UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMATICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador
Línea de Investigación:
Ciencias de la ingeniería aplicadas a la producción, sociedad y desarrollo sustentable
Campo amplio de conocimiento:
Tecnologías de la Información y la Comunicación (TIC)
Autor/a:
Camacho Tulcanazo René Alexander
Tutor/a:
PhD. Valverde Alulema Francisco Xavier

Quito – Ecuador

20224

APROBACIÓN DEL TUTOR

Yo, **Francisco Xavier Valverde Alulema** con C.I: 1712156684 en mi calidad de Tutor del proyecto de investigación titulado: *Evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador*.

Elaborado por: **René Alexander Camacho Tulcanazo**, de C.I **1711616233**, estudiante de la Maestría: Seguridad Informática de la **UNIVERSIDAD TECNOLÓGICA ISRAEL (UISRAEL)**, como parte de los requisitos sustanciales con fines de obtener el Título de Magister, me permito declarar que luego de haber orientado, analizado y revisado el trabajo de titulación, lo apruebo en todas sus partes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
FRANCISCO XAVIER VALVERDE ALULEMA

_____

Firma

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, René Alexander Camacho Tulcanazo con C.I: 1711616233, autor/a del proyecto de titulación denominado: **EVALUACIÓN DE NIVEL DE MADUREZ DE CUMPLIMIENTO DE POLÍTICAS EN SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN CENTROS DE DATOS DE INSTITUCIONES DE EDUCACIÓN SUPERIOR, BASADO EN LA NORMA ISO 27001, CASO DE ESTUDIO: UNIVERSIDAD CENTRAL DEL ECUADOR**. Previo a la obtención del título de Magister en Seguridad Informática.

1. Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar el respectivo trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Manifiesto mi voluntad de ceder a la Universidad Tecnológica Israel los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4, 5 y 6, en calidad de autor@ del trabajo de titulación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital como parte del acervo bibliográfico de la Universidad Tecnológica Israel.
3. Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de prosperidad intelectual vigentes.

Quito D.M., marzo de 2024

Firmado electrónicamente por:
RENE ALEXANDER CAMACHO TULCANAZO

_____

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

El estatuto de la Universidad Central del Ecuador (Universidad Central del Ecuador, 2019), indica entre sus artículos más relevantes que:

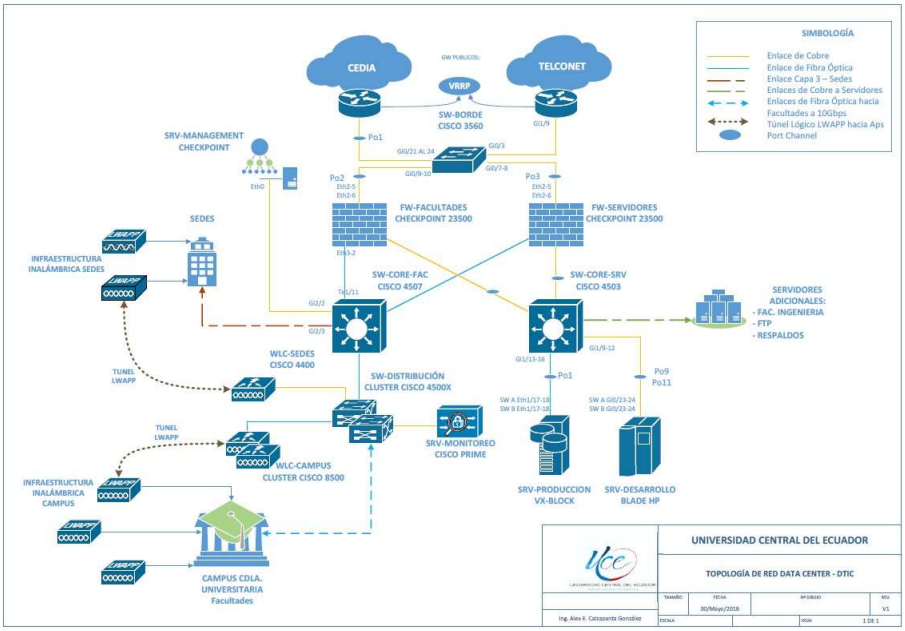
La Universidad Central del Ecuador, fundada el 18 de marzo de 1826, es una institución de educación superior ubicada en el centro norte de la ciudad de Quito, es una de las universidades más antiguas y prestigiosas del país y la región, con una larga historia de excelencia académica y compromiso con el desarrollo social y cultural del país. La academia propone una extensa gama de programas de pregrado y posgrado en diversas áreas del conocimiento a la sociedad ecuatoriana, incluyendo ciencias sociales, humanidades, ciencias exactas, ciencias de la salud, ingeniería, entre otras (Universidad Central del Ecuador, 2024).

La estructura orgánica de la Universidad Central del Ecuador descrita en su estatuto (Universidad Central del Ecuador, 2019, pág. 15), se caracteriza por la colaboración de diversos órganos que operan de manera conjunta para la gestión y administración eficaz de la institución. En este contexto, el Consejo Universitario se erige como el máximo órgano de gobierno, donde se adoptan decisiones de trascendencia para la comunidad universitaria. Este consejo despliega su labor en aras del beneficio colectivo y el progreso institucional.

