, los beneficios relacionados con la compra de equipos o programas informáticos, aspectos del uso y mantenimiento, formación para el personal de soporte y usuarios, así como el costo de operación y de los equipos o trabajos de consultoría necesarios?	X					✗ 2,50	Ninguna
4	¿Los proyectos de tecnología informática tienen asignado formalmente un servidor responsable con capacidad de decisión y autoridad y administradores o líderes funcionales y tecnológicos con la descripción de sus funciones y responsabilidades?			X			✓ 7,50	Contrato e informe BDE
5	¿En los proyectos de tecnología informática se identifican, aprueban y comunican las etapas de: inicio, planeación, ejecución, control, monitoreo y cierre de proyectos, así como los entregables, aprobaciones y compromisos formales mediante el uso de actas o documentos electrónicos legalizados?	X					✗ 2,50	Ninguna
6	¿En la ejecución de los proyectos de tecnologías informáticas se evalúo permanentemente los riesgos identificados y se registró su evolución para que sirva de insumo para la planificación de nuevoas proyectos?	X					✗ 2,50	Ninguna
7	¿La unidad de tecnología de información elaboró un plan de control de cambios y un plan de aseguramiento de la calidad, cuya ejecución fue aprobado por las partes competentes?	X					✗ 2,50	Ninguna
8	¿La unidad de tecnología de información registró el monitoreo realizado al avance del proyecto y la evaluación final obtenida en la que se incluye el cierre formal y pruebas que certifiquen la calidad, el cumplimiento de los objetvios planetados y los beneficios obtenidos?			X			✓ 7,50	Contrato e informe BDE

Desarrollo, mantenimiento y adquisición de software de aplicación	Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-08**
No.	Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**30,67**	Acciones Tomadas por la Entidad
		1,3	2,7	4,0	5,3	6,7		
1	¿La unidad de tecnologías de la información y comunicaciones regulò los procesos de desarrollo, mantenimiento y adquisición de softw are de aplicación y de usuario final, estableciendo, documentando y aprobando un procedimiento o metodología para estas actividades?	X					✗ 1,33	Ninguna
2	¿La adquisición de softw are o soluciones tecnológicas se realizan sobre la base del portafolio de proyectos y servicios priorizados en los planes estratégico y operativo, previamente aprobados, considerando las políticas públicas establecidas por el Estado, o en el caso contrario son autorizadas por la máxima autoridad previa justificación técnica documentada?			X			✓ 4,00	Contrato e informe BDE
3	¿En los procesos de desarrollo, mantenimiento o adquisición de softw are aplicativo se consideró la adopción, mantenimiento y aplicación de políticas públicas y estándares internacionales para: codificación de softw are, nomenclaturas, interfaz de usuario, interoperabilidad, eficiencia de desempeño de sistemas, escalabilidad, validación contra requerimientos, planes de pruebas unitarias y de integración.		X				! 2,67	Informe tecnico
4	¿Se Identifican, priorizan, especificación acuerdos de los requerimientos funcionales y técnicos institucionales con la participación y aprobación formal de las unidades usuarias, incluyendo: tipos de usuarios, ciclo de vida del softw are, seguridad, plan de pruebas y trazabilidad o pistas de auditoría de las transacciones en caso aplique?		X				! 2,67	Contrato e informe BDE
5	Se especifican criterios de aceptación de los requerimientos considerando la definición detallada de las necesidades que motivan el requerimiento, su factibilidad tecnológica y económica, el análisis de riesgo y de costo-beneficio, la estrategia de desarrollo o compra del softw are de aplicación, así como el tratamiento que se dará a aquellos procesos de emergencia que pudieran presentarse?	X					✗ 1,33	Ninguna
6	¿En la contratación de servicios externos de desarrollo de sistemas se estipula que el softw are, la documentación y demás servicios adquiridos se sometan a prueba y revisión antes de la aceptación por parte de la unidad de TIC y de las áreas usuarias, incluyendo aspectos relativos a la seguridad de los desarrollos.	X					✗ 1,33	Ninguna
7	¿Se aplican las disposiciones de la normativa que regula los derechos de propiedad intelectual en los contratos realizados con terceros para desarrollo de softw are de manera que consten que los derechos de autor serán de la entidad contratante y el contratista entregará el código fuente para actualización y mantenimiento?		X				! 2,67	Contrato catastro
8	¿Los derechos de autor del softw are desarrollado a la medida fueron registrados en el organismo competente como de propiedad de la entidad conforme la normativa que regula los derechos de propiedad intelectual? En el caso de softw are adquirido se obtendrá las respectivas licencias de uso.	X					✗ 1,33	Ninguna
9	Los derechos de autor del softw are desarrollado a la medida pertenecerán a la entidad y serán registrados en el organismo competente,	X					✗ 1,33	Ninguna
10	¿La implementación de softw are adquirido incluiye los procedimientos de configuración, aceptación y prueba personalizados e implantados considerando la validación contra los términos contractuales, la arquitectura de información de la organización, las aplicaciones existentes, la interoperabilidad con las aplicaciones existentes y los sistemas de bases de datos, la eficiencia en el desempeño del sistema, la documentación y los manuales de usuario, integración y planes de prueba del sistema?		X				! 2,67	Manuales de usuario y sistemas
11	¿Se realizarán pruebas, conforme a un plan de pruebas y de control de calidad aprobado, en un ambiente específico y distinto del ambiente de producción. Se deben establecer los criterios de aceptación para concluir el proceso de prueba previo la liberación de la versión pertinente?	X					✗ 1,33	Ninguna
12	¿Se formaliza con actas de aceptación por parte de los usuarios, del paso de los sistemas probados y aprobados desde el ambiente de desarrollo/prueba al de producción?		X				! 2,67	Actas de reuniones
13	¿Se realizará una fase de estabilización y revisión de conformidades para retroalimentar el ciclo de vida del softw are?	X					✗ 1,33	Ninguna
14	¿Se lleva control de las versiones del softw are liberado y la biblioteca de respaldo con las versiones retiradas?	X					✗ 1,33	Ninguna
15	¿Se elaboraron manuales técnicos informáticos, de instalación y configuración, así como de usuario y fueron difundidos, publicados y actualizados de forma permanente?		X				! 2,67	Manuales de usuario y sistemas

