Pontificia Universidad Católica del Ecuador | SEDE ESMERALDAS

Escuela de Sistemas de Información

TEMA DE INVESTIGACIÓN:

Evaluación de la seguridad física del centro de datos de la prefectura de Esmeraldas basado en la norma ISO 27005

AUTOR:

Oswaldo Edwin Toro Cabrera

LÍNEA DE INVESTIGACIÓN:

Gobierno y administración de tecnologías de la información

TRABAJO DE GRADO PRESENTADO PARA OPTAR POR EL TÍTULO DE:

Ingeniero en Sistemas y Computación

ASESOR:

Mgt. Xavier Quiñonez Ku

Esmeraldas, 2023

TRIBUNAL DE GRADUACIÓN

Titulo: Evaluación de la seguridad física del centro de datos de la prefectura de Esmeraldas basado en la norma ISO 27005

Autor: Oswaldo Edwin Toro Cabrera

Mgt. Xavier Quiñones Ku f._____

Asesor

Mgt. José Luis Carvajal f._____

Lector #1

Mgt. Jaime Sayago Heredia f._____

Lector #2

Mgt. Homero Velastegui f._____

Coordinador de carrera

AUTORÍA

Yo, **TORO CABRERA OSWALDO EDWIN**, declaro que el contenido de la tesis "**Evaluación de la seguridad física del centro de datos de la prefectura de Esmeraldas basado en la norma ISO 27005**" presentado como requisito previo, a la obtención del título de "**INGENIERO EN SISTEMAS Y COMPUTACIÓN**", es original, de mi autoría y responsabilidad.

En virtud, declaro que el contenido, resultados, efectos legales y académicos que se desprenden del trabajo de investigación propuesto son y serán de exclusiva responsabilidad académica y legal del autor y de la PUCESE.

_____

Oswaldo Toro Cabrera
0803477207

DEDICATORIA

La investigación es una herramienta importante para lograr adquirir nuevos conocimientos y encontrar soluciones a problemas que se presentan en diferentes áreas del campo profesional. La presente investigación es dedicada principalmente a Dios por ser mi guía incondicional en todo momento, a mis padres por haber sido el soporte afectivo que fortalecían mis emociones y responsabilidades.

Con mucho cariño dedico mi trabajo de pregrado a mis hijas y esposa que siempre me motivan en seguir adelante para cumplir con objetivos propuestos.

Oswaldo Toro.

AGRADECIMIENTO

El presente trabajo de fin de grado se llevó a cabo con mucha dedicación por parte del autor y su tutor Mgtr. Xavier Quiñonez Ku, que fue un guía en el proceso de investigación, motivando y generando buenas ideas para avanzar de forma eficaz.

Agradezco a todos los docentes que fueron participe del proceso de enseñanza- aprendizaje que se llevó a cabo en cada uno de los niveles y brindaron su apoyo profesional y humanitario en todo momento.

Agradezco a mi familia que fueron un pilar importante en el proceso educativo, por el apoyo emocional, su aliento y comprensión han sido un motor que permitió superar los desafíos presentados en el camino.

Gracias Dios por la fuerza y sabiduría brindada en este proceso profesional que es el inicio de muchos éxitos en la vida.

Oswaldo Toro.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

Resumen

Esta investigación se enfocó en una evaluación exhaustiva del riesgo asociado a los activos de información alojados en el centro de datos de la Prefectura de Esmeraldas, con el propósito de fortalecer la seguridad física mediante la implementación de controles basados en las directrices de la normativa ISO 27005. Para alcanzar este objetivo, se llevaron a cabo múltiples fases de análisis y evaluación. De este modo, se abarcó la identificación de activos críticos, el minucioso cálculo del nivel de riesgo y, finalmente, la formulación de objetivos específicos de control de seguridad de la información. Por consiguiente, la metodología empleada en esta investigación se sustentó en un proceso exhaustivo que involucró estas etapas esenciales: la identificación de activos críticos, la evaluación precisa del nivel de riesgo y la definición de objetivos de control concretos.

Por otra parte, los resultados obtenidos en este estudio arrojaron luz sobre las limitaciones que actualmente afectan al centro de datos en cuestión. Pues, estas limitaciones comprenden la carencia de un sistema de climatización redundante, la ubicación poco estratégica de las instalaciones, una infraestructura que se considera limitada en sus capacidades y, significativamente, una amenaza latente, teniendo un nivel de riesgo resultante calificado como "Moderado", con un total de 11 puntos en la escala cuantitativa utilizada para la evaluación.

En consecuencia, se ha llegado a la conclusión de que resulta imperativo abordar de manera efectiva las amenazas y vulnerabilidades identificadas para garantizar la continuidad de los servicios tecnológicos esenciales. Además, se sugiere que las autoridades de la Prefectura de Esmeraldas respalden y promuevan la implementación de los objetivos de control propuestos en este estudio, asegurando que estén en consonancia con los objetivos organizacionales y se integren de manera efectiva en la cultura institucional existente. También, se recomienda que la Coordinación de la Escuela de Sistemas de Información promueva la realización de investigaciones similares en otros centros de datos de relevancia en la región, permitiendo, mejorar la seguridad física en estos entornos críticos y, al mismo tiempo, fortalecer la resiliencia de las infraestructuras tecnológicas en toda la región.

***Palabras clave**:* evaluación, seguridad física, ISO 27005, centro de datos.

Abstract

This research focused on a comprehensive assessment of the risk associated with the information assets housed in the data center of the Prefecture of Esmeraldas, with the aim of strengthening physical security through the implementation of controls based on the guidelines of ISO 27005 standards. To achieve this objective, multiple phases of analysis and evaluation were conducted. Thus, it encompassed the identification of critical assets, a meticulous calculation of the risk level, and, finally, the formulation of specific objectives for information security control. Consequently, the methodology employed in this research was grounded in a thorough process that involved these essential stages: the identification of critical assets, the precise assessment of the risk level, and the definition of specific control objectives.

Furthermore, the results obtained in this study shed light on the limitations currently affecting the data center in question. These limitations include the lack of a redundant air conditioning system, the non-strategic location of the facilities, infrastructure considered limited in its capabilities, and significantly, a looming threat, resulting in a risk level classified as "Moderate," with a total of 11 points on the quantitative scale used for evaluation.

Therefore, it has been concluded that it is imperative to effectively address the identified threats and vulnerabilities to ensure the continuity of essential technological services. Moreover, it is recommended that the authorities of the Prefecture of Esmeraldas support and promote the implementation of the control objectives proposed in this study, ensuring they align with organizational goals and are effectively integrated into the existing institutional culture. It is also suggested that the Coordination of the School of Information Systems encourages the conduct of similar research in other relevant data centers in the region, allowing for the enhancement of physical security in these critical environments and, at the same time, strengthening the resilience of technological infrastructures throughout the region.

Keywords: *assessment, physical security, ISO 27005, data center.*

INTRODUCCIÓN

Presentación del tema de investigación

En pleno siglo XXI, no hay una organización, empresa o compañía que, de una u otra forma, no sea dependiente de las tecnologías para llevar a cabo sus procesos y objetivos, porque en la actualidad toda información generada o empleada es procesada, almacenada y transmitida, básicamente, en formato digital. En un mundo dominado por el desarrollo tecnológico, conectado a través de Internet desde cualquier lugar y mediante el uso de variados tipos de dispositivos electrónicos, la exposición a múltiples amenazas de sus sistemas informáticos es una constantemente preocupación de autoridades y empleados.

Uno de los principales riesgos a los que está expuesta la información digital es la vulnerabilidad a los llamados ataques informáticos, especialmente los vinculados a los activos de una organización o empresa. Cualquier ataque informático puede provocar la pérdida de disponibilidad, confidencialidad e integridad del contenido, lo que implicaría grandes y, a veces irrecuperables, pérdidas [1].

Durante el año 2021, por ejemplo, los expertos de Kaspersky descubrieron varias vulnerabilidades y, aunque se observó una tendencia a la baja en el número de ataques a las vulnerabilidades de Microsoft Office, las explotaciones para este paquete de software siguen siendo las más populares entre los ciberdelincuentes, siendo la forma más fácil de comprometer los sistemas de usuarios vulnerables [2]. También a fines de ese año, se observó una vulnerabilidad activa en el motor MSHTML de Internet Explorer, frecuentemente explotada a través de un documento de Microsoft Office especialmente preparado con un control ActiveX malicioso incorporado para ejecutar código arbitrario en el sistema. De igual manera, Kaspersky detectó intentos de instalar malware de minería en las computadoras de 1,184,986 usuarios únicos, lo que representó el 2,19% de todos los ataques y el 16,88% de todos los programas del tipo Risktool [2]. Estos datos son una prueba innegable de la importancia de la seguridad informática.

A la par con el desarrollo de las ciencias informáticas, también se han ido actualizando muchos conceptos; es por eso por lo que actualmente se cuenta con un conjunto de definiciones que apoyan

y justifican el concepto de seguridad informática. Para esta investigación, se ha tomado la conceptualización dada por Roa [3], quien plantea que la seguridad física cubre todo lo referido a los equipos informáticos (computadoras de propósito general, servidores especializados y equipamiento de red), a diferencia de la seguridad lógica, que se refiere a las distintas aplicaciones que se ejecutan en cada uno de estos equipos. De forma particular, interesa la definición de la seguridad activa, la que se plantea como aquella que intenta protegernos de los ataques mediante la adopción de medidas que protejan los activos de la empresa.

Ante esta problemática mundial han surgido un conjunto de estándares y regulaciones relacionados con el tema de la seguridad informática y que constituyen normas certificables de gran aceptación a nivel internacional. De trascendental importancia para el presente estudio están las normas ISO, específicamente la serie de numeración 27000, estrechamente vinculantes con los sistemas de gestión de seguridad de la información. La primera numeración de esta serie ISO fue la 27001, que apareció en 2005, y es un estándar diseñado para la gestión de la seguridad de la información utilizable por cualquier tipo de organización o empresa, sea pública o privada. Para la adecuada gestión de la seguridad de la información, según la 27001, es necesario implantar un sistema que trate el tema de forma documentada y basada en objetivos precisos de seguridad, con una evaluación de los riesgos a los que está sometida la información de la organización o empresa. Es a partir de ella que se crea la ISO 27005, como guía para la gestión del riesgo de seguridad de la información.

Planteamiento del problema

El organigrama estructural por procesos del Gobierno Autónomo Descentralizado de la provincia de Esmeraldas (GADPE) cuenta con la Prefectura, que dentro de su estructura tiene el Departamento de Apoyo Técnico, oficialmente designado como Tecnología de la Información y la Comunicación, y que abarca tres subprocesos: Aplicaciones y Sistemas, Soporte Técnico e Infraestructura Tecnológica, que son los directamente vinculados a los activos de información del Centro de Datos.