El Rectorado, es el miembro ejecutivo responsable de la dirección y gestión general de la universidad. El Rector es la figura de máxima autoridad académica y administrativa, y es quien representa a la institución ante la comunidad universitaria y la sociedad ecuatoriana en general (Universidad Central del Ecuador, 2019, pág. 21). Junto con los Vicerrectorados Académico, Administrativo y de Investigación, Doctorados e Innovación, conforman las cabezas visibles que dirigen el rumbo de la institución educativa.

La institución presenta una estructura organizacional compuesta por varias direcciones administrativas (Universidad Central del Ecuador, 2019, pág. 52), abarcando aspectos en la parte académica, talento humano, investigación, vinculación con la sociedad y el área tecnológica. La Dirección de Tecnologías de la Información y Comunicaciones (DTIC) se encarga de gestionar estos aspectos técnicos y administrativos, regulando, planificando y administrando los recursos tecnológicos destinados al uso y la transferencia de información dentro de la comunidad universitaria. La infraestructura tecnológica, como se muestra en la figura 1, proporciona diversos servicios a las facultades de la universidad.

Figura 1.
Topología de red UCE



Nota: Dirección de Tecnologías de la Información y Comunicaciones DTIC - UCE

El Centro de Datos de la Universidad Central del Ecuador (CD-UCE) fue remodelado en el año 2015 con proceso de contratación No. SIE-UCE-0026-2015 (Sistema Oficial de Contratación Pública, 2015), al igual que muchas instituciones modernas, despliega una infraestructura tecnológica robusta para respaldar sus operaciones académicas, administrativas e investigativas. Como institución enfrenta un desafío significativo en cuanto a ciberseguridad, dada su extensa red y la atención a una comunidad de alrededor de 40,000 personas.

Pese de haber implementado medidas de seguridad como firewalls, sistemas de detección de intrusos y cifrado de datos, entre otros, estas no están adecuadamente dimensionadas para el tamaño de la institución. Se destaca la ausencia de políticas de seguridad y la escasa adopción de guías y procedimientos en este ámbito dentro de la academia. Esta situación dificulta la protección efectiva de los datos y sistemas del CD-UCE, dejándolos vulnerables a diversas amenazas cibernéticas (World Economic Forum, 2024).

Para abordar estos desafíos de manera efectiva, es de suma importancia que la Universidad Central del Ecuador establezca medidas de seguridad sólidas. Esto implica la implementación de estrategias como la actualización regular del software, la formación del personal en materia de seguridad, la vigilancia constante de la red y el establecimiento de políticas y procedimientos de seguridad rigurosos (EcuaCERT, 2024).

Problema de investigación

Con el crecimiento continuo del uso de Internet (Unión Internacional de Telecomunicaciones (UIT), 2024), la demanda de aplicaciones web que requieren una infraestructura tecnológica robusta está en constante aumento. Estas aplicaciones se apoyan en centros de datos distribuidos en diversas ubicaciones globales. En la actualidad, la gestión de estas aplicaciones se lleva a cabo a través de terminales conectadas al ciberespacio, como portátiles, computadoras personales y teléfonos móviles, lo que permite a los usuarios llevar a cabo diversas acciones en sus actividades diarias.

Para garantizar la eficiencia en la operación de cualquier negocio (Naciones Unidas, 2018), diversas organizaciones, incluida la Universidad Central del Ecuador, deben automatizar sus procesos. A pesar de ello, aún persisten ciertas fases y registros que se llevan a cabo de manera manual. Esta práctica prolonga los tiempos de respuesta y genera molestias en los usuarios que esperan servicios de tecnologías de la información (TI) óptimos.

En este contexto, para automatizar estos procesos, la institución ha implementado un robusto centro de datos con una infraestructura de red sólida y servidores potentes (Sistema Oficial de Contratación Pública, 2015). A través de esta infraestructura, se están desarrollando una serie de aplicaciones y servicios de TI que permiten generar tareas específicas para los usuarios, optimizando así tiempos y recursos en beneficio de sus miembros.

Estos servicios y aplicaciones se encuentran centralizados en un lugar específico, compuesto por una serie de equipos tecnológicos y de comunicaciones (Red Hat, 2023). Esta infraestructura ha permitido sistematizar muchos de los procesos clave para el funcionamiento y la operación de la organización, lo que a su vez facilita la obtención de mejores resultados a partir de la información recopilada y procesada en beneficio de su comunidad. Sin embargo, esta centralización también expone a la organización a nuevos riesgos y vulnerabilidades, tanto internos como externos, que pueden introducir algún tipo de ataque y afectar las operaciones de la organización (AWS, 2023).

En este sentido, se destaca la importancia de asegurar tanto los bienes tecnológicos como la información del CD-UCE mediante la aplicación de un estándar internacional centrado en la gestión de la seguridad de la información (VISTAZO, 2022). Por lo tanto, es necesario realizar un análisis de los niveles de madurez de las políticas de seguridad, basado en la normativa internacional, mediante el uso de una herramienta que permita identificar posibles brechas de seguridad. Esto se considera un eje clave en las operaciones que maneja la institución.

Lo descrito en los párrafos anteriores sienta las bases para el desarrollo de una herramienta de análisis diseñada para detectar riesgos y vulnerabilidades en el entorno organizacional. Esta herramienta se enfoca en evaluar los niveles de madurez de las políticas de seguridad aplicadas a los activos del centro de datos de la Universidad Central del Ecuador. Su función es identificar áreas de mejora y facilitar la toma de acciones correctivas en las políticas y procedimientos relacionados con la seguridad, todo ello en cumplimiento de las normativas internacionales pertinentes.