Entidad: GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTON ESMERALDAS

Area o rubro evaluado: Evaluación Integral del Sistema de Control Interno Institucional

Período : 2023 - 2024 — DEL 4 de febrero de 2024 AL 5 de abril de 2024

Adquisiciones de infraestructura tecnológica — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	Total % factor	**410-09**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**32,50**	Acciones Tomadas por la Entidad
	2,5	5,0	7,5	10,0	12,5		
1 ¿La unidad de tecnologías de la información y comunicaciones define, justifica, implanta y actualiza la infraestructura tecnológica de la organización?		X				5,00	Politicas de Seguridad sin aprobacion
2 ¿Las adquisiciones tecnológicas están alineadas a los objetivos de la institución, principios de calidad de servicio, portafolios de proyectos y servicios, están basadas en los estándares vigentes para el sector público y constan en el plan anual de contrataciones aprobado por la institución?		X				5,00	Informe de gestion
3 ¿Las adquisiciones tecnológicas, incluidas las de consultoría y de servicios de procesamiento, soporte y/o almacenamiento prestados por terceros, estàn debidamente justificadas, documentadas y respaldadas por la planificación de su capacidad, el análisis de costo/beneficio, la previsión de su vida útil y la evaluación de riesgos pertinentes?	X					2,50	Actas de entrega, contrato catastrol
4 ¿Tienen los contratos de adquisición de hardw are el detalle suficiente que permita establecer las características técnicas de los principales componentes tales como: marca, modelo, número de serie, capacidades, interfaces, softw are instalado, entre otros?			X			7,50	Politicas de Seguridad revisadas
5 ¿Se evalúa que los bienes adquiridos respondan a las especificaciones técnicas y requerimientos establecidos en todas las fases precontractuales y contractuales, y que se encuentre confirmado en las respectivas actas de entrega/recepción?		X				5,00	Ninguna
6 ¿Los contratos con proveedores de servicio incluyen las especificaciones formales sobre acuerdos de nivel de servicio, puntualizando explícitamente los aspectos relacionados con la seguridad, propiedad y confidencialidad de la información?	X					2,50	Ninguna
7 ¿Se toman las previsiones necesarias en caso de alguna contingencia o salida del mercado del proveedor en las contrataciones de servicios externos en los que el proveedor realice el procesamiento o almacenamiento de la información en la "nube", mediante el análisis de riesgos y de costo/beneficio para ser aprobado por la máxima autoridad?	X					2,50	Ninguna
8 ¿En las bajas de equipamiento y/o residuos de aparatos tecnológicos, así como la finalización de contratos de servicios externos de procesamiento y/o almacenamiento de la información se considera el respaldo previo al borrado seguro de la información almacenada, así como la normativa ambiental de gestión de residuos aplicable?	X					2,50	Ninguna