Técnicamente considerado dentro de los procesos de apoyo, la gestión Tecnología de la Información y la Comunicación tiene como misión la planificación, organización, ejecución y evaluación de los sistemas, servicios e infraestructura de tecnología de información y

comunicación que requieren las diferentes instancias del GADPE [4]. Y dentro de sus atribuciones y responsabilidades, son pertinentes para el presente estudio las siguientes:

- Elaborar planes operativos de tecnología de la información alineados con el plan estratégico informático y los objetivos estratégicos de la institución, incluyendo los portafolios de proyectos y de servicios, las estrategias de migración, los aspectos de contingencia, y consideraciones relacionadas con la incorporación de tecnologías vigentes.
- Definir, documentar y difundir las políticas, estándares y procedimientos que regulen las actividades relacionadas con tecnología de información y comunicaciones, considerando temas como: calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos, legalidad del software, etc.
- Establecer procedimientos de comunicación, difusión y coordinación entre las funciones de tecnología de información y las funciones propias de la organización.
- Incorporar controles, sistemas de aseguramiento de la calidad y de gestión de riesgos, al igual que directrices y estándares tecnológicos.
- Definir el modelo de información de la organización a fin de que se facilite la creación, uso y compartición de la misma; y se garantice su disponibilidad, integridad, exactitud y seguridad sobre la base de la definición e implantación de los procesos y procedimientos correspondientes.
- Regular los procesos de desarrollo y adquisición de software aplicativo con lineamientos, metodologías y procedimientos.
- Definir, justificar, implantar y actualizar la infraestructura tecnológica de la organización.

Como subproceso, el interés de la actual investigación se focaliza en la Infraestructura Tecnológica, y específicamente en las siguientes tareas y actividades bajo su responsabilidad:

- Administrar las redes de voz y datos con los que cuenta o a los que accede la institución en calidad de usuario de administrador.
- Crear, modificar, eliminar, activar, desactivar usuarios, perfiles, roles o cualquier parámetro necesario de configurar en servidores a cargo de la dirección.
- Mantener los puntos de acceso y el cableado estructurado, de tal manera que se garantice la operatividad de la red.
- Planificar y administrar la asignación de recursos para el desarrollo, mantenimiento y

operación de la red.

- Desarrollar políticas, estándares y normas de seguridad lógica y física para la protección de la red.
- Coordinar las actividades con el área de Infraestructura para mantener la operatividad de la red local y la comunicación eficiente entre los puntos de red.
- Mantener un plan de contingencia para recuperación y funcionamiento de los servidores y redes luego de un siniestro.
- Mantener actualizado el inventario de puntos de acceso y equipos de comunicación de la institución.
- Coordinar con los usuarios la implantación de nuevos servicios de red que respondan a las necesidades institucionales.
- Implantar soluciones informáticas eficientes y de calidad, que garanticen su correcto funcionamiento.
- Proponer y coordinar cambios para mejorar la explotación de la red con los sistemas y las aplicaciones.
- Administrar los usuarios y contraseñas, de los sistemas y aplicaciones, documentando las asignaciones y definiendo la respectiva política de seguridad [4].

Sin embargo, independientemente de lo planificado en las tareas y actividades del subproceso Infraestructura Tecnológica, nunca se ha hecho un estudio que evalúe los riesgos a sus activos de información del centro de datos, que se conoce están expuestos constantemente a potenciales acciones delictivas y el robo de la información, y así poder preservar la confidencialidad, disponibilidad e integridad de la información.

De igual forma, no se ha hecho en la Prefectura de Esmeraldas un estudio del Sistema Gestión de Seguridad de la Información a partir del estándar internacional ISO 27001, lo que facilitaría hacer un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información del GADPE. Y es por eso por lo que la norma ISO 27005 se convierte en el eje central para los fines investigativos que aquí se persiguen, ya que proporciona directrices, recomendaciones, lineamientos de métodos y técnicas de evaluación para la gestión de riesgos de seguridad de la información. Diseñada para ayudar a la implementación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos, la ISO 27005 es

perfectamente aplicable al Data Center de la Prefectura objeto de estudio.

Es por ese análisis realizado que surge la siguiente pregunta científica: ¿Cómo mejorar la seguridad física a través de los controles detallados en la normativa ISO 27005?

Justificación

La Prefectura de Esmeraldas, específicamente su Centro de Datos, por sus sistemas, requiere imperiosamente que se desarrolle una evaluación de los riesgos a sus activos informáticos, potencialmente expuestos a riesgos y vulnerabilidades constantemente, y con ellos poder fortalecer sus procesos, protocolos, políticas y lineamientos de seguridad. El primer impacto se producirá al concientizar a los empleados sobre el manejo de la información sensible que tiene la Prefectura.

Para muchos organismos y empresas el principal problema que enfrentan es la falta de cultura sobre la importancia de la seguridad de su información y a lo que eso conllevaría. Muchas veces no se visualiza el riesgo propio y que lo ven como algo que le ocurre a otras empresas u organismos. [5], por ejemplo, se refiere al Informe sobre las Amenazas para la Seguridad en Internet, que en su informe de 2018 reflejó que era más probable que los empleados de pequeñas organizaciones o empresas se vieran afectados por amenazas de correo electrónico, incluidos el spam, el phishing y el malware de correo electrónico que los de las grandes organizaciones. También se reportó que los grupos de ataque se centraron en el uso de archivos adjuntos de correo electrónico maliciosos como un vector de infección primario.

Es por eso por lo que la seguridad física a través de controles detallados en la normativa ISO 27005 producirá un impacto de buenas prácticas de seguridad de la información, al conllevar al resguardo y protección de los principios de disponibilidad, integridad y confidencialidad de los activos de información, no solo para la prefectura, sino también para sus colaboradores y clientes vinculados.

La novedad se apreciará en que el GADPE podrá brindar más seguridad a todas las entidades vinculadas y ofrecer nuevos servicios de valor agregado, por la evaluación del riesgo desarrollado al gestionar la seguridad de la información, una herramienta de crecimiento que le otorgue un valor agregado ante sus clientes y el mercado.

La prioridad del estudio se da desde la perspectiva de que, con base en las consecuencias negativas

de robo de la información que podría tener el Centro de Datos del GADPE, al hacer una evaluación de riesgos de seguridad de la información bajo la norma ISO 27005, se podrán proponer objetivos de control de seguridad de la información para dicho Data Center.

OBJETIVOS

Objetivo general:

Evaluar el nivel de riesgo de los activos de información del centro de datos de la prefectura de Esmeraldas, para mejorar la seguridad física a través de los controles detallados en la normativa ISO 27005.

Objetivos específicos:

1) Identificar los activos de información del centro de datos críticos para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC.

2) Calcular el nivel de riesgo al que está expuesto el data center de la gestión de TIC del GADPE, en base a lo que refiere la normativa de certificación ISO 27005.

3) Proponer objetivos de control de seguridad de la información para el centro de datos, basado en la normativa ISO 27005.

CAPÍTULO I:

MARCO TEÓRICO

1.1 Bases teórico- científicas

1.1.1 Centros de datos

Un centro de datos (Data Center, en inglés) es definido como el lugar donde se concentran los servidores y equipos de comunicación [6]. Según la norma ANSI/TIA-942 [7], para el diseño de un Centro de Datos hay que considerar cuatro aspectos:

1. En su arquitectura, el diseño debe basarse en la seguridad, en su ubicación física dentro de un edificio, con accesos lógicos y seguros y ajustarse a las especificaciones de la norma particular para ese centro de datos.

2. El sistema eléctrico, en cuanto a la energía, la energía de reserva y la puesta a tierra deben cumplir todas las normas de protección establecidas, considerando PDU dedicados y paneles de energía alimentada por UPS. Se establece que la cantidad de circuitos eléctricos debe depender de los requisitos de los equipos que se ubicarán en los locales. Las salas deben tener sistemas de respaldo (UPS eléctricos y generadores), utilizados para la sala de computadoras, y el grado de redundancia para sistemas mecánicos y eléctricos tiene que ser la misma en todo el centro de datos.

3. El sistema de climatización, sea con unidades individuales o múltiples de aire acondicionado, debe constar con capacidad de refrigeración combinado para mantener la temperatura y la humedad relativa en condiciones óptimas.

4. El aspecto de las telecomunicaciones, por la propia naturaleza de los centros de datos de consumir grandes cantidades de energía, que esencialmente se convierten en calor, hace que se considere seriamente la eficiencia del enfriamiento. El no existir una arquitectura única de gestión térmica eficiente para todas las instalaciones, por la diversidad de elementos a tener en cuenta, hace que los factores físicos y el medio ambiente deben ser cuidadosamente evaluados en el análisis de puesta en marcha, junto con el análisis operativo.

Pero, paralelamente a esos cuatro aspectos, todo centro de datos deberá contar con sistema de monitoreo y control estandarizado en todas sus áreas, para precautelar ataques maliciosos, accidentes, y garantizar que todas las áreas sean seguras para el trabajo de sus obreros [6].

1.1.2 Riesgos de seguridad de la información

Solo mediante la implementación de un conjunto adecuado de controles, que incluya políticas, procesos, procedimientos, estructuras organizacionales (de software y hardware), se podrá garantizar la seguridad de la información. "Estos controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplen los objetivos de seguridad y de negocios específicos de la organización" [8] (p.4). La ISO/IEC 27001 tiene una visión integral y coordinada de los riesgos de seguridad de la información.

La seguridad de la información es una actividad que exige una alta responsabilidad por la mucha información que siempre se debe proteger y por existir muchos puntos o puertas a través de las cuales se pueden producir intrusiones; es decir, hablar de seguridad es referirse a la práctica orientada hacia la eliminación de cualquier vulnerabilidad, de forma tal que se eviten o reduzcan las posibilidades que las amenazas potenciales se concreten. Es por eso que se recomienda, en primer lugar, identificar los activos a proteger, y entre los que destacan los equipos, los datos, comunicaciones y las aplicaciones con que se cuenta. Es por eso que en su libro "Seguridad Informática", Roa [3] sugiere un grupo de buenas prácticas, y en ellas recomienda la revisión de la política de copias de seguridad (qué se copia, cuándo se hace, dónde se ha copiado, dónde se guarda de forma, cómo se comprueba que la copia se ha hecho bien y cuándo se hace una prueba de recuperación de una copia).

Es a su vez importante el revisar sistemáticamente los planes ante catástrofes, incluyendo todas las posibilidades, desde un ataque intencionado o desastre natural, hasta un arranque parcial de los servicios.

Otra buena práctica para la seguridad de la información es el no instalar algo que no sea completamente necesario, revisando la configuración de los sistemas y las aplicaciones, porque se pudieran otorgar más permisos de los estrictamente imprescindibles [3].

De igual forma, es necesario actualizarse constantemente sobre todos los informes de seguridad que surjan, registrándose en listas de correo sobre seguridad y en las listas de los proveedores de la empresa u organismo, ya sean de hardware o de software, de forma tal que se puedan recibir sus noticias directamente [3].

Las aplicaciones instaladas deben tener activados los mecanismos de actualización automática; hay que lograr que los clientes usen la seguridad y la visualicen como una ayuda. Otro problema de seguridad se presenta cuando no se revisa sistemáticamente la lista de los usuarios activos en una institución. Se han detectado riesgos en la seguridad informática cuando hay trabajadores que ya no pertenecen a la empresa, pero se le mantienen todos los privilegios asociados a él o a alguien de su confianza.

Muchas y variadas han sido las publicaciones sobre los riesgos de la seguridad de la información; por ejemplo, la normativa ISO/IEC 27002:2009, que trata sobre la gestión de la seguridad de la información, fue adaptada al contexto ecuatoriano, tal y como se plantea por [8]: "Para el propósito de esta Norma Técnica Ecuatoriana, se ha hecho el siguiente cambio editorial:

a) Las palabras "esta Norma Internacional" ha sido reemplazada por "esta norma nacional" (p. i). En ella se propone implantar controles para afrontar los riesgos inherentes a los sistemas informáticos. Esos controles incluyen políticas, estructura de la organización, así como procedimientos. Los controles, según esa norma ISO se aplican a todas las partes involucradas, desde la gestión de activos hasta la seguridad sobre los recursos humanos (antes, durante y después de pertenecer a la empresa), pasando por la seguridad física y ambiental, la gestión de las comunicaciones y operaciones y el control de acceso.