Objetivos

En este contexto, el presente trabajo de investigación reviste suma importancia para garantizar el correcto funcionamiento de las operaciones de la Universidad Central del Ecuador, con un enfoque específico en su centro de datos. Con este propósito, se plantean los siguientes objetivos:

Objetivo general

Elaborar una herramienta de evaluación basada en la norma ISO 27001, que permita medir el nivel de madurez de cumplimiento de políticas de seguridad de la Información en centros de datos de instituciones de educación superior públicas.

Objetivos específicos

- Diagnosticar el estado actual de las políticas de seguridad de la información implementadas en el Centro de Datos de la Universidad Central del Ecuador
- Analizar el proceso de aplicación de políticas y normativas relacionadas a la seguridad de la información, sus características, formas de selección y evolución histórica en el ámbito de las universidades públicas
- Diseñar una herramienta que permita evaluar y medir el nivel de madurez de cumplimiento de políticas en sistemas de gestión de seguridad enfocados a los centros de datos de universidades públicas y que esté basado en la norma ISO 27001.
- Validar la herramienta y establecer el nivel de cumplimiento de normativas de seguridad de la información en el Centro de Datos de la Universidad Central del Ecuador.

Vinculación con la sociedad y beneficiarios directos:

La investigación tiene implicaciones significativas en aspectos clave relacionados con la sociedad. En primer lugar, implica la creación de una herramienta para evaluar el nivel de madurez en el cumplimiento de políticas en Sistemas de Gestión de Seguridad de la Información

(SGSI) para centros de datos en instituciones de educación superior, tomando como caso de estudio la Universidad Central del Ecuador y basándose en una norma reconocida (Organización Internacional de Normalización (ISO), 2024). Esto tiene el potencial de generar un impacto positivo en varias partes interesadas:

Por un lado La Universidad Central del Ecuador, mediante la herramienta propuesta proporcionará a la institución una forma sistemática de evaluar y mejorar su postura de seguridad de la información, fortaleciendo así la protección de sus activos digitales y datos sensibles (Centro Criptológico Nacional CCN-CERT, 2024). Los docentes, estudiantes y personal administrativo y de servicios, mediante la creación de un entorno universitario más seguro que beneficia directamente a los estudiantes, profesores y personal administrativo al garantizar la confidencialidad, integridad y disponibilidad de los recursos digitales y datos relevantes para su trabajo y estudios.

La sociedad en general, a través de una herramienta efectiva para evaluar y mejorar la seguridad de la información principalmente en centros de datos de instituciones educativas lo que puede servir como un modelo para otras universidades y organizaciones, contribuyendo así a elevar los estándares de seguridad a nivel nacional e internacional, en definitiva la propuesta no solo beneficia a la Universidad Central del Ecuador y su comunidad, sino que también tiene el potencial de tener un impacto más amplio en la sociedad al promover prácticas de seguridad de la información más sólidas y efectivas.

Al proteger la información sensible y promover prácticas de seguridad sólidas, se contribuye a crear un entorno más confiable y seguro para los estudiantes, profesores y personal administrativo. Además, al establecer vínculos colaborativos entre los diferentes actores dentro de la comunidad educativa, se fomenta el intercambio de conocimientos y experiencias, lo que puede conducir a una mayor conciencia y preparación en materia de seguridad de la información (EcuaCERT, 2024). Esta mejora en la seguridad de la información en el sector educativo beneficia a toda la sociedad al garantizar la protección de datos críticos y promover un entorno digital más seguro y confiable para todos.

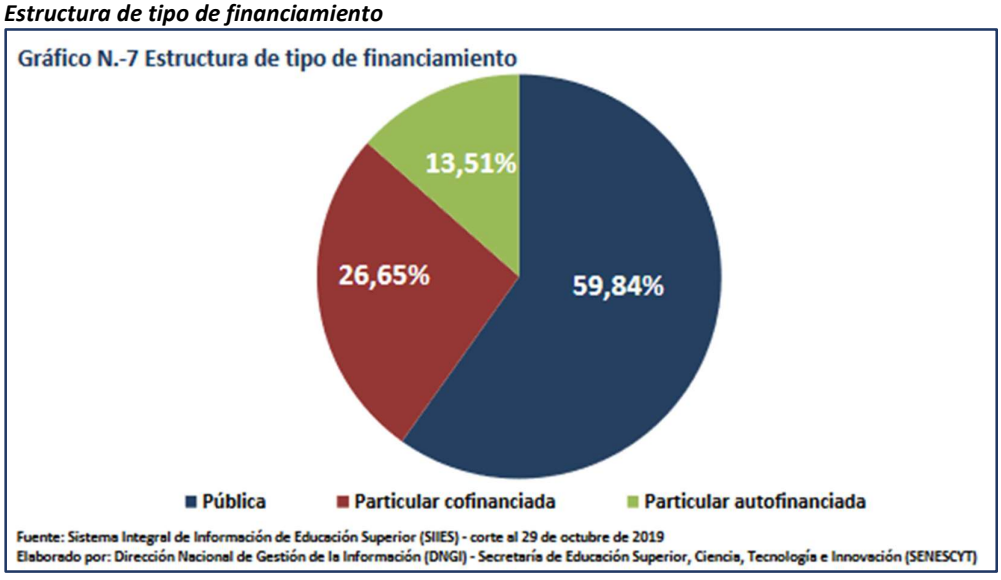
CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

La revisión del estado del arte en este campo de estudio proporciona una comprensión profunda de los fundamentos teóricos, metodológicos y prácticos relacionados con la seguridad de la información en centros de datos de instituciones de educación superior (DATA CENTER MARKET, 2024). Esto establece una base sólida para el desarrollo de la herramienta de evaluación propuesta.