Mantenimiento, actualización y control de la infraestructura tecnológica — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	Total % factor	**410-10**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**33,33**	Acciones Tomadas por la Entidad
	2,2	4,4	6,7	8,9	11,1		
1 ¿La unidad de TIC definió y reguló los procedimientos que garantizan el mantenimiento y uso adecuado de la infraestructura tecnológica?			X			6,67	Seguimiento de Plan de mantenimiento preventivo
2 ¿Se registró, evaluó y autorizó los cambios de procedimientos, procesos, sistemas y acuerdos de servicios previo a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción?	X					2,22	Ninguna
3 Los cambios que se realicen en procedimientos, procesos, sistemas y acuerdos de servicios son registrados, evaluados, autorizados e informados de forma previa a su implantación a fin de disminuir los riesgos de integridad del ambiente de producción, de manera que exista un detalle e información de estas modificaciones en su correspondiente bitácora adjuntando las respectivas evidencias.	X					2,22	Ninguna
4 ¿Se mantuvo un control y registro de las versiones del softw are que ingresa a producción?	X					2,22	Ninguna
5 ¿La unidad de tecnología de información actualizo, publicò y difundiò los manuales técnicos y de usuario por cada cambio o mantenimiento que se realice a los sistemas informáticos?	X					2,22	Ninguna
6 ¿La entidad mantiene ambientes de desarrollo/pruebas y de producción independientes, en los cuales se verifican medidas y mecanismos lógicos y físicos de seguridad para proteger los recursos y garantizar su integridad y disponibilidad a fin de proporcionar una infraestructura de tecnología de información confiable y segura?	X					2,22	Ninguna
7 ¿La unidad de tecnología de información elaboró e implmentó formalmente el plan de mantenimiento preventivo y/o correctivo de la infraestructura tecnológica sustentado en revisiones periódicas y monitoreo en función de las necesidades organizacionales (principalmente en las aplicaciones críticas de la organización), estrategias de actualización de hardw are y softw are, riesgos, evaluación de vulnerabilidades y requerimientos de seguridad		X				4,44	Plan de mantenimiento, informe de seguimiento
8 ¿La unidad de tecnología de información mantiene un control de los activos informáticos a través de un inventario actualizado con el detalle de las características y responsables a cargo, conciliado con los registros contables?		X				4,44	Inventario de activos informáticos
9 ¿El mantenimiento de los bienes relacionados con la infraestructura tecnológica, que se encuentran en garantía fueron proporcionados por el proveedor, sin que represente un costo adicional para la entidad?			X			6,67	Reporte de garantias y control de bienes

Seguridad de tecnología de información — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	Total % factor	**410-11**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**37,14**	Acciones Tomadas por la Entidad
	2,9	5,7	8,6	11,4	14,3		
1 ¿La unidad de TIC garantiza el cumplimiento de la normativa de protección de datos personales?		X				5,71	Se ha designado un responsable
2 ¿La unidad de TIC garantiza el cumplimiento de la normativa de propiedad intelectual del softw are?	X					2,86	Ninguna
3 ¿La unidad de TIC cumple de la normativa de seguridad de la información?		X				5,71	Plan de seguridad sin aprobar
4 ¿Se utilizan estándares acordes a los principios de calidad de servicio y a los objetivos de la organización?	X					2,86	Ninguna
5 ¿La utilizacion de sistemas o plataformas establecidas para el sector público están alineadas a los objetivos de la organización?			X			8,57	Plataforma AME
6 ¿Se ha implementado una política de seguridad de la información sobre la base de las disposiciones legales y reglamentarias vigentes?		X				5,71	Politica de seguridad sin aprobar
7 ¿La implementacion de infraestructura para seguridad de tecnología de información consta en el plan informático y en el plan anual de contrataciones aprobado de la institución?		X				5,71	POA 2024