1.1.3 Criterios de la seguridad (disponibilidad, confidencialidad, integridad)

La imperiosa necesidad de implementar buenas prácticas de seguridad de la información tiene como objetivo principal orientarse hacia el resguardo de tres principios básicos: la disponibilidad, la integridad y la confidencialidad de los activos de información para un organismo, empresa, sus clientes, proveedores, colaboradores u otras personas, empresas u organismos interesados.

El principio de la disponibilidad indica cuán disponible está la información, sea en un sistema o un servicio, para que la misma pueda ser consultada en cualquier momento. Para garantizar la disponibilidad de la información hay varios métodos o vías disponibles. Los más frecuentes se dan en la redundancia de sistemas, la realización de copias de seguridad del sistema, una mayor recuperabilidad de dicho sistema; el mantenimiento de los equipos y sistemas operativos; el mantener software actualizados y la existencia de planes para recuperarse rápidamente de desastres no planificados [9].

Por su parte, el principio de integridad está estrechamente relacionado con el concepto de la completitud del dato; es decir, que el dato se conserve como es al principio, con su estructura e información, sin afectarse por el momento en que sea consultado.

Para garantizar esa integridad, se pueden utilizar métodos como las comprobaciones de consistencia de los datos y los controles de acceso, la función hash o las comprobaciones de validación de datos [10].

El tercer principio dentro de los criterios de la seguridad es el de la confidencialidad, cuyo concepto se relaciona con el término "privado", significando que el dato de información no puede o no debe ser compartido (o publicado) como algo del conocimiento de todos, independientemente de si se refiere a personas, organizaciones o empresas. Para darle cumplimiento a este principio, se pueden también utilizar determinados métodos para proteger o precautelar la información o los datos en sí mismos, tales como la autenticación, el control de acceso, el cifrado o encriptación [9].

Estos criterios de la seguridad de los datos o información han de ser la guía para concienciar a los trabajadores de las TIC para mitigar la materialización de riesgos asociados a la confidencialidad, integridad y disponibilidad de la información que se utiliza o maneja. La cultura que tengan los usuarios en su interacción con los activos que posee una organización o empresa debe llevar a alinear los objetivos institucionales para asegurar el flujo de información junto con la reducción de los factores de riesgo.

1.1.4 Vulnerabilidades de los activos

Vallejo [12] plantea que la ISO 27005 define a una vulnerabilidad como la debilidad del activo o

activos de las compañías, las cuales podrían ser usadas por las amenazas para causar daño a los sistemas. Roa [3] amplía el concepto al decir que una vulnerabilidad es un defecto de una aplicación que puede ser aprovechado por un atacante. Cuando un atacante descubre el defecto, programará un software (malware) que utiliza esa vulnerabilidad para tomar el control de la computadora o realizar operaciones no autorizadas. Según [3], las vulnerabilidades se dividen en tres tipos:

1.- Las ya reconocidas por el suministrador de la aplicación y para las que cuenta con un parche que las corrige.

2.- Las que, aunque conocidas por el suministrador, no cuentan aún con un parche.

3.- Las no reconocidas por el suministrador, que constituyen las más peligrosas porque el organismo o empresa puede estar expuesto a un ataque durante un tiempo largo sin que se sepa que está siendo atacado.

Debido al amplio uso de Internet, de manera programada, los programas se conectan con la web del suministrador y si hay actualizaciones automáticas, se aplican, introduciendo el parche a esa vulnerabilidad.

Los malware que atacan por las vulnerabilidades se clasifican en tres tipos:

- Los virus, cuya meta mayor es dejar inservible la computadora infectada.
- Los gusanos, que van afectando todos los recursos de la computadora (disco duro, memorias, red), y que se puede sospechar su presencia porque la persona nota que el sistema se va ralentizando progresivamente, hasta que no se puede trabajar en ella.
- Los troyanos, que habilitan puertas traseras en los equipos informáticos y que facilitan que desde otra PC se puedan ejecutar programas en la computadora infectada.

Todos esos malware tienen una meta común, y es su afán de replicación para contaminar el mayor número de computadoras posibles y así continuar la infección.

El Servicio Ecuatoriano de Normalización [8] reconoce que los activos están sujetos tanto a amenazas deliberadas como accidentales, mientras que los procesos relacionados, los sistemas, las

redes y las personas tienen vulnerabilidades inherentes. Por lo tanto, dada la cantidad y variedad de formas, esas amenazas pueden tomar ventajas de las vulnerabilidades para dañar a la empresa u organización. Sin embargo, una seguridad de la información eficaz va a eliminar o reducir los riesgos, protegiendo a la organización o empresa frente a las amenazas y vulnerabilidades, y de esa forma reducir el impacto en sus activos.

Toda la literatura sobre el tema enfatiza, por entorno de constantes amenazas de seguridad, es la automatización de los controles de seguridad informática, basadas en medidas a tomar para mitigar las vulnerabilidades, y entre las que se encuentran los inventarios de activos, el uso aceptable y propiedad de esos activos, y el etiquetado y manipulación de la información [12].

1.1.5 Amenazas de los activos

Sosa [13] definió las amenazas como cualquier hecho que puede producir un daño al ser capaz de violentar la seguridad de la información o la seguridad informática. La amenaza siempre estará presente cuando se haga presente una vulnerabilidad.

La norma ISO 27005 describe los diferentes tipos de amenazas, a partir de las cuales Vallejo [11], las resumió según su origen en la tabla que se muestra a continuación:

Tabla 1. Origen de las amenazas.

Amenaza	Descripción	Ejemplo
Natural	son fenómenos naturales que afectan a los activos	Terremoto
Humano	Es un fenómeno causado por el ser humano	Consumir líquido cerca de los equipos
Intencionado	Alteración de la información	Destrucción de la información
No intencionado	Ponen en riesgo los activos informáticos inconscientemente	Divulgar contraseñas

Fuente: Vallejo [11], basado la norma ISO 27005.

Enríquez e Hidalgo [14] aclaran que las amenazas no atacan directamente a los procesos o servicios, sino a los activos que los soportan, por lo que para su valoración es importante considerar ciertos factores que inciden directamente sobre estos, como son el costo original o de reemplazo y los costos de las posibles consecuencias debido a la pérdida de confidencialidad, integridad y disponibilidad, como resultado de un incidente. Sobre ese planteamiento, se tomaron en consideración las siguientes amenazas:

- Daño Físico: Fuego, Agua, Desastre Industrial.
- Desastres Naturales: Fenómeno Sísmico, Volcánico, Meteorológico, etc.
- Pérdida de Servicios Esenciales: Corte del suministro eléctrico, climatización, comunicaciones, etc.
- Compromiso de la Información: Fugas de información, Espionaje remoto, Hurto de medios o documentos, Recuperación de medios reciclados, etc.
- Fallas Técnicas: Avería de origen físico o lógico, Errores de mantenimiento, Caída del sistema por agotamiento de recursos, etc.
- Acciones no Autorizadas: Manipulación del software y equipos, Uso no previsto de equipos, Destrucción de información, etc.
- Compromiso de Funciones: Errores de los usuarios, Errores de configuración, Suplantación de la identidad del usuario, Abuso de privilegios de acceso, Ataque destructivo, Extorsión, etc. [14].

La mayoría de las amenazas pueden ser combatidas mediante la reducción de sus niveles de riesgo; pero eso requiere que se seleccionen controles y se generen políticas, y que faciliten que varias amenazas puedan resolverse aplicando el mismo control, aunque una amenaza específica puede requerir varios controles diferentes para su eliminación o mitigación.

1.1.6 Nivel de riesgo (probabilidad, impacto)

Una perspectiva acertada sobre qué es la probabilidad de un riesgo es verla cuando una amenaza intenta materializar una vulnerabilidad, que afecte la confidencialidad, la integridad o la disponibilidad de la información activo primario. Sosa [13] presenta una definición de escalas de las probabilidades, que se muestra en la siguiente tabla:

Tabla 1: Definición de probabilidad

No.	Nivel de probabilidad		Definición de la probabilidad	Nivel de ocurrencia
	Cualitativa	cuantitativa		
1	Alta	3	La fuente de amenaza es altamente motivada y suficientemente capaz. Los controles para prevenir que la vulnerabilidad suceda son ineficientes.	1- 5 veces al mes
2	Media	2	La fuente de la amenaza es motivada y capaz. Los controles pueden impedir el éxito de que la vulnerabilidad suceda.	1-3 veces al mes
3	Baja	1	La fuente de amenaza carece de motivación. Los controles están listos para prevenir o impedir significativamente que la vulnerabilidad suceda.	1 vez al mes

Fuente: Sosa [13].

El impacto no es más que una medición y valoración o análisis de los daños causados a la organización o empresa si un riesgo se llega a materializar, causando pérdidas materiales, económicas y de información [15].

Para valorar el impacto es necesario tomar en consideración tanto los daños tangibles como la estimación de los daños intangibles (que incluye la información).

Es imprescindible que todo organismo o empresa tenga, en su sistema de gestión de incidentes, el valor de los sistemas de información que pudieran ser afectados por incidentes de seguridad. Dentro de los valores para el sistema se pueden distinguir la confidencialidad de la información, la integridad (de aplicaciones e información) y la disponibilidad del sistema información y del sistema [16].

De acuerdo a la norma ecuatoriana ISO 27002, debido a la cantidad de formas en que las amenazas

podrían aprovecharse de las vulnerabilidades para dañar una organización, los riesgos de seguridad de la información siempre estarán presentes, y plantea que un sistema de seguridad de la información eficaz puede reducir esos riesgos, protegiendo a la organización frente a las amenazas y vulnerabilidades, y en consecuencia, se reduciría el impacto en sus activos [8].

1.1.7 Como se debe calcular el riesgo

Un aspecto central en el presente estudio es el calcular el nivel de riesgo al que está expuesto el data center de la gestión de TIC del GADPE, midiendo los niveles de riesgo según criterios expresados en la norma ISO/IEC 27005.

Varios han sido los autores que han realizado mediciones o evaluaciones de riesgos Informáticos. Corda, Viñas y Coria [17] comienzan por definir el riesgo informático como "aquella eventualidad que imposibilita el cumplimiento de un objetivo, es decir, todo aquel peligro o daño que puede afectar el funcionamiento directo o los resultados esperados de un sistema informático." (P.7). Y amplían su descripción al plantear que todo riesgo informático tiene una serie de componentes a considerar, entre los que se incluyen la seguridad física, el control de accesos, la protección de los datos y seguridad en las redes, la división de responsabilidades, la cuantificación de los riesgos, qué políticas hay establecidas hacia el personal, los aspectos legales y delitos, la función de los auditores internos y externos, la seguridad que tengan los sistemas operativos y de red y la creación de un plan de contingencia.

De forma similar, Montoya [18] define que "La gestión de riesgos es un método que abarca procesos de identificar, comprender, evaluar, eliminar riesgos basándose en sus vulnerabilidades, amenazas subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de esta para cumplir a cabalidad con sus operaciones." (P. 43), y que el proceso de gestión de riesgos se procede con el análisis de los riesgos respectivos, identificando y evaluando los activos, amenazas y vulnerabilidades, incluido en el Proceso Gestión de Riesgo de la ISO 27005. Fue a partir de ahí que [18] creó una matriz de riesgos de activos que se determinaron de acuerdo con la definición de criterios según la probabilidad (P) e impacto (I).