Las Universidades Públicas en el Ecuador, desempeñan un papel fundamental en el acceso a la educación superior para el desarrollo nacional, la promoción de la investigación y la innovación de la sociedad ecuatoriana (Universidad Central del Ecuador, 2024). Sin embargo, debido a la situación económica actual del país, estas instituciones enfrentan desafíos financieros y buscan fortalecer su perfil internacional y su contribución al desarrollo regional mediante el aprovechamiento de las tecnologías de la información. En el país, debido al cambio constitucional en el año 2008, "la implementación de políticas educativas dirigidas al desarrollo de la ciencia y tecnología, con un enfoque social, y asociado a la política estatal del Buen Vivir, se ha suscitado la emergencia de una serie de políticas públicas" (Barros, 2020, pág. 169).

Figura 2.
Estructura de tipo de financiamiento



Nota: Boletín Anual Educación superior, ciencia, tecnología e innovación. (Secretaria de Educación Suerior, Ciencia, Tecnología e Innovación, 2020)

En este sentido como muestra la figura 2, las universidades públicas han experimentado una mayor demanda y con esto a una transformación digital en sus servicios, orientada a beneficiar a los miembros de sus comunidades. En este proceso, las tecnologías de la información y la

seguridad de la información han adquirido un papel fundamental como ejes clave para el funcionamiento de las instituciones educativas. Al adoptar normas internacionales, se promueve la creación de un entorno seguro para las actividades administrativas, académicas e investigativas en las instituciones de educación superior del país (Servicio Ecuatoriano de Normalización INEN, 2024).

Centros de Datos en Instituciones de Educación Superior, la importancia de estos espacios para satisfacer la demanda de servicios tecnológicos debe ir seguido de un análisis detallado de las características específicas de los centros de datos, que abarcan su infraestructura, procesos y desafíos en seguridad de la información (DATA CENTER MARKET, 2024). Entender la infraestructura para administrar de manera efectiva las tecnologías de la información en las instituciones donde "las TI son un elemento táctico que proporciona soporte a los principales servicios universitarios, pero en el futuro están llamadas a convertirse en un elemento estratégico para la universidad" (ANUIES, 2018, pág. 32).

Un centro de datos necesita establecer sólidamente sus operaciones en una infraestructura robusta para garantizar las operaciones tecnológicas de la institución (ODATA, 2022). El hardware de servidores, que constituyen la columna vertebral de la infraestructura de un centro de datos (AXENTIO, 2023), puede ser físicos o virtuales y son el lugar donde se unen los aplicativos y servicios críticos como los sistemas de gestión del aprendizaje, aulas virtuales, sistemas administrativos, alojamiento web, etc. Almacenamiento de datos en medios físicos o en la nube (Google, 2024), para contener grandes volúmenes de datos recolectados de diversas fuentes como sistemas académicos, programas de vinculación, investigaciones, gestión de talento humano, entre otros.

Las redes de datos son esenciales para interconectar los componentes del centro de datos (routers, firewall, switches, etc.) y permitir el acceso a Internet (CEPAL, 2024), un servicio fundamental para la comunidad universitaria. Los sistemas de refrigeración y energía requeridos son básicos debido al calor generado por los equipos en funcionamiento continuo. Es valioso contar con la refrigeración en el área para mantener una temperatura óptima de operación de los equipos. La seguridad física y lógica del centro de datos no queda aislada (SISSA Monitoring, 2023). Este aspecto es esencial para proteger, resguardar o poner a salvo tanto los bienes como los datos sensibles y garantizar el trabajo ininterrumpido de los servicios organizacionales provistos.

Otro punto valioso está relacionado con el suministro eléctrico (Obama, 2022). Los equipos y dispositivos dependen de esta fuente de energía para funcionar y mantener las operaciones

de un centro de datos. En este sentido, se emplea un conjunto de baterías, conexiones eléctricas y generadores de energía para garantizar que toda la infraestructura continúe funcionando incluso en caso de un corte de energía. Estos aspectos y tecnologías se basan en las mejores prácticas y normativas de la industria están integrados en el diseño y construcción de la infraestructura de un centro de datos en cualquier organización. Se adoptan normativas, prácticas y estándares internacionales para garantizar su eficiencia y seguridad (CEPAL, 2024).

Seguridad de la información es fundamental para proteger datos sensibles y garantizar la integridad, confidencialidad y disponibilidad de la información (Organización Internacional de Normalización (ISO), 2024). Debido al aumento exponencial de datos en las organizaciones y a la constante evolución de las amenazas cibernéticas (Thales, 2024), es crucial trabajar en la implementación de medidas sólidas de seguridad. En este sentido, se examinan los aspectos principales para tener en cuenta, como la gestión de acceso, la protección de datos y el seguimiento continuo y sistemático de amenazas (World Economic Forum, 2024). Además, se considera la conformidad normativa a través de acciones que se ajusten a las disposiciones legales establecidas en el país, incluida la reciente ley orgánica para la protección de datos en Ecuador.