Plan de contingencias — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	Total % factor	**410-12**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**22,50**	Acciones Tomadas por la Entidad
	2,5	5,0	7,5	10,0	12,5		
1 ¿La Unidad de Tecnología de Información definió, aprobó e implementó formalmente un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado?		X				5,00	Se ha designado un responsable
2 ¿La unidad de tecnología de información dispone de un plan de respuesta a los riesgos que incluye la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento?	X					2,50	Ninguna
3 ¿La unidad de tecnología de información definió y ejecutó procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización?	X					2,50	Plan de seguridad sin aprobar
4 ¿La unidad de tecnología de información desarrolló e implmentó formalmente un plan de continuidad de las operaciones que contemple la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un Data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos?	X					2,50	Ninguna
5 ¿La unidad de tecnología de información diseño e implmentó formalmente un plan de recuperación de desastres que contenga las actividades previas al desastre (bitácora de operaciones), las actividades durante el desastre (plan de emergencias, entrenamiento) y las actividades después del desastre?	X					2,50	Ninguna
6 ¿Existe un comité designado con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia?	X					2,50	Ninguna
7 ¿El plan de contingencias de la entidad ha sido categorizado como un documento de carácter confidencial que describe los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información?	X					2,50	Ninguna
8 ¿El plan de contingencias aprobado es difundido entre el personal responsable de su ejecución y ha sido sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento.?	X					2,50	POA 2024

Entidad: GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTON ESMERALDAS

Area o rubro evaluado: Evaluación Integral del Sistema de Control Interno Institucional

Período : 2023 - 2024 — DEL 4 de febrero de 2024 AL 5 de abril de 2024

Administración de soporte de tecnología de información — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-13**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**33,85**	Acciones Tomadas por la Entidad
	1,5	3,1	4,6	6,2	7,7		
1 ¿La Unidad de Tecnología de Información definió, aprobó y difundió procedimientos de operación que faciliten una adecuada administración del soporte tecnológico y garanticen la seguridad, integridad, confiabilidad y disponibilidad de los recursos y datos, tanto como la oportunidad de los servicios tecnológicos que se ofrecen?		X				! 3,08	Manual de procesos
2 ¿Se realizan revisiones periódicas para determinar si la capacidad y desempeño actual y futuro de los recursos tecnológicos son suficientes para cubrir los niveles de servicio acordados con los usuarios?	X					✗ 1,54	Ninguna
3 ¿El acceso a los sistemas informáticos de la entidad se realiza bajo el otorgamiento de una identificación única a todos los usuarios internos, externos y temporales que interactúen con los sistemas y servicios de tecnología de información de la entidad?		X				! 3,08	Control de usuarios
4 ¿Existen estandares técnicos legalizados que avalen y operativicen la identificación, autenticación y autorización de los usuarios, así como la administración de las cuentas?		X				! 3,08	Control de usuarios
5 ¿Se realizan revisiones regulares de todas las cuentas de usuarios y los privilegios asociados a cargo de los dueños de los procesos y administradores de los sistemas de tecnología de información?	X					✗ 1,54	Ninguna
6 ¿Existen medidas de prevención, detección y corrección debidamente legalizados que apoyen en la protección a los sistemas de información y a la tecnología de la organización de softw are malicioso y virus informáticos?	X					✗ 1,54	Ninguna
7 ¿La unidad de de Tecnología de Información definió legalmente los niveles de servicio y operación para todos los procesos críticos de tecnología de información, sobre la base de requerimientos de los usuarios o clientes internos y externos de la entidad y de las capacidades tecnológicas?	X					✗ 1,54	Ninguna
8 ¿Se definieron los procesos clave de tecnología de información, en base de los requerimientos y prioridades de la organización sustentados en la revisión, monitoreo y notificación de la efectividad y cumplimiento de dichos acuerdos?	X					✗ 1,54	Ninguna
9 ¿La entidad mantiene mecanismos efectivos y oportunos, como mesas de ayuda o de servicios, que permitan administrar incidentes reportados, requerimientos de servicio, solicitudes de información o cambios que demandan los usuarios?			X			✓ 4,62	Mesa de ayuda de TI
10 ¿La entidad ha implementado mecanismos, de preferencia electrónicos o a través de aplicativos informáticos, que permita a los usuarios conocer el estado de los trámites administrativos que mantienen con la entidad?			X			✓ 4,62	Sistema de hoja de ruta
11 ¿La unidad de tecnología de información mantiene un repositorio de diagramas y configuraciones de hardw are y softw are actualizado que garantice su integridad, disponibilidad y faciliten una rápida resolución de los problemas de producción?	X					✗ 1,54	Ninguna
12 ¿La unidad de de Tecnología de Información cuenta con una administración adecuada de la información, librerías de softw are, respaldos y recuperación de datos			X			✓ 4,62	Servidor de respados
13 ¿La entidad ha Incorporado mecanismos de seguridad aplicables a la recepción, procesamiento, almacenamiento físico y entrega de información y de mensajes sensitivos, así como la protección y conservación de información utilizada para encriptación y autenticación?	X					✗ 1,54	Ninguna