Enríquez e Hidalgo [14] declaran que el estándar ISO/IEC 27005 brinda una guía que permite identificar y estimar los riesgos, para mitigarlos a un nivel aceptable, utilizando un plan de

seguridad. Ese proceso de gestión de riesgos está especificado en la norma ISO 27001, utilizando el enfoque de manejo de riesgos [19], como se muestra en la Figura 1.

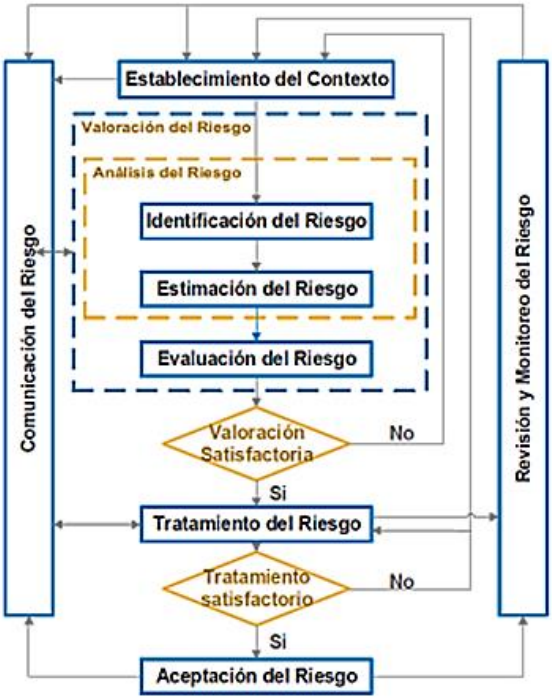

Figura 1: Proceso de gestión de riesgo [19].

Su metodología utiliza una valoración cualitativa con un equivalente cuantitativo, en una escala de 5 valores que van del 1 al 5 (1 - Muy Bajo, 2 - Bajo, 3 - Moderado, 4 - Alto y 5 - Muy Alto), lo que permite realizar cálculos matemáticos.

Un aspecto interesante es que los costos de consecuencias están definidos para cada requerimiento de seguridad (confidencialidad, integridad y disponibilidad), y que los delimita de la siguiente manera: "Pérdida de reputación y confianza del cliente (Rep), Pérdida de ventaja competitiva (VCo), Violación asociada a la información privada, (IP), Violación del contrato de confidencialidad del cliente (CC), Violación de la ley y regulaciones (LR), Interrupción del servicio (IS), Interrupción de la administración y gestión (Adm) e Incumplimiento del contrato del cliente (CCl)." (p. 3).

Para Bohorquez [20], la evaluación del riesgo consta de dos actividades. En primer lugar, el análisis del Riesgo, que incluye la identificación y estimación del riesgo; y en segundo lugar, la evaluación del riesgo en sí mismo. Para completar ambas actividades, el investigador se propuso una metodología propia, enfocada en la valoración de activos, impactos y riesgos, basada en otras existentes, pero siempre dentro de las metodologías descritas en la norma ISO/IEC 27005.

Finalmente, la forma de calcular el riesgo de Vallejo [11], también basada en la ISO 27005, es no solo interesante, sino también con fuerte fundamento científico. En el ejemplo de matriz de riesgo que propone, se ilustra que la probabilidad de ocurrencia va de 0 – 4, y donde la ocurrencia y el impacto se califican con la escala Baja (B), Media (M), Alta (A) y la valoración del riesgo va en una escala de 0 – 8.

Tabla 2: Matriz de riesgo [11]

	Probabilidad (Ocurrencia)	Baja			Media			Alta		
	Valor (Impacto)	B	M	A	B	M	A	B	M	A
Valor (Cumplimiento) Escala: (0-4)	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8
Cumplimiento: Escala (0 = 0%), (1 = 25%), (2 = 50%), (3 = 75%), (4 =										
Ocurrencia: Escala Baja (B), Media (M), Alta (A)										
Impacto: Escala Baja (B), Media (M), Alta (A)										
Valoración Riesgo: Escala 0 - 8										
Criterios de Valoración del Riesgo: Valores mayores a 7 (7,8)										

1.2 Antecedentes

Tapiero y Suárez [21] desarrollaron un modelo de gestión de riesgos de la seguridad de la información, con base en el enfoque de gestión de riesgos de la norma técnica colombiana NTC-ISO/IEC 27005, la cual ofrece las pautas para implementar satisfactoriamente un modelo de seguridad en cualquier tipo de organización que quiera mitigar el riesgo en la seguridad de la información. Se realizó un análisis a la situación de las empresas estudiadas, para determinar su

estado en la gestión del riesgo en la seguridad de la información; se hizo una valoración de activos presentes en las empresas y se evaluaron los impactos que pueden llegar a tener. De igual forma, se determinaron cuáles pueden ser las vulnerabilidades en las empresas en cuanto a la seguridad de la información y se buscaron los métodos de evaluación, para poder disminuir los riesgos en cada uno de los hallazgos. Se definieron políticas de seguridad de la información que permiten reducir las vulnerabilidades y amenazas en esas entidades. Finalmente, se describen las recomendaciones que permiten definir estrategias en la gestión de riesgos de la seguridad de la información para crear planes de acción ajustados a la realidad.

Bruno [22] realizó un estudio con el objetivo de evaluar la Seguridad del Centro de Datos del Hospital de Apoyo II-2 Sullana, por medio de la identificación de las condiciones en las que se encuentra ese centro de datos y conocer sus vulnerabilidades, amenazas y nivel de riesgo de cada activo de TI. Fue una investigación no experimental, con corte transversal, propositiva, de innovación incremental, todo para reducir los niveles de riesgo que podría presentar. Se aplicó la NTP ISO/IEC 27005 para desarrollar dicha evaluación del riesgo de seguridad.

Arévalo y Montalvo [23] hicieron una investigación con el objetivo de mejorar la gestión de incidencias de los activos informáticos en una universidad de Trujillo, en Perú, a través del desarrollo de un sistema web y móvil. Dentro de los objetivos específicos se propusieron la reducción del tiempo en que se realiza el seguimiento y registro de atención de una incidencia del activo informático y la reducción del tiempo de reportes de los activos informáticos. Como población se escogió el área de TIC y como muestra la sub-área de Administración de Recursos Informáticos. Para la obtención de los datos, se utilizó una encuesta y como instrumento un cronómetro para determinar los tiempos del pre-test y del pos-test. Se concluyó que, en el tiempo promedio del registro de incidencias de los activos informáticos, con el sistema actual, se encontró una diferencia de 486.32 segundos y con la implementación del sistema propuesto 45.61 segundos. En el tiempo promedio en el seguimiento de los activos informáticos, con el sistema actual se encontró una diferencia de 336.69 segundos y con la implementación del sistema propuesto 32.51 segundos.

Enríquez e Hidalgo [14] fundamentaron su estudio en el hecho de que la gestión operativa de un centro de datos no siempre es suficiente para mantener su correcto funcionamiento, porque existen

riesgos de seguridad de la información que pueden provocar impactos negativos sobre los objetivos de una organización. El estudio tuvo como fin el desarrollo de una metodología para gestionar el riesgo como parte de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los lineamientos de la Norma ISO/IEC 27005. La metodología se enfocó en la valoración de activos, impactos y riesgos y en la aplicación de controles sobre los activos de información de un Data Center de gama alta.

Vallejo [11] centró su investigación en la elaboración de una propuesta de un sistema de gestión de seguridad de la información para el Centro de Datos de la empresa Leterago, del Ecuador S.A, utilizando las Normas ISO 27001 e ISO 27005, que permitieron identificar los riesgos existentes en los activos de información y la forma de mitigarlos. A partir de los controles que utilizan en la organización para evitar riesgos, se logró analizar las políticas de seguridad de la información y la propuesta de SGSI que permitiría a la organización disminuir los riegos a un nivel aceptable y por lo tanto poder proteger las actividades que son esenciales en el negocio.

Astudillo y Cabrera [24] plantean que es usual que las empresas o instituciones construyan sus centros de datos fundamentándose en normas de diseño de construcción, para alcanzar la certificación basándose en la disponibilidad de estos. Sin embargo, al tratar de implementar políticas de seguridad de la información, se evidencian los inconvenientes que no fueron tomados en cuenta en la construcción, afectando a la financiación del proceso. Se asevera que la forma eficaz de gestionar estas áreas es fundamental para lograr contrarrestar amenazas e incrementar controles. Es necesario que se cuente con políticas de seguridad de la información que garanticen la disponibilidad de los servicios que los sistemas consumen. Enfocados en eso, los autores exponen una propuesta de gestión de seguridad de la información, fundamentado en la generación de políticas en este aspecto, usando como referencia la norma ISO/IEC 27001:2013 para el Centro de Datos diseñado con el estándar ANSI/TIA-942, garantizando la confidencialidad, integridad y disponibilidad de la información.

Rojas [20] realizó su estudio en MASTER-SECURITY S.A., empresa que brinda servicios profesionales de seguridad con una de sus sucursales situada en el norte de la ciudad de Guayaquil. Su trabajo investigativo tuvo como finalidad realizar una auditoria informática para obtener el estado actual de los riesgos a que se expone la empresa, evaluar los niveles de cumplimientos según

el estándar ISO/IEC 27001 para corroborar si la entidad se encuentra apta a futura implementación de un SGS, además de medir los niveles de riesgo según los criterios expresados en la norma ISO/IEC 27005. La metodología pudo dar a conocer los activos, controles existentes y amenazas que presenta la empresa, para luego proceder a realizar el cálculo del nivel de riesgo para los activos y controles. Se concluye que la realización de la auditoria permitió que la empresa conozca los riesgos a los que se encuentra expuesto y su nivel actual de cumplimiento según la norma ISO/IEC 27001.

Chipantiza [25] realizó su investigación sobre el Centro de Datos del Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas (GADMCE), con la finalidad de detectar las debilidades y necesidades existentes; y en base a ello, formular una propuesta de mejora, a partir de la importancia de las crecientes amenazas existentes en el sector informático. [25] parte del criterio de que la detección temprana de amenazas o posibles riesgos minimiza los mismos; mientras que la pérdida de información almacenada podría ocasionar graves consecuencias en el funcionamiento del GADMCE, debido a la información delicada que se encuentra alojada en los servidores y sistemas de almacenamiento ubicado en el centro de datos. La información concerniente a la detección de las debilidades y riesgos existente en el Centro de Datos del GADMCE se obtuvo mediante la realización de entrevistas a profundidad al personal de mantenimiento técnico de Sistemas del GADMCE, en relación directa con la infraestructura, con el propósito de conocer cómo se administra el centro de datos, observando el mejoramiento continuo de la seguridad.

CAPÍTULO II

MATERIALES Y MÉTODOS

La Prefectura de Esmeraldas, ubicada en la ciudad capital de la provincia, tiene como misión promover el desarrollo y bienestar integral de todos los cantones, procurando la participación inclusiva de sus habitantes en los planes, programas y proyectos que se ejecutan en el territorio de manera eficiente, eficaz y con calidad, orientándolos hacia una gestión por resultados, consolidando con su liderazgo la transparencia en su accionar.

2.1 Tipo de estudio

Se realizó un estudio mixto (Cuan/ Cual), con enfoque descriptivo, que permitió evaluar el nivel de riesgo de los activos de información del centro de datos de la Prefectura de Esmeraldas, para mejorar la seguridad física a través de los controles detallados en la normativa ISO 27005.

La parte cuantitativa permitió contabilizar los activos de información del centro de datos de la Prefectura y calcular el nivel de riesgo al que está expuesto el data center de la gestión de TIC del GADPE, en base a lo que refiere la normativa de certificación ISO 27005. La parte cualitativa permitió analizar las variables "criterios de la seguridad" (confidencialidad, disponibilidad e integridad de los datos), "vulnerabilidades de los activos", "amenazas de los activos" y "nivel de riesgo", en base a la probabilidad e impacto.