La gestión de acceso desempeña un papel fundamental en la salvaguarda de la información. En este sentido, la implementación de controles de acceso físico y lógico, autenticación multifactorial y políticas de privilegios mínimos son políticas que contribuyen a prevenir accesos no autorizados y minimizar riesgos en las organizaciones, como se indica "La gestión de acceso es un componente esencial para garantizar la seguridad de los datos en centros de datos. La implementación de controles sólidos de autenticación y autorización es crucial para proteger contra amenazas internas y externas" (García, 2023).

La protección de datos abarca diversas medidas (CEPAL, 2021, pág. 27), como la encriptación, la segmentación de redes y la implementación de firewalls, que se consideran buenas prácticas para salvaguardar la información sensible. Además, el tratamiento de datos personales incluye técnicas como la anonimización, que convierte los datos en anónimos para evitar su asociación con individuos específicos, y la pseudonimización, que implica reemplazar ciertos campos de datos identificativos con valores ficticios o irreversibles. Estas prácticas son importantes para proteger la privacidad de los usuarios en el entorno organizacional.

En este contexto, tal como se indica "Es la forma más sencilla e importante para garantizar que la información de un sistema de computadora no pueda robarla ni leerla alguien que desee utilizarla con fines maliciosos." (Kaspersky, 2024). A este respecto "la vigilancia constante de

amenazas posibilita la detección precoz y una respuesta ágil ante potenciales vulnerabilidades de seguridad, ya que "la monitorización de amenazas es esencial para mantener la seguridad en centros de datos. La combinación de herramientas de detección avanzada y análisis de registros en tiempo real permite una respuesta rápida ante incidentes de seguridad" (Hernández, 2022).

La adopción e implementación de sistemas de detección y localización de intrusiones, análisis de comportamiento y análisis de registros son herramientas efectivas para identificar actividades sospechosas en entornos empresariales u organizacionales. El cumplimiento normativo implica adherirse a normas como la Ley Orgánica de Protección de Datos Personales de nuestro país, lo cual es un aspecto fundamental para que cualquier tipo de organización garantice la seguridad y privacidad de los datos almacenados (MINTEL, 2021). Por lo tanto, aceptar políticas y procedimientos que cumplan con los requisitos regulatorios puede ayudar a evitar sanciones y proteger la reputación de una organización.

Dado lo anteriormente expuesto, "La protección de datos se refiere a los derechos de las personas cuyos datos se recogen, se mantienen y se procesan, de saber qué datos están siendo retenidos y usados y de corregir las inexactitudes. Si la investigación involucra a personas, se deben considerar las obligaciones legales y éticas con respecto a compartir los datos." (CEPAL, 2024). Por lo tanto, la seguridad de la información es un proceso continuo que requiere la combinación de tecnología, políticas y prácticas de gestión activas y efectivas. Al implementar medidas de seguridad sólidas y comprender las últimas tendencias y regulaciones en ciberseguridad, las organizaciones pueden proteger proactivamente su información y reducir el riesgo.

La seguridad informática es un aspecto decisivo en el campo de la tecnología de la información, que implica proteger sistemas, redes y datos de amenazas cibernéticas. Su importancia aumenta aún más a medida que los ataques cibernéticos se vuelven más frecuentes y los dispositivos y sistemas se interconectan a nivel global. A este apartado se la caracteriza como “la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable” (Aguilera, 2019). Frente a esta situación se debe tomar en cuenta puntos importantes asociados con este ámbito como son:

La gestión de riesgos, que es esencial para desarrollar estrategias de seguridad positivas (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020). Esto implica la identificación y evaluación exhaustiva de los riesgos asociados, así como también el cumplimiento de regulaciones y estándares de seguridad pertinentes, como ISO 31000, COBIT,

entre otros y es de suma importancia para garantizar la protección de datos y preservar la integridad de los sistemas. La protección perimetral, mediante la implementación de firewalls, sistemas de detección de intrusiones y filtrado de contenido, libran un papel fundamental en la defensa de las redes contra ataques externos.

Estas acciones no solo aportan a prevenir intrusiones no autorizadas, además respaldan la confidencialidad y disponibilidad de los datos. La protección de los datos es esencial para salvaguardar la información almacenada y durante su transmisión. El cifrado, la segmentación de la red y la gestión del acceso son aspectos clave e importantes de esto. Estas medidas garantizan la confidencialidad e integridad de los datos, aseguran que sólo el personal autorizado tenga acceso a la información y certifican que la información esté protegida de posibles amenazas.

El manejo de identidad y acceso es crítico para asegurar el entorno organizacional (IBM, 2023). La autenticación multifactorial, el control de acceso basado en roles y la gestión de privilegios son habilidades que contribuyen a garantizar que únicamente los usuarios autorizados accedan a los recursos y datos sensibles. Estas medidas no solo fortalecen la seguridad, además ayudan a la protección de la información confidencial y la prevención de posibles brechas de seguridad.

De la misma manera que en el ámbito de la seguridad de la información, la supervisión y la capacidad de respuesta ante incidentes son igualmente importantes, la implementación de soluciones de monitoreo continuo de seguridad y la capacidad de responder rápidamente a los incidentes son elementos críticos para detectar y mitigar amenazas en tiempo real, al alcanzar este objetivo, se reduce al mínimo el impacto de posibles vulnerabilidades de seguridad en la organización (Ortega, 2021).