Monitoreo y evaluación de los procesos y servicios — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-14**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**24,00**	Acciones Tomadas por la Entidad
	4,0	8,0	12,0	16,0	20,0		
1 ¿La entidad dispone de una metodología legalmente establecida que permita monitorear la contribución y el impacto de las acciones realizadas por la unidad de tecnología de información?	X					✗ 4,00	Ninguna
2 ¿La Unidad de Tecnología de Información definió sobre la base de las actividades y operaciones de la entidad, indicadores de desempeño y métricas de los procesos que permitan monitorear la gestión y tomar los correctivos que se requieran?	X					✗ 4,00	Ninguna
3 ¿La Unidad de Tecnología de Información definió y ejecutó formalmente los procedimientos, mecanismos y la periodicidad para la medición, análisis y mejora del nivel de satisfacción de los clientes internos y externos por los servicios tecnológicos recibidos?	X					✗ 4,00	Ninguna
4 ¿La Unidad de Tecnología de Información presentó informes periódicos de gestión a las máximas autoridades, para que ésta supervise el cumplimiento de los objetivos institucionales planteados y se identifiquen e implanten acciones correctivas y de mejoramiento del desempeño?		X				✓ 8,00	Inofrme de gestiòn
5 ¿Las acciones correctivas que se han planteado por las autoridades de la entidad para el mejoramiento de la gestión de tecnologías, han sido ejecutadas por la unidad de tecnología de información?	X					✗ 4,00	Ninguna

Portal web, servicios telemáticos e intranet — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-15**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**65,00**	Acciones Tomadas por la Entidad
	5,0	10,0	15,0	20,0	25,0		
1 ¿La unidad de tecnología de información dispone de normas, procedimientos e instructivos de los servicios de internet, intranet, correo electrónico y sitio w eb de la entidad?			X			! 15,00	Instructivo de servicios w eb, Manual de uso del corre electrònico.
2 ¿Los esquemas normativos han sido desarrollados de conformidad con las disposiciones legales y considerando los requerimientos de los usuarios externos e internos		X				✗ 10,00	Informe tècnico
3 ¿La unidad de tecnología desarrolló aplicaciones w eb y/o móviles que automaticen los procesos o trámites orientados al uso de instituciones y ciudadanos en general.				X		✓ 20,00	Sistema de hora de ruta Portal ciudadano
4 La unidad de TIC mantiene aplicaciones w eb y/o móviles operativas o en funcionamiento?				X		✓ 20,00	Munidigital, Intranet, Portal ciudadano.

Capacitación relacionada a las TIC — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-16**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**35,00**	Acciones Tomadas por la Entidad
	5,0	10,0	15,0	20,0	25,0		
1 ¿La entidad cuenta con un plan de capacitación que contemple la capacitación especializada del personal de tecnología de información			X			✓ 15,00	Capacitaciones de la CGE en temas TIC
2 ¿La entidad cuenta con un plan de capacitación relacionada a las TIC que contemple la capacitación de todo el personal que utiliza aplicaciones tecnológicas, los servicios y sistemas de información para la ejecución de los procesos institucionales?	X					✗ 5,00	Ninguna
3 ¿El plan de capacitación relacionada a las TIC fue desarrollado en coordinación con la unidad de talento humano identificando y documentanado las necesidades de capacitación de todo el personal?	X					✗ 5,00	Ninguna
4 ¿El plan de capacitación contiene temas, contenidos, actividades y eventos de capacitación relacionados con las responsabilidades, funciones o actividades que deben cumplir los servidores de acuerdo a su cargo y que están determinadas en su evalaución de desempeño?		X				! 10,00	Plan de capacitacion