2.2 Población y muestra

La población del estudio quedó conformada por los 12 trabajadores y el Director del Departamento de Gestión de las TIC de la Prefectura de Esmeraldas y el muestreo no probabilístico, dirigido, fue categorizado como muestra de expertos al quedar constituida por tres personas: los dos ingenieros en Sistemas que trabajan en el Data Center, que está a cargo del subproceso de Infraestructura Tecnológica y el Director del Departamento, al considerar que son las únicas personas que manejan el data center y son, por tanto, las personas que mejor información podían brindar acerca de los activos de información del centro de datos.

2.3 Definición conceptual y operacionalización de las variables

Las variables del estudio fueron conceptualizadas de la siguiente forma:

Activos de información: Según la norma ISO 27005, son definidos como activos primarios, cuya cuantificación se puede hacer a través de tres variables: confidencialidad, integridad y disponibilidad y que son necesarios para que una empresa u organización funcione y consiga los objetivos que se ha propuesto.

Servicios tecnológicos: Conjunto de servicios que Internet pone a disposición de los usuarios, entre los que se encuentran las consultas a páginas Web, el correo electrónico, la transferencia de ficheros (FTP), los chats y conversaciones.

Nivel de riesgo: Es el grado de exposición a la ocurrencia de una pérdida, con la probabilidad de que la amenaza se materialice utilizando vulnerabilidades existentes en un activo, generando pérdidas o daños en los activos que se encuentran relacionados, directa o indirectamente.

ISO 27005: Es la guía para la gestión del riesgo de seguridad de la información.

Seguridad de la información: Conjunto de métodos y herramientas destinados a proteger la información ante cualquier amenaza.

La operacionalización de variables se muestra en el Anexo A.

2.4 Métodos de investigación

Se utilizó una metodología de tratamiento de riesgos centrada en la norma ISO 27005, y que en forma de seis cláusulas establece el proceso que se debe seguir para analizar el nivel de riesgo, siendo esas fases las siguientes:

- Cláusula 7: Establecer el contexto.
- Cláusula 8: Evaluación del riesgo.
- Cláusula 9: Tratamiento del riesgo.
- Cláusula 10: Aceptar el riesgo.

- Cláusula 11: Comunicar el riesgo.

- Cláusula 12: Monitorizar y revisar el riesgo.

Teóricamente fue necesario utilizar el método analítico- sintético, que posibilitó analizar cada uno de los elementos que componen los activos de información primarios y se interrelacionan, para luego hacer la síntesis correspondiente y llegar a conclusiones sobre la vulnerabilidad, amenazas, confidencialidad, integridad y la disponibilidad de dichos activos. Fue a partir de ahí que se definieron los objetivos de control de seguridad de la información que se proponen para el centro de datos, basado en la normativa ISO 27005.

2.5 Técnicas e instrumentos

La primera técnica aplicada fue la observación individual, no participante en el Departamento de la Gestión de TIC de la Prefectura de Esmeraldas, y en la que se utilizó una Guía de Observación (instrumento, Anexo B) en la que se registraron las observaciones sobre los activos de información del centro de datos críticos para la continuidad de los servicios tecnológicos.

La segunda técnica utilizada fue la entrevista semiestructurada, cuya guía de 5 preguntas (instrumento, Anexo C) se aplicó a los dos ingenieros informáticos que trabajan en el subproceso de Infraestructura Tecnológica y al Director de la Unidad, y que habían sido seleccionados como la muestra del personal.

La tercera técnica que se utilizó fue el Estudio documental, utilizando como documentos primarios las Normativas de certificación ISO 27001 (que proporciona un amplio conjunto de directrices para la correcta realización de un análisis de riesgos) y la ISO 27005 (herramienta que permite identificar las amenazas a las que se encuentran expuestos todos los activos, estimar la frecuencia en la que se materializan esas amenazas y valora el impacto que supone que se materialice en una empresa u organización).

2.6 Análisis de datos

Para el análisis de los datos cuantitativos, se tabularon en Excel los activos de información del centro de datos de la Prefectura y se calculó el nivel de riesgo al que está expuesto el data center

de la gestión de TIC del GADPE, en base a lo que refiere la normativa de certificación ISO 27005. Esos datos fueron llevados a tablas y figuras con sus frecuencias relativas.

Los datos obtenidos en las entrevistas y en el estudio documental se redactaron en forma de texto narrativo en Microsoft Word, y donde se plantean los objetivos de control de seguridad de la información para el centro de datos, basado en la normativa aplicada.

CAPÍTULO III

RESULTADOS

3.1 OBJETIVO 1

Los resultados de la observación durante la inspección y visita al data center permitieron identificar los activos de información del centro de datos críticos para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC del GADPE. Aunque se visualiza que hay una intención hacia un proceso de mejoramiento de sus prácticas y de sus procesos con respecto a lo que conlleva el uso y el almacenamiento de la información, tienen deficiencias pues el data center tiene limitaciones y problemas que se convierten vulnerabilidades, al no contar con un sistema de climatización redundante. Este aspecto hay que tomarlo bien en cuenta porque en caso de falla del sistema de climatización, los equipos pueden presentar fallas por la elevada temperatura que pueden llegar alcanzar; el data center está ubicado en un lugar poco estratégico dentro del edificio, es de dimensiones pequeñas y de infraestructura media, teniendo en cuenta el alcance y la cantidad de información que maneja el GADPE en estos momentos y las que puede llegar a manejar a futuro. Estos aspectos ubican la disponibilidad de la información en un nivel de vulnerabilidad alto.

Sin embargo, se pudo observar que tanto la confidencialidad como la integridad de la información están en un nivel de vulnerabilidad bajo porque se han tomado medidas y se han creado procesos para que la información se encuentre segura y bien resguardada dentro de su data center.

Una amenaza latente es la ocurrencia de sismos, como desastre natural más relevante. Al ser Esmeraldas una provincia que registra eventos sísmicos de considerables magnitudes y frecuencias, la estructura del departamento TIC ha sido afectada en más de una ocasión, lo que se convierte en un riesgo latente, especialmente para el data center, que está ubicado en la segunda planta alta del edificio. En este sentido, el sistema de climatización también se convierte en amenaza, al no ser redundante, lo que lo hace un problema crítico pues cuando hay sismos se producen fallas eléctricas que afectan la red, comprometiendo el funcionamiento del equipo vigente. Otra amenaza radica en la imposibilidad actual de desarrollar nuevos servicios, por lo señalado sobre las dimensiones del data center.

Sobre la implementación y operación de los controles, procesos y procedimientos, fue posible observar que están en procesos de mejora y de implementación de planes, y para mejorar los controles y sus activos, en apego a las buenas prácticas del manejo, almacenamiento y uso de la información en la entidad y quiénes hacen uso de la información. Por ello han reformado su Plan de Contingencia y han establecido procesos y procedimientos para la mejora y el beneficio del Departamento y sus activos.

En el control del desempeño de los procesos contra la política y los objetivos de seguridad, en el data center tienen conformado un comité informático, el cual tiene como tarea evaluar los procesos existentes y futuros, a fin de verificar si están encaminados a los objetivos y políticas existentes de la gestión de TIC.

Acerca del origen de las amenazas, desde el punto de vista de las naturales, queda claro que las sísmicas son las que se visualizan, pues la provincia ha sufrido varios de esos eventos. Las amenazas técnicas se observan por el sistema de climatización no redundante, los que los deja expuestos por posibles fallas o retrasos en el mantenimiento o reparación del único con el que se cuenta. Desde el punto de vista humano, no se aprecian amenazas, ya que existen criterios y políticas bien establecidos y que se cumplen para el ingreso y la seguridad del data center, como son los casos de la restricción del ingreso a personas no autorizadas y la supervisión y vigilancia cuando se realizan trabajos dentro del data center.

Como fuente de vulnerabilidades, en el ambiente físico se plantea, como problema principal, la ubicación del data center en un pasillo principal de la segunda planta alta del edificio y sus pequeñas dimensiones, lo cual sería un impedimento para futuros proyectos de implementación de nuevos equipos para sus procesos. No se detecta como fuente de vulnerabilidad aspectos claves como el Plan de tratamiento de riesgo, el registro de ingreso al centro, o los sistemas con los que cuentan ya que tienen un sistema de seguridad de acceso, con una puerta de seguridad, el uso del biométrico y video vigilancia; también tienen sistema contra incendios y, aunque con las falencias señaladas, cuentan con un sistema de climatización.

Los resultados de las entrevistas, realizadas a dos ingenieros encargados del data center (identificados aquí como I1 e I2) y al Director de la Gestión TIC (de aquí en lo adelante DG), con

el objetivo de verificar las percepciones de la muestra de estudio acerca de los activos de información para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC, se obtuvo la siguiente información:

Sobre cuál es el equipamiento del centro de datos y si alguna vez han tenido inconvenientes o problemas en el funcionamiento de los equipos, según I1, el data center del GADPE está cercano a entrar en la categoría Tier 2, pues tiene PDU tablero eléctrico, sistema de seguridad y vigilancia, cuenta con piso falso y cielorraso, sistema de climatización, sistema de contraincendios, 2 ups, sistema de luminarias emergentes, 3 rack donde se encuentran los servidores y el firewall; además, dispone de un servidor principal y uno espejo, además de un servidor NAS. Con el sistema de climatización tuvieron un problema provocado por una intermitencia eléctrica y el equipo se apagó y no volvió a encenderse de forma automática y tuvo que ser reiniciado de forma manual.

De acuerdo con I2, cuentan con un equipamiento acorde a sus necesidades actuales, además de que se enfocan en alinearse a lo que indican las normativas internacionales. El último evento sísmico que se vivió causó fisuras en las paredes del data center y es preocupante que se de otro evento de superior magnitud y pueda causar daños en los equipos.

El DG planteó que "*el data center con el que contamos se creó en el año 2012 y desde aquel entonces no ha sufrido cambios significativos; solo mantenimientos*", pero considera que faltan equipos para poder ofrecer más servicios y también prepararse para futuros requerimientos y necesidades del GADPE. Luego añadió que "*sufrimos un evento sísmico el que causó daños leves*" y uno de sus objetivos es la adquisición de un sistema de climatización redundante para mitigar esa vulnerabilidad.

La siguiente pregunta estuvo enfocada hacia la existencia de un Plan estratégico de Tecnologías de la Información y si hay un plan operativo acorde a eso. I1 refirió que sí se cuenta con un plan estratégico, pero está siendo actualizado para una futura aprobación de cambios y actualizaciones que se proponen realizar en el mismo. Por su parte, I2 informó que cuentan con un Plan estratégico de Tecnologías "acorde a nuestra realidad de hoy", pero debe ser actualizado en base a los cambios o mejoras que se deben realizar a futuro. DG también aseguró la existencia del Plan, pero que es

vital que lo actualicen y mejoren para evolucionar, "*al igual que lo hacen nuestras necesidades y requerimientos*".

Sobre el tema de cómo consideran el ambiente físico para su apropiado funcionamiento y si se lleva algún registro de ingreso al centro de datos, I1 expresó que es apropiado, pues se tiene un buen equipamiento a excepción del sistema de climatización, que está por pasar a uno redundante, pero al ser una institución pública, hay que esperar a que el proceso de licitación sea aprobado para así adquirir el mismo. También afirma que sí se lleva un registro del ingreso, permitiéndose solo a los 3 funcionarios que están registrados en el biométrico. Cuando se hace necesario el ingreso de personal externo, se tienen establecidas la normas y procedimientos para el ingreso de dicho personal.