La educación y concientización juegan un papel fundamental en la seguridad de una organización (Organización de los Estados Americanos (OEA), 2020). La capacitación regular de los empleados en prácticas seguras de navegación web, manejo de contraseñas y detección de correos electrónicos engañosos es crucial para fortalecer la postura de seguridad y mitigar los riesgos asociados con el factor humano, que suele ser el eslabón más débil de la cadena de seguridad. Al aumentar la conciencia y el conocimiento de los empleados sobre las amenazas cibernéticas y las mejores prácticas de seguridad, se reduce significativamente la probabilidad de incidentes causados por errores humanos o ataques de ingeniería social.

1.2. Proceso investigativo metodológico

El marco metodológico establece la secuencia de la investigación que se llevará a cabo, permitiendo desarrollar los parámetros investigativos de manera lógica y coherente (Pereyra, 2022). Proporciona una estructura que guía al investigador en la selección de métodos, herramientas y técnicas adecuadas para recopilar y analizar los datos de investigación de manera efectiva. Al seguir este marco, se asegura que la investigación sea rigurosa, sistemática y que se alcancen los objetivos planteados de manera eficiente.

Para medir el nivel de madurez de cumplimiento de políticas de seguridad de la información en una organización, y de forma específica para el caso de estudio conforme a la norma ISO 27001, es fundamental seguir un enfoque investigativo que permita evaluar de manera objetiva y sistemática la implementación y el cumplimiento de estas políticas. A continuación, se detallan los pasos a seguir:

1. Revisión de Documentación: Analizar la documentación existente, incluyendo políticas de seguridad, procedimientos, registros de auditorías anteriores, entre otros, para comprender el marco normativo y los requisitos específicos de la ISO 27001.

2. Entrevistas y Encuestas: Realizar entrevistas con los responsables de la seguridad de la información y otros empleados clave para obtener una comprensión más profunda de cómo se implementan y cumplen las políticas de seguridad en la organización. Asimismo, se pueden administrar encuestas para recopilar información de un mayor número de personas.

3. Análisis de Vulnerabilidades: Practicar un análisis de vulnerabilidades técnicas y de procesos para identificar posibles brechas en la seguridad de la información. Esto abarca el escaneo de redes, pruebas de penetración y evaluaciones de riesgos.

4. Evaluación de Controles: Evaluar la efectividad de los controles de seguridad de la información implementados en la organización, como sistemas de detección de intrusos, firewalls, políticas de gestión de accesos, entre otros.

5. Revisión de Incidentes de Seguridad: Analizar incidentes de seguridad anteriores para identificar áreas de mejora y evaluar la efectividad de los procedimientos de respuesta a sucesos.

6. Comparación con los Requisitos de ISO 27001: Comparar los hallazgos obtenidos durante la investigación con los requisitos establecidos por la norma ISO 27001, identificando las brechas de cumplimiento y áreas de mejora.

7. Elaboración de Informe y Recomendaciones: Consolidar los hallazgos de la investigación en un informe detallado que incluya recomendaciones específicas para mejorar el cumplimiento de las políticas de seguridad de la información, así como la madurez en términos de implementación de la norma ISO 27001.

Al seguir estos pasos de manera sistemática y rigurosa, tal como se aprecia en la figura 3, se podrá llevar a cabo una evaluación exhaustiva del nivel de madurez en el cumplimiento de políticas de seguridad de la información en una organización. Esto facilitará la identificación de áreas de mejora y el fortalecimiento de la postura de seguridad.

Figura 3.
Proceso de Investigación

Nota: Elaboración propia

Los enfoques científicos empleados en esta investigación se destacan por su rigurosidad metodológica y su fundamentación empírica de los que resaltan:

Los Métodos Lógicos (Pereyra, 2022), también conocidos como método comparativo, constituyen un tipo de razonamiento basado en la comparación lógica. Es crucial tener en cuenta que este método se emplea dentro del contexto de la investigación. Mientras que el Método Analítico-Sintético es una estrategia de investigación que combina dos enfoques para desarrollar trabajos formales con un esquema claro para alcanzar objetivos específicos.

Los Métodos Empíricos (Pereyra, 2022) constituyen un tipo de investigación científica fundamentado en la lógica experimental y empírica. Este enfoque es ampliamente empleado en las ciencias sociales y naturales mediante la observación de fenómenos y su posterior análisis

estadístico. Al igual, el Método Experimental es un modelo de investigación científica que se basa en el razonamiento lógico y en la experimentación para observar y analizar fenómenos. Este método es ampliamente utilizado en diversos ámbitos, incluyendo el social y el ambiental.

De forma especial este método suministra un sólido fundamento para la toma de decisiones informadas y permite la optimización de las actividades relacionadas con la gestión del centro de datos de la Universidad Central del Ecuador. Al seguir este enfoque, se obtiene una comprensión detallada de cómo se implementan y cumplen las políticas de seguridad de la información, lo que facilita la identificación de áreas de mejora y la adopción de medidas correctivas apropiadas. Además, al utilizar un método sistemático y riguroso, se garantiza la fiabilidad y validez de los resultados obtenidos, lo que aumenta la confianza en las conclusiones y recomendaciones derivadas del estudio.