Firmas electrónicas — Estado del factor =>	Incipiente	Básico	Confiable	Muy confiable	Optimo	**Total % factor**	**410-17**
No. / Preguntas de evaluaciòn y diagnòstico	1	2	3	4	5	**64,00**	Acciones Tomadas por la Entidad
	4,0	8,0	12,0	16,0	20,0		
1 ¿La entidad ajustó los procedimientos y operaciones internas e incorporó los medios técnicos necesarios para permitir el uso de la firma electrónica de conformidad con la Ley de comercio Electrónico, Firmas y Mensajes de Datos?					X	✓ 20,00	Instalacionde firma EC, Reglamento Compras
2 ¿La unidad de tecnología capacitó a los servidores de la entidad respecto de las medidas de seguridad, condiciones, alcances, limitaciones y responsabilidades que deben observar en el uso de la firma electrónica?			X			! 12,00	Soporte en sitio y virtual
3 ¿Los aplicativos desarrollados o implementados por la unidad de tecnología, que incluyen firma electrónica, disponen de mecanismos y reportes que faciliten una auditoría de los mensajes firmados electrónicamente?		X				✗ 8,00	Intranet
4 ¿Los servidores de la entidad que disponen de firma electrónica, verifican mediante procesos automatizados de validación que el certificado de firma electrónica de las comunicaciones recibidas sea emitido por una entidad de certificación acreditada y que se encuentre vigente?				X		! 16,00	Firma .EC
5 ¿La unidad de tecnología dispone de procedimientos que permitan respaldar y almacenar bajo su responsabilidad en su estado original, los archivos electrónicos o mensajes de datos firmados electrónicamente, a través de medios electrónicos seguros?		X				✗ 8,00	Carpetas compratidas

ANEXO G

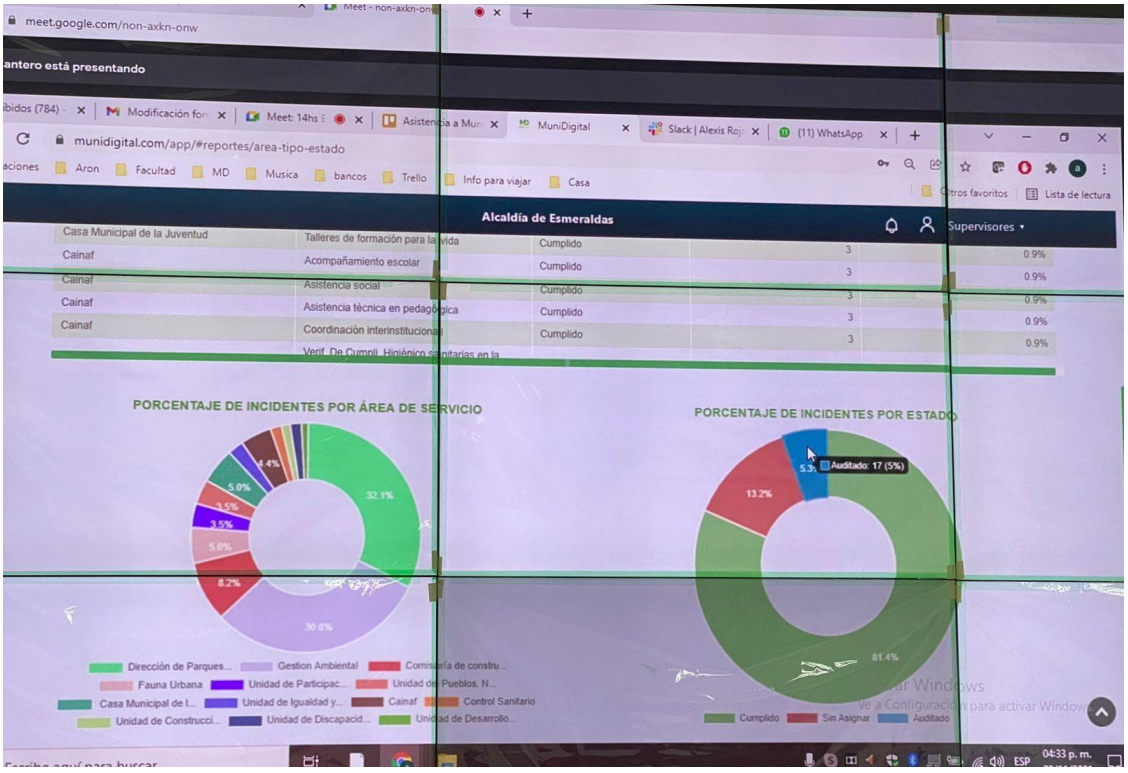
Evidencia fotográfica de la infraestructura tecnológica del GADMCE

Datacenter Portable

Poste de videogilancia / wifi / sensores

CCTV Sala de control y monitoreo de la ciudad

Centro de Operación y control de la ciudad



Sistema de registro de incidencias

ANEXO H

Carta de pedido para autorización de la investigación

06. 3442
23-10-2023 HORA 11:33

Esmeraldas 20 de octubre del 2023

Abogado
Vicko Alfredo Villacis Tenorio
ALCALDE DEL CANTON ESMERALDAS
Presente.