I2 considera que se tiene un data center bien equipado y con un funcionamiento óptimo. Considera fundamental el tener el registro de ingreso y políticas para restringir o supervisar el ingreso de personas externas y así se hace. El DG considera que la ubicación del data center no es la mejor y que, para acceder, la persona tiene que estar registrada en el biométrico o acceder con alguien que sí lo esté, lo cual creará un registro en el sistema y además será respaldado por lo que capte el sistema de video vigilancia con el que cuentan.

La penúltima pregunta de la entrevista solicitaba los procedimientos administrativos que se realizan respecto al centro de datos como controles preventivos, detectivos y correctivos. I1 solo hizo referencia a mantenimientos anuales; mientras I2 se refirió al control de los activos que tienen como proceso que realiza la administración para saber si algún equipo va a ser cambiado o dado de baja. Por su parte, DG se refirió a la gestión de mantenimientos anuales para evitar deterioros de la infraestructura tecnológica con la que cuentan.

La última pregunta realizada fue si cuentan con un plan particular para el tratamiento de riesgo para el centro de datos del GADPE, a lo que I1 y DG respondieron que tienen un plan de contingencia; I2 dio la misma respuesta, pero añadió "*que es analizado por el consejo informático a fin de realizarle mejoras*".

3.2 OBJETIVO 2

Tomando como punto de partida los resultados de la observación y las entrevistas, se procedió a calcular el nivel de riesgo al que está expuesto el data center de Gestión de TIC del GADPE, en base a lo que refiere la normativa de certificación ISO 27005. Con tal objetivo en mente, se seleccionó la guía (modificada para este objetivo) propuesta por Enríquez e Hidalgo [14], basada en la ISO 27005, y cuya metodología utiliza una valoración cualitativa con un equivalente cuantitativo. En el presente estudio, se ha utilizado una escala de 5 valores que van del 0 al 4 (0 - Muy Bajo, 1 - Bajo, 2 - Moderado, 3 - Alto y 4 - Muy Alto), lo que permite realizar cálculos matemáticos, y totalizar el peso del impacto. La Tabla 3 muestra las consideraciones teóricas que se tomaron en cuenta para la escala de valores:

Tabla 3: Consideraciones teóricas tomadas en cuenta para la escala de valores.

Escala de Valores		
Valor cualitativo	**Probabilidad de ocurrencia**	**Peso (cuantitativo)**
Muy alto (MA)	Amenaza que ya se ha materializado por las vulnerabilidades	4
Alto (A)	Muy posible que la amenaza se materialice por las vulnerabilidades	3
Moderado (M)	Hay probabilidad de que la amenaza se materialice por las vulnerabilidades	2
Bajo (B)	La probabilidad de que la amenaza se materialice por las vulnerabilidades es reducida	1
Muy bajo (MB)	No se visualiza que la amenaza se materialice por las vulnerabilidades	0

Para calcular el peso total del impacto por el nivel de riesgo, se utilizó la siguiente escala, teniendo en cuenta que se incluyeron 6 categorías en el análisis, por lo que la sumatoria final podría estar en una escala de 0 a 24:

Valor (cualitativo)	**Peso (cuantitativo)**
Muy alto:	20 – 24
Alto:	15 – 19
Moderado:	9 – 14
Bajo:	5 – 8
Muy bajo:	0 – 4

Figura 2: Impacto por niveles de riesgo

La Tabla 4 muestra el cálculo realizado sobre el nivel de riesgo. Las categorías incluidas fueron la seguridad física, el control de accesos, la protección de los datos y seguridad en las redes, las políticas establecidas hacia el personal, la seguridad de los sistemas operativos y de red y la creación de un plan de contingencia, siempre partiendo del identificar, comprender, evaluar los riesgos basados en sus vulnerabilidades y amenazas subyacentes.

Tabla 4: Cálculo realizado sobre el nivel de riesgo, según los resultados de las técnicas de investigación.

Categoría	**Amenaza y vulnerabilidad**	**Valor (cualitativo)**	**Peso (cuantitativo)**
Seguridad física	Sismos; sistema de climatización redundante; ubicación; dimensiones e infraestructura del data center; sistema contra incendios.	MA	4
Control de accesos	Ingreso a personas no autorizadas, biométrico, cámaras de vigilancia	B	1
Protección de los datos y seguridad en las redes	Información se encuentra segura y bien resguardada; un servidor principal y uno espejo; servidor NAS; firewall.	MB	0
Políticas establecidas	Para desarrollar nuevos servicios, mantenimientos sistemáticos, ingreso de personas al data center.	M	2
Seguridad de los sistemas operativos y de red	Fallas eléctricas, corte del suministro eléctrico, climatización, comprometiendo el funcionamiento de equipos	MA	4
Plan de contingencia	No existencia o desactualizado	MB	0
Peso total del impacto	-	M	11

De acuerdo al cálculo realizado, el nivel de riesgo del data center del GADPE, según el peso del impacto, se ubica en la categoría de Moderado.

Con toda la información recabada en el análisis y cálculo de riesgos, que mostraron las amenazas y vulnerabilidades que podrían afectar al data center del GADPE, tanto en la integridad y

disponibilidad como en la confidencialidad de los activos de información, no solo para la prefectura, sino también para sus colaboradores y clientes vinculados, se procedió a proponer objetivos de control de seguridad de la información para el centro de datos, basados en la normativa ISO 27005. Es conveniente aclarar que cuando se habla de objetivos de seguridad es importante diferenciar los dos tipos de objetivos que contempla un SGSI: los generales del sistema y los de control resultantes del proceso de análisis y valoración de riesgos. En la presente investigación el foco estuvo dirigido a los segundos, según el numeral 6.2 de la ISO 27001.

El Anexo A de la ISO 27001:2013 está compuesto por 114 controles de seguridad agrupados en 14 secciones. De ellas, según los riesgos encontrados, este estudio se basó en los siguientes:

- A.9: Control de Acceso: control del acceso tanto a la información como a aplicaciones u otro medio que contenga información.
- A.11: Seguridad física y ambiental: controles para garantizar factores externos, seguridad de equipos y medios que puedan comprometer la seguridad.
- A.12: Seguridad Operacional: controles relacionados con gestión de la protección de malware o vulnerabilidades.
- A.14: Adquisición, desarrollo y mantenimiento de Sistemas: controles que establecen los requisitos de seguridad en desarrollo y soporte.
- A.17: Aspectos de Seguridad de la Información de la Gestión de la Continuidad del Negocio: referidos a la planificación de continuidad de negocio.

3.3 OBJETIVO 3

Propuesta de objetivos de control de seguridad de la información para el centro de datos del GADPE

Objetivo 1: Crear planes para el tratamiento de riesgos ante la ocurrencia de sismos para garantizar la seguridad de equipos y medios (A.11).

Objetivo 2: Asegurar la integridad y continuidad de los servicios por medio de un sistema de climatización redundante y un sistema contra incendios (A.11).

Objetivo 3: Gestionar proyectos de inversión que permitan la reubicación del data center en un local más amplio en la planta baja del edificio del GADPE (A.17).

Objetivo 4: Establecer, mediante su adquisición, un sistema de energía eléctrica con alimentadores independientes de otras cargas, que permita la seguridad de los sistemas operativos y de red ante fallas eléctricas o el corte del suministro eléctrico y que comprometen el funcionamiento de equipos (A.12).

Objetivo 5: Actualizar las políticas establecidas para poder desarrollar nuevos servicios y realizar mantenimientos sistemáticos a todos los equipos y sistemas del data center (A.14).

Objetivo 6: Generar el sentido de pertenencia y apropiación en temas de seguridad en los trabajadores de todo el GADPE, especialmente a los que laboran en las cámaras de vigilancia, para lograr la participación activa de todos en los controles de ingreso de personas al data center (A.9).

Los objetivos propuestos han de permitir el apoyo incondicional por parte de la máxima dirección del GADPE, la alineación de los objetivos de seguridad con los objetivos de la Prefectura y la compatibilidad de los controles con la cultura organizacional.

CAPÍTULO IV

DISCUSIÓN

Es un hecho confirmado que el data center del departamento de la Gestión de TIC del GADPE tiene limitaciones y problemas en sus activos de información para la continuidad de los servicios tecnológicos y que hacen que se conviertan en vulnerabilidades, al no contar con un sistema de climatización redundante y está ubicado en un lugar poco estratégico dentro del edificio; sus dimensiones son pequeñas y la infraestructura se considera media, teniendo en cuenta el alcance y la cantidad de información que maneja la Prefectura de Esmeraldas en estos momentos y, mucho más, las que puede llegar a manejar. Estos aspectos ubican la disponibilidad de la información en un nivel de vulnerabilidad alto. No se puede negar, sin embargo, que tanto la confidencialidad como la integridad de la información están en un nivel de vulnerabilidad bajo, por las medidas que se han tomado y por los procesos creados para que la información se encuentre segura y bien resguardada dentro de su data center.

En este sentido, la literatura refleja el estudio de Astudillo y Cabrera [24], quienes plantean que lo ideal es que las empresas o instituciones construyan sus centros de datos fundamentándose en normas de diseño de construcción, como forma eficaz de gestionar estas áreas para lograr contrarrestar amenazas e incrementar controles; y recomiendan la norma ISO/IEC 27001:2013 para garantizar la confidencialidad, integridad y disponibilidad de la información.

Una amenaza latente para el data center estudiado es la ocurrencia de sismos, por ser Esmeraldas una provincia que registra eventos sísmicos de considerables magnitudes y frecuencias. En este sentido, la estructura del departamento TIC ha sido afectada en más de una ocasión, y hay que tener en cuenta que el mismo está ubicado en la segunda planta del edificio. Cuando hay sismos (amenaza de origen natural), se tienden a producir fallas eléctricas que afectan la red y comprometen el funcionamiento de los equipos. En este sentido, el estudio de Enríquez e Hidalgo [14] coincide con la realidad encontrada en la presente investigación, ya que ellos aclaran que las amenazas no atacan directamente a los procesos o servicios, sino a los activos que los soportan, por lo que para su valoración es importante considerar ciertos factores que inciden directamente sobre estos, como son el costo original o de reemplazo y los costos de las posibles consecuencias

debido a la pérdida de confidencialidad, integridad y disponibilidad, como resultado de un incidente.

Tapiero y Suárez [21], al desarrollar su modelo de gestión de riesgos de la seguridad de la información alertan de la necesidad de definir estrategias al crear planes de acción ajustados a la realidad. Esa es una tarea pendiente en el GADPE con respecto a su data center. De igual manera, se hace válido el estudio de Enríquez e Hidalgo [14] y cuyas conclusiones amparan el estudio, al decir que se necesita una metodología para gestionar el riesgo como parte de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en los lineamientos de la Norma ISO/IEC 27005.

Otra amenaza radica en la imposibilidad actual de desarrollar nuevos servicios, por las limitadas dimensiones del data center, observación que se pudo verificar en las entrevistas realizadas y en las que se pudo conocer que faltan equipos para poder ofrecer más servicios y también prepararse para futuros requerimientos y necesidades del GADPE. La situación descrita demuestra una limitante importante para los planes de desarrollo futuros de la Prefectura de Esmeraldas. Y es que no basta con estar concentrándose en procesos de mejora y de implementación de planes, e incluso reformar su Plan de Contingencia si no cuentan con el local idóneo para realizar su trabajo con toda la calidad y alcance propios del desarrollo tecnológico y de trabajo del GADPE.