En última instancia, esta metodología contribuye a fortalecer la postura de seguridad de la universidad y a garantizar la protección efectiva de los datos y sistemas críticos en el centro de datos, lo que afirma su operación eficiente e inequívoca en todo momento. Esto, a su vez, contribuye a fortalecer su imagen institucional, demostrando un compromiso sólido con la seguridad y el buen manejo de la información.

1.3. Análisis de resultados

Para el análisis e interpretación de los resultados, es importante tener en cuenta que la Universidad Central del Ecuador, reconocida en el ámbito de la educación superior y clasificada como una de las más destacadas del país, cuenta con una población de 42,883 estudiantes matriculados para el período 2023-2024 en sus diversas facultades (Universidad Central del Ecuador, 2024). Este dato proporciona contexto y relevancia a los hallazgos obtenidos en el estudio, ya que refleja el alcance y la influencia de las políticas y prácticas de seguridad de la información dentro de una institución de gran envergadura y prestigio académico.

Dentro de la Dirección de Tecnologías de la Información y Comunicaciones (DTIC), el área de Infraestructura juega un papel importante al administrar y gestionar el centro de datos. Para garantizar una operación eficiente y segura, es fundamental establecer procedimientos claros que deben ser aplicados y respetados como parte del proceso de gestión. Estos procedimientos pueden abarcar una variedad de áreas, como la configuración y mantenimiento de servidores, almacenamiento de datos, redes, seguridad física y lógica, gestión de energía, entre otros.

Al definir y seguir procedimientos estandarizados, se asegura que las operaciones en el centro de datos se realicen de manera consistente y conforme a las mejores prácticas. Esto ayuda a minimizar el riesgo de errores y aumenta la eficiencia en la gestión de la infraestructura tecnológica. Conjuntamente, el cumplimiento de estos procedimientos contribuye a mantener la seguridad y disponibilidad de los sistemas y datos críticos alojados en el centro de datos.

Es importante que los procedimientos sean documentados de manera clara y accesible para todo el personal involucrado en la gestión del centro de datos. Al mismo tiempo, deben ser revisados y actualizados periódicamente para asegurar que reflejen los cambios en la infraestructura tecnológica y en los requisitos de seguridad y cumplimiento. De esta manera, el área de Infraestructura puede cumplir efectivamente con su responsabilidad de garantizar el funcionamiento seguro y confiable del centro de datos.

En este contexto, se ha realizado una encuesta anónima (ver anexo 1) dirigida a los funcionarios responsables de la administración del centro de datos de la institución. En dicha encuesta, se les solicita responder a nueve preguntas relacionadas con el cumplimiento de políticas conforme a la normativa internacional. Posteriormente, se lleva a cabo un análisis cualitativo de las respuestas obtenidas (consultar anexo 2).

Con respecto a la existencia de un Sistema de Gestión de la Seguridad de la Información (SGSI) implementado conforme a alguna norma existente y reconocida en el CD-UCE, tres de los operadores responsables del área afirman no tenerlo implementado, sin embargo uno menciona que hay documentación no tan formalizada al respecto, y que además no está aprobada por algún comité directivo de la institución

Con relación a las medidas de seguridad físicas para proteger los recursos críticos de información implementadas en el CD-UCE, la totalidad de los encuestados mencionaron tener acceso biométrico para proteger la infraestructura y los recursos críticos de información, mientras que dos operadores del sitio indicaron tener redundancia eléctrica, de los encuestados tres indicaron contar con sistemas contra incendios, y para otros dos operarios revelaron poseer un generador eléctrico. Igualmente se mencionaron por parte de los indagados otros elementos como cámaras de seguridad, respaldo energético mediante UPS y un sistema de enfriamiento.

Con respecto a la evaluación regular del riesgo del centro de datos, dos empleados mencionan que esta actividad no se lleva a cabo en el sitio, mientras que los otros dos operadores afirman que se realiza una evaluación de riesgos al implementar soluciones de hardware, software o ambos. Además, señalan que esta tarea no se documenta en los archivos del área.

En relación con la existencia de un proceso para la gestión de incidentes de seguridad de la información relacionados a eventos en el centro de datos, tres de los encuestados indican que no hay un proceso definido para manejar incidentes. Dos funcionarios mencionan que reciben notificaciones de alertas de vulnerabilidades sobre la red de la institución a través del proveedor de servicios de internet, mientras que otra persona señala que se toman medidas según el evento y que algunos incidentes son recurrentes en la organización. En lo que respecta a la realización de auditorías internas periódicas para medir el cumplimiento de las políticas de seguridad de la información en el centro de datos, todos los encuestados indicaron que no se llevan a cabo dichas auditorías internas.

La mayoría de los responsables del centro de datos señalan la falta de capacitación en seguridad de la información como un factor que contribuye a la persistencia de riesgos. Un funcionario destaca que el aprendizaje es principalmente autónomo, mientras que otro menciona la escasez de recursos presupuestarios para formar al personal en temas de seguridad informática. En cuanto a establecer políticas y procedimientos claros para el control de acceso físico y lógico en el centro de datos, dos encuestados exteriorizan que algunos procesos están documentados en el archivo del área, mientras que uno menciona la falta de documentación formal. Sin embargo, todos confirman la presencia de controles físicos y lógicos en el centro de datos.