De mi consideración,

Yo, David Leonardo Rodriguez Portes, con C.I. # 0802079772, estudiante de la MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA de la UNIVERSIDAD TÉCNICA DEL NORTE, en cumplimiento de los principios bioéticos que orientan cualquier investigación (beneficencia, precaución, responsabilidad), que involucre grupos humanos y sus saberes; solicito a usted en calidad de Máxima Autoridad la autorización para poder realizar el Trabajo de Titulación con el tema:

"EVALUACIÓN DE LA SEGURIDAD DE TECNOLOGÍA DE INFORMACIÓN DEL GAD MUNICIPAL DE ESMERALDAS BASADO EN LAS NORMAS DE CONTROL INTERNO."

El producto final de esta investigación será entregado a la institución como un aporte académico, y será costeado de manera personal en su totalidad.

Por la atención a la presente, antelo mi agradecimiento, no sin antes desearle éxitos en sus funciones.

Atentamente,

Ing. David Leonardo Rodriguez Portes
ESTUDIANTE UTN
C.I. 0802079772

ANEXO I

Acta de Compromiso – Seguimiento a recomendaciones

Nº	Código de la Recomendación	Funcionario responsable del tratamiento	Plazo de cumplimiento	Observación o comentario
1	410-01.01	Alcalde	Inmediato	
2	410-02.01	Alcalde	Inmediato	
3	410-03.01	Director de TIC	Inmediato	
4	410-03.02	Director de TTHH	Doce meses	
5	410-04.01	Director de TIC	Un mes	
6	410-04.01	Director de TIC	Un mes	
7	410-05.01	Alcalde	Un mes	
8	410-05.02	Director de TIC	Dos meses	
9	410-06.01	Director de TIC	Seis meses	
10	410-06.02	Jefe de Sistemas	Seis meses	
11	410-07.01	Director de TIC	Seis meses	
12	410-07.02	Administrador C.	Inmediato	
13	410-08.01	Jefe de Sistemas	Inmediato	
14	410-08.02	Director de TIC	Inmediato	
15	410-09.01	Director de TIC	Inmediato	
16	410-09.02	Jefe de Sistemas	Inmediato	
17	410-09.03	Especialista de soporte	Inmediato	
18	410-10.01	Jefe de Sistemas	Inmediato	
19	410-10.02	Director de TIC	Inmediato	
20	410-11.01	Director de TIC	Un mes	
21	410-11.02	Jefe de Sistemas	Inmediato	
22	410-12.01	Director de TIC	Dos meses	
23	410-12.02	Jefe de Sistemas	Dos meses	
24	410-13.01	Director de TIC	Dos meses	
25	410-13.02	Jefe de Sistemas	Inmediato	
26	410-13.01	Director de TIC	Doce meses	
27	410-14.01	Coordinador General	Seis meses	
28	410-14.01	Director de TIC	Dos meses	
29	410-14.01	Director de TIC	Inmediato	
30	410-15.01	Director de TIC	Dos meses	
31	410-15.01	Director de TIC	Seis meses	
32	410-16.01	Director de TIC	Inmediato	
33	410-16.01	Director de TIC	Un mes	
34	410-16.01	Director Financiero	Doce meses	
35	410-17.01	Director de TIC	Doce meses	
36	410-17.01	Director de TIC	Seis meses	

Esmeraldas, a los 14 días, del mes de junio de 2024, suscriben el acta:

Entregue conforme

Firmado electrónicamente por: DAVID LEONARDO RODRIGUEZ PORTES

Ing. David Rodríguez P.
Maestrante UTN

Recibí conforme

Firmado electrónicamente por: JOSE DAMIAN MEZA ANCHUNDIA

Ing. Damián Meza A.
Coordinador General GADMCE