De los tres posibles orígenes de amenazas, es reconfortante saber que las del tipo humano son improbables, por la preparación científica de sus ingenieros y por tener criterios y políticas bien establecidos. Las de origen técnico se centran en el sistema de climatización no redundante, por lo que están expuestos a daños por posibles fallas o retrasos en el mantenimiento, como se materializó cuando hubo un problema provocado por una intermitencia eléctrica y el equipo se apagó y no se prendió de manera automática, por lo que hubo que reiniciarlo de forma manual. Sin lugar a duda, esa es una dificultad que se puede eliminar si se trabaja de forma intencionada y bien dirigida.

Pero sí es una fuerte amenaza las que tienen un origen natural, especialmente las sísmicas, por la ubicación geográfica de la provincia dentro del llamado Anillo o Cinturón de fuego del Pacífico, donde se registra casi toda la actividad sísmica a nivel mundial y lugar de ocurrencia de los sismos más grandes del planeta. A pesar de lo prácticamente imposible de predecir con exactitud, el GADPE ha de concebir las medidas que ayuden a minimizar los daños al data center ante la

ocurrencia de un evento sísmico de gran magnitud. Reforzando este planteamiento, se encuentra el resultado de Chipantiza [25], quien al estudiar el Centro de Datos del Gobierno Autónomo Descentralizado Municipal del Cantón Esmeraldas (GADMCE), analiza que la detección temprana de amenazas o posibles riesgos minimiza los mismos; mientras que la pérdida de información almacenada podría ocasionar graves consecuencias en el funcionamiento del GADMCE.

Otra dificultad detectada se presenta con el Plan Estratégico de Tecnologías, apropiado para la realidad actual, pero que no responde a los cambios o mejoras que se deben realizar a futuro. De forma similar, en esta esfera se valora como una falencia que los mantenimientos dentro del data center solo se hacen anualmente, básicamente por los costos económicos. Independientemente que hoy se valora como bien equipado y con un funcionamiento óptimo, a largo plazo puede convertirse en un gasto financiero mayor. Coincidiendo con el punto de vista aquí presentado, el Servicio Ecuatoriano de Normalización [8] establece que los controles se deben establecer, implementar, supervisar, revisar y mejorar, cuando sea necesario, para asegurar que se cumplen los objetivos de seguridad y de negocios específicos de la organización, algo que no está ocurriendo en el data center estudiado, con su mantenimiento anual.

Al calcular el nivel de riesgo al que está expuesto el data center de Gestión de TIC del GADPE, según el peso del impacto, se ubica en la categoría de Moderado desde el punto valorativo cualitativo, con 11 puntos en la escala cuantitativa. Aquí la mayor incidencia, catalogada de Muy Alta, fue "Amenaza que ya se ha materializado por las vulnerabilidades" (Seguridad física: sismos, sistema de climatización redundante, ubicación, dimensiones e infraestructura del data center, sistema contra incendios; y Seguridad de los sistemas operativos y de red: fallas eléctricas, corte del suministro eléctrico, climatización, comprometiendo el funcionamiento de equipos). La literatura apoya el estudio que se presenta, porque se ha dicho que es importante que toda empresa u organismo conozca los riesgos a los que se encuentra expuesto y su nivel actual de cumplimiento según la norma ISO/IEC 27001 [20]. Para Bohorquez [20], la valuación del riesgo consta de dos actividades. En primer lugar, el análisis del riesgo, que incluye la identificación y estimación del riesgo; y en segundo lugar, la evaluación del riesgo en sí mismo. Su metodología, enfocada en la valoración de activos, impactos y riesgos, como la nuestra aquí presentada, estuvo fundamentada en la norma ISO/IEC 27005.

También afecta negativamente el cálculo de riesgos, calificado de Moderado con peso cuantitativo de 2, las Políticas establecidas para desarrollar nuevos servicios, mantenimientos sistemáticos, e ingreso de personas al data center; y calificado de bajo, con peso cuantitativo de 1, el Control de accesos. De la misma manera se pronunciaron Astudillo y Cabrera [24], cuando concluyeron que es necesario que se cuente con políticas de seguridad de la información que garanticen la disponibilidad de los servicios que los sistemas consumen, y en eso se centraron para exponer una propuesta de gestión de seguridad de la información, fundamentado en la generación de políticas en este aspecto, usando como referencia la norma ISO/IEC 27001, tal y como se hizo en la actual investigación

Los seis objetivos de control de seguridad de la información que se han propuesto en este estudio para el centro de datos, basados en la normativa ISO 27005, se centraron en los conocidos como de control resultantes del proceso de análisis y valoración de riesgos, y focalizados en el numeral 6.2 de la ISO 27001. Esos objetivos han de ayudar a resolver las amenazas, vulnerabilidades y riesgos aquí analizados, de forma tal que se garantice permanentemente la disponibilidad, integridad y confidencialidad de los activos de información, no solo para la prefectura, sino también para sus colaboradores y clientes vinculados.

Son varios los estudios que han tenido como fin el ayudar al control de seguridad de la información de organismos y empresas. Así, por ejemplo, Tapiero y Suárez [21] desarrollaron un modelo de gestión de riesgos de la seguridad de la información, con base en el enfoque de gestión de riesgos de la norma técnica colombiana NTC- ISO/IEC 27005, la cual ofrece las pautas para implementar satisfactoriamente un modelo de seguridad en cualquier tipo de organización que quiera mitigar el riesgo en la seguridad de la información y definieron políticas de seguridad de la información que permiten reducir las vulnerabilidades y amenazas en esas entidades. De igual forma, Vallejo [11] centró su investigación en la elaboración de una propuesta de un sistema de gestión de seguridad de la información para el Centro de Datos de la empresa Leterago. A partir de los controles que utilizan en la organización para evitar riesgos, se logró analizar las políticas de seguridad de la información y la propuesta de SGSI que permitiría a la organización disminuir los riegos a un nivel aceptable y por lo tanto poder proteger las actividades que son esenciales en el negocio.

Los objetivos propuestos en el presente estudio deben recibir todo el apoyo necesario por parte de la máxima dirección del GADPE, la alineación de los objetivos de seguridad con los objetivos de la Prefectura y la compatibilidad de los controles con la cultura organizacional.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

La investigación que aquí se concluye buscó evaluar el nivel de riesgo de los activos de información del centro de datos de la prefectura de Esmeraldas, para mejorar la seguridad física a través de los controles detallados en la normativa ISO 27005. Con esa meta en mente, se identificaron los activos de información del centro de datos críticos para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC, se calculó el nivel de riesgo al que está expuesto el data center de la gestión de TIC del GADPE, en base a lo que refiere la normativa de certificación ISO 27005, para finalmente proponer objetivos de control de seguridad de la información para el centro de datos.

Se identificó que el data center del departamento de la Gestión de TIC del GADPE tiene limitaciones y problemas en sus activos de información para la continuidad de los servicios tecnológicos y que hacen que se conviertan en vulnerabilidades, al no contar con un sistema de climatización redundante y está ubicado en un lugar poco estratégico dentro del edificio, con dimensiones pequeñas y una infraestructura considerada media. La mayor amenaza para el data center es la ocurrencia de sismos, al estar Esmeraldas en el Anillo de Fuego del Pacífico, por lo que se registran eventos sísmicos de considerables magnitudes y frecuencias. Una vulnerabilidad importante es que el Plan Estratégico de Tecnologías no responde a los cambios o mejoras que se deben realizar a futuro. Estos aspectos ubican la disponibilidad de la información en un nivel de vulnerabilidad alto.

También se puede concluir que el nivel de riesgo al que está expuesto el data center de Gestión de TIC del GADPE, según el peso del impacto, se ubica en la categoría de Moderado desde el punto valorativo cualitativo, con 11 puntos en la escala cuantitativa, y donde tienen mayor incidencia las amenaza que ya se ha materializado por las vulnerabilidades, como los sismos, el sistema de climatización redundante, su ubicación dentro de la Prefectura, y la seguridad de los sistemas operativos y de red ante fallas eléctricas o el corte del suministro eléctrico, lo que compromete el funcionamiento de los equipos.

Los seis objetivos de control de seguridad de la información que se han propuesto en este estudio, basados en la normativa ISO 27005, han de ayudar a resolver las amenazas, vulnerabilidades y riesgos analizados, de forma tal que se garantice permanentemente la disponibilidad, integridad y confidencialidad de los activos de información, no solo para la prefectura, sino también para sus colaboradores y clientes vinculados.

5.2 Recomendaciones

A partir de los resultados encontrados y discutidos, que han llevado a las conclusiones antes mencionadas, se realizan las siguientes recomendaciones:

1.- A las autoridades del GADPE, apoyar el cumplimento de los objetivos propuestos en el presente estudio, alineándolos con los objetivos de trabajo de la Prefectura y la compatibilidad de los controles con la cultura organizacional.

2.- A la Coordinación de la Escuela de Sistemas de Información, que promueva entre sus estudiantes la realización de otras investigaciones sobre el mismo tema en otros centros de importancia vital para la ciudad y provincia de Esmeraldas, de forma tal que se contribuya al mejoramiento de la seguridad física de otros centros de datos.

REFERENCIAS BIBLIOGRÁFICAS

[1]	V. Rughoonauth, "CSI computer crime and security survey. Computer Security Issues & Trends". Computer Security Institute, 2005. Disponible en: https://www.academia.edu/1237543/CSI_computer_crime_and_security_survey
[2]	Global cloud service Kaspersky Security Network, "Kaspersky Security Bulletin 2021. Statistics", Kaspersky, 2021. Disponible en: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2021_eng.pdf
[3]	J. F. Roa Buendía, "Seguridad informática", Academia: Accelerating the World´s research. España: McGraw-Hill Interamericana de España, S.L, 2013. Disponible en: https://d1wqtxts1xzle7.cloudfront.net/34758985/Seguridad_Informatica_McGraw-Hill_2013_-_www.FreeLibros.me_-_copia-with-cover-page-v2.pdf?Expires=1658771365&Signature=EN2qyODkc6RdvegODWBYGVWg2YqkR9qldSducbs2tZQ-NVpHGDX5N8R1BOYXpz1cmTK8MiUCfKTIchIbSI5DrZI7tsdc7YWlGI1DC2bL8umSXUIxIWcYtTfXgtQz~8TFTIzt6RQKztRjsd4qMSxXUVQPQsb2XOccSdpsFvNBuRpbi32YbQeHOtOjgNLquWjhS9pc85vcVr6AeyReYFDZBjpczy56spFqYNnQLzZEmu4tU~~cpUwea~ctmGIqvtSI6RhARoHsqso9ehGqX62Kh5FiEv0f8nZyf~LY1KamWfIKLU1NjrQGiLKE9epBDoSDiZXGwJDaCV9YvsfBEghyWg__&Key-Pair-Id=APKAJLOHF5GGSLRBV4ZA
[4]	Prefectura de Esmeraldas, "Estatuto Orgánico de Gestión por Procesos", Resolución Administrativa N°2017-003- B, 2017. https://www.prefecturadeesmeraldas.gob.ec/web/assets/estructura-organica-de-gestion-por-proceso.pdf
[5]	Comparabien."Asobancaria2".[Internet].2019. https://comparabien.com.co/sponsor/asobancaria.(Accedido: 18- dic- 2021)
[6]	M.F. Molina-Miranda, "Análisis de Riesgos de Centro de Datos Basado en la Herramienta Pilar de Magerit". *Espirales revista multidisciplinaria de investigación, v*ol. 1, No. 11, Dic 2017. [En línea]. Disponible en: https://1library.co/document/y4g127vy-analisis-riesgos-centro-datos-basado-herramienta-pilar-magerit.html?utm_source=search_v3

[7]	Telecommunications Industry Association. “TIA -942”. TIA 942 Certifications & Ratings. https://tiaonline.org/products-and-services/tia942certification/tia-942-certifications-ratings/ (Accedido: 30- nov- 2021).
[8]	Servicio Ecuatoriano de Normalización. Norma Técnica Ecuatoriana. NTE INEN-ISO/IEC 27002. Segunda edición 2017-04. 2017. Disponible en: https://www.normalizacion.gob.ec/buzon/normas/nte_inen_iso_iec_27002.pdf
[9]	Fernández, J. (10 de 2013). Aprocal. Obtenido de Aprocal: http://www.aprocal.org.mx/files/2200/03SeguridadenInformaticaV1.0.pdf [Consulta: 27 de junio de 2018]
[10]	MinTic. (07 de 2016). Gobierno de Colombia - MinTic - Modelo de Seguridad y Privacidad de la Información. Obtenido de https://www.mintic.gov.co/gestionti/615/article5482_Modelo_de_Seguridad_ Privacidad.pdf
[11]	A. Vallejo Cáceres, “ Propuesta de sistema de gestión de seguridad de la información para el Centro De Datos de la empresa Leterago del Ecuador S.A”, Tesis de Grado, Sistemas Informáticos, Universidad Israel, Quito, 2018, 136p. Disponible en: http://repositorio.uisrael.edu.ec/handle/47000/1673
[12]	Y. Herrera Vive y L. García Membribes, “Sistema para el control de activos informáticos de la facultad 4”, Tesis de Grado, Universidad de las Ciencias Informáticas, Cuba,2014. Disponible en: https://repositorio.uci.cu
[13]	Sosa, J. (27 de 01 de 2012). Análisis de Riesgos . Obtenido de Análisis de Riesgos : http://pegasus.javeriana.edu.co/~CIS1130SD03/Documentos_files/Analisis_de_Riesgos.pdf [Consulta: 28 de julio de 2018]
[14]	V. Enríquez y P. Hidalgo, «Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama», Rev. Politéc. Nac., vol. 36, n.º 1, p. 45, sep. 2015. Quito, Ecuador. Disponible en: https://revistapolitecnica.epn.edu.ec/ojs2/index.php/revista_politecnica2/article/view/494
[15]	Vieites, Á. G. (2011). Enciclopedia de la Seguridad Informática. 2ª edición. Grupo Editorial RA-MA.

[16]	Fernández, J. (10 de 2013). Aprocal. Obtenido de Aprocal: http://www.aprocal.org.mx/files/2200/03SeguridadenInformaticaV1.0.pdf [Consulta: 27 de junio de 2018]
[17]	Corda, María Cecilia , & Viñas, Mariela , & Coria, Marcela Karina (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. Palabra Clave (La Plata), 7(1),1-18.[fecha de Consulta 8 de junio de 2022]. Disponible en: https://www.redalyc.org/articulo.oa?id=350553375007
[18]	Montoya, B. (2018). Implementación de un sistema de gestión de seguridad de la información para la seguridad lógica en base a las normativas ISO 27001 en la red del hospital de especialidades guayaquil Dr. Abel Gilbert Pontón, tesis de grado,. Disponible en: http://repositorio.ug.edu.ec/handle/redug/30466
[19]	Information technology - Security techniques - Information security risk management, ISO/IEC Estándar 27005, 2008.
[20]	B.J. Rojas Bohorquez, "Auditoria de seguridad de la información para la empresa Master-Security S.A. para determinar el nivel de cumplimiento de los controles definidos por la Norma ISO/IEC 27005", Facultad de Ciencias Matemáticas y Físicas, Universidad de Guayaquil, 2022. Disponible en: http://repositorio.ug.edu.ec/handle/redug/59681
[21]	H.A. Tapiero Tapiero, H. Suárez Ramírez, "Modelo de gestión de riesgos de la seguridad de la información en empresas del sector asegurador utilizando la norma ISO/IEC 27005", Tesis de Grado, Facultad Tecnológica, Universidad Distrital Francisco Jose De Caldas, Bogotá, Colombia, 2017. Disponible en: http://hdl.handle.net/11349/8322
[22]	E. O. Bruno Pizarro, "Evaluación de la seguridad del centro de datos del Hospital de Apoyo II-2 Sullana," Tesis de Grado, Escuela Académico Profesional De Ingeniería Informática Y De Sistemas, Facultad De Ingeniería, Universidad San Pedro, Piura – Perú, 2019. Disponible en: http://repositorio.usanpedro.pe/bitstream/handle/USANPEDRO/13655/Tesis_62544.pdf?sequence=1&isAllowed=y
[23]	P. F. Arévalo Rodríguez y L.C. Montalvo Martínez, "Sistema Web y Móvil para Mejorar la Gestión de Incidencias de los Activos Informáticos en una Universidad de Trujillo - 2019", Tesis de Grado, Escuela Académico Profesional de Ingeniería de Sistemas, Facultad de

	Ingeniería, Universidad César Vallejo, Perú, 2019. Disponible en: https://repositorio.ucv.edu.pe
[24]	C. Astudillo-García, A. Cabrera-Duffaut, "Políticas de gestión de seguridad de la información, fundamentadas en la norma ISO/IEC 27001", Centro de datos diseñado con el estándar ANSI/TIA 942". *Dominio de las Ciencias*, 5(3), 132-158, 2019. Manabí, Ecuador. doi: http://dx.doi.org/10.23857/dc.v5i3.929
[25]	G.R. Chipantiza Sifuente, "Análisis de riesgo tecnológico del centro de datos basado en normas internacionales: Caso GADMCE", Tesis de Grado, Escuela de Sistemas y Computación, Pontificia Universidad Católica del Ecuador, sede Esmeraldas, 2018. Disponible en: https://repositorio.pucese.edu.ec/handle/123456789/1476

ANEXOS

ANEXO A

OPERACIONALIZACIÓN DE VARIABLES

Objetivo	Variable	Definición	Dimensión	Indicador	Técnica/ Instrumento
1) Identificar los activos de información del centro de datos críticos para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC.	Activos de información	Son los activos primarios, necesarios para que una empresa u organización funcione y consiga los objetivos que se ha propuesto.	Confidencialidad Integridad Disponibilidad	- criterios de la seguridad - vulnerabilidades de los activos - amenazas de los activos	Observación / ficha de observación Estudio documental/ Normativas de certificación ISO 27001) y la ISO 27005
	Servicios tecnológicos	Conjunto de servicios que Internet pone a disposición de los usuarios.	Consultas a páginas Web, el correo electrónico, transferencia de ficheros (FTP), chats y conversaciones	- Planeación acorde con las políticas y objetivos globales de la prefectura - Implementación y operación de los controles, procesos y procedimientos - Medición del desempeño de los procesos contra la	Observación / ficha de observación Entrevista semiestructurada / Guía de preguntas

				política y los objetivos de seguridad	
Objetivo	**Variable**	**Definición**	**Dimensión**	**Indicador**	**Técnica/ Instrumento**
2) Calcular el nivel de riesgo al que está expuesto el data center de la gestión de TIC del GADPE, en	Nivel de riesgo	Es el grado de exposición a la ocurrencia de una pérdida, con la probabilidad de que la	Amenazas (físicas, lógicas o estratégicas)	De origen: - natural, - técnico, - humano accidental o intencional	Observación / ficha de observación

base a lo que refiere la normativa de certificación ISO 27005.		amenaza se materialice utilizando vulnerabilidades existentes en un activo, generando pérdidas o daños en los activos que se encuentran relacionados, directa o indirectamente.	Vulnerabilidades	- El ambiente físico - Plan de tratamiento de riesgo - Registro de ingreso al centro - Equipos en el centro de datos - Sistemas con los que cuentan	Entrevista semiestructurada / Guía de preguntas

Objetivo	**Variable**	**Definición**	**Dimensión**	**Indicador**	**Técnica/ Instrumento**

3) Proponer objetivos de control de seguridad de la información para el centro de datos, basado en la normativa ISO 27005.	Objetivos de control	Metas que surgen del análisis de cada uno de los elementos que componen los activos de información primarios y que permiten corregir y controlar las debilidades por vulnerabilidad o amenazas, asegurando la confidencialidad, integridad y la disponibilidad de los activos de información, amparándose en las normativas internacionales ISO 27001 e ISO 27005.	Controles preventivos, detectivos y correctivos en cuatro esferas: a) Estructuración de la unidad de sistemas b) Procedimientos administrativos c) Plan estratégico de Tecnologías de la Información d) Plan operativo	Existencia de: - malla de alta frecuencia - sistema de control de acceso - sistema de detección y extinción de incendio - sistema de video seguridad - servidores con garantías vigentes - Planes de capacitación del personal - Documentación técnica - Predicción de pérdidas por riesgos en términos de impacto	Estudio documental/ Normativas de certificación ISO 27001 e ISO 27005

ANEXO B

Guía de Observación

Objetivos:

- Identificar los activos de información del centro de datos críticos para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC.
- Calcular el nivel de riesgo al que está expuesto el data center de la gestión de TIC del GADPE, en base a lo que refiere la normativa de certificación ISO 27005.

Fecha y hora: _____

A) Activos de información (Confidencialidad, Integridad, Disponibilidad)

1) Cumplimiento de los criterios de la seguridad en los tres componentes

_____

_____

_____

2) Nivel de vulnerabilidades de los activos en los tres componentes

_____

_____

_____

3) Posibles amenazas de los activos en los tres componentes

_____

_____

_____

B) Servicios tecnológicos (Consultas a páginas Web, correo electrónico, transferencia de ficheros (FTP), chats y conversaciones)

4) Implementación y operación de los controles, procesos y procedimientos

_____

_____

_____

5) Control del desempeño de los procesos contra la política y los objetivos de seguridad

_____

_____

_____

C) Nivel de riesgo percibido (Amenazas físicas, lógicas o estratégicas y las vulnerabilidades relacionadas)

6) Origen de las amenazas (natural, técnico, humano)

_____

_____

_____

_____

_____

7) Fuente de las vulnerabilidades (El ambiente físico, Plan de tratamiento de riesgo, Registro de ingreso al centro, Equipos en el centro de datos, Sistemas con los que cuentan)

_____

_____

_____

_____

_____

ANEXO C

Entrevista semiestructurada

Guía de preguntas para los ingenieros informáticos que trabajan en el subproceso de Infraestructura Tecnológica y al Director de la Unidad

Objetivo:

- Verificar las percepciones de la muestra de estudio acerca de los activos de información para la continuidad de los servicios tecnológicos del departamento de la Gestión de TIC.

Preguntas:

1.- ¿Cuál es el equipamiento del centro de datos? ¿Alguna vez han tenido inconvenientes o problemas en el funcionamiento de los equipos? (de responder afirmativamente, preguntar: ¿Ha sido necesaria la contratación de terceros para solucionar el problema?)

2.- ¿Cuentan ustedes con un Plan estratégico de Tecnologías de la Información? ¿Hay un plan operativo acorde a eso?

3.- ¿Cómo considera usted que es el ambiente físico para su apropiado funcionamiento? ¿Se lleva algún registro de ingreso al centro de datos?

4.- ¿Qué procedimientos administrativos se realizan respecto al centro de datos? ¿Se incluyen controles preventivos, detectivos y correctivos?

5.- ¿Cuentan con plan particular para el tratamiento de riesgo para el centro de datos del GADPE?