Frente a la presencia de pruebas frecuentes de seguridad para detectar posibles brechas, la mayoría de los encuestados señalan que no se realizan ensayos de forma regular. Algunos mencionan la realización de pruebas de hacking ético y también resaltan la notificación de vulnerabilidades por parte del proveedor de servicios de internet, mientras que un funcionario indica que las pruebas realizadas carecen de una planificación dentro de la organización. En cuanto a la existencia de un proceso de mejora continua para fortalecer la seguridad de la información basado en evaluaciones y auditorías previas, los funcionarios del área de tecnologías afirman que no hay un proceso formal de mejora continua. Además, uno de estos funcionarios menciona que se realizan correcciones o mejoras en respuesta a un incidente.

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

Actualmente, existen cambios vertiginosos en el entorno organizacional debido a la globalización de los mercados, invenciones tecnológicas, cambios sociales y políticos, así como al aumento de la conciencia y demanda por parte de los usuarios de servicios tecnológicos, por ello las organizaciones buscan estar renovando cada día sus plataformas tecnológicas en favor de sus comunidades para brindar soluciones (CEPAL, 2021). Estas soluciones conducen a la gestión (tratamiento y manipulación) de información sensible relacionada con el buen uso y confidencialidad de esta.

Como lo señala la CEPAL "Las amenazas a la seguridad de los datos pueden tener como resultado el acceso no autorizado a un conjunto de datos, su corrupción e incluso su pérdida total. Es por esto por lo que es importante considerar algunos riesgos comunes en el manejo de los datos y saber cómo enfrentarlos" (CEPAL, 2024). **La ciberseguridad** posee una correlación con la seguridad de la información, en este sentido la podemos definir como la "protección de activos de información que aborda las amenazas a la información procesada, almacenada y transportada a través de los sistemas interconectados" (Ortega, 2021).

Confidencialidad, como se lo describe es el "principio que indica que solo pueden acceder a los recursos de un sistema los usuarios autorizados" (Ortega, 2021). La confidencialidad se centra en restringir el acceso a personas no autorizadas y consiste en proteger la información para prevenir su acceso o divulgación no autorizados.

La integridad, es la propiedad mediante la cual se "garantiza la exactitud de los datos transportados o almacenados, asegurando que no se ha producido su alteración, pérdida o destrucción ya sea de forma accidental o intencionada por errores de software o hardware o por condiciones medioambientales" (Ortega, 2021). Este apartado se refiere a mantener los datos intactos, sin modificaciones o alteraciones por parte de terceros.

La disponibilidad, hace referencia a la "capacidad de un servicio, un sistema o una información a ser accesible y utilizable por los usuarios o procesos autorizados cuando estos lo requieran" (Ortega, 2021). La garantía de un acceso oportuno y confiable al uso de la información y de los sistemas es lo que se establece como disponibilidad. Este aspecto es importante, dado que cualquier interrupción en su disponibilidad podría ocasionar una pérdida del servicio que se está proporcionando. Esto no solo se aplica al ámbito del software, sino también al mantenimiento del hardware, las redes, los dispositivos y la protección general de

los equipos físicos utilizados para llevar a cabo los procesos de almacenamiento de la información.

Normas familia ISO, ante lo mencionado anteriormente, es necesario buscar en las organizaciones medidas que puedan asegurar los pilares de la información. Tomando las palabras del presidente de la ISO, John Walter, "La familia de normas ISO es fundamental para la mejora continua y la excelencia en las organizaciones de todo el mundo. Proporciona un marco sólido para la gestión de la calidad, el medio ambiente y otros aspectos clave del desempeño empresarial" (Organización Internacional de Normalización (ISO), 2024).

La norma ISO de la serie ISO/IEC 27000, establece los principios teóricos esenciales para la gestión de la seguridad de la información en las organizaciones. Desarrollada por la Organización Internacional de Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC), esta norma ofrece un marco completo para la implementación y gestión de un sistema de gestión de seguridad de la información (SGSI) (Organización Internacional de Normalización (ISO), 2024).

El estándar ISO 27000 describe la implementación de un sistema de gestión integral para la seguridad de la información, que abarca todos los controles administrativos, técnicos y operativos necesarios para mantener protegida la información dentro de la organización. Esta norma define doce dominios de seguridad, como se aprecia en la figura 4, donde se representan los componentes de esta norma. Estos dominios sirven como base común para el desarrollo de indicadores de seguridad organizativa y prácticas eficaces de gestión de la seguridad.

Figura 4.
Dominios de seguridad ISO 27000

Nota: Propia, adaptación ISO 27000 (Organización Internacional de Normalización (ISO), 2024)

Los centros de datos son infraestructuras físicas diseñadas para albergar servidores, sistemas de almacenamiento, equipos de red y otros componentes ineludibles para el procesamiento, almacenamiento y distribución de información y aplicaciones informáticas. Estos centros juegan un papel fundamental en el funcionamiento de redes, servicios en línea, aplicaciones web y diversas operaciones digitales (Check Point Software Technologies Ltd., 2024).

También conocidos como "Data Center", estos centros son lugares donde convergen varios aspectos críticos relacionados con la infraestructura tecnológica de una organización, "es un espacio con determinadas características físicas especiales de refrigeración, protección, redundancia, cuyo objetivo es alojar todo el equipamiento tecnológico de la compañía brindando seguridad y confiabilidad" (Pacio, 2014). Una interrupción en el servicio ya sea por problemas en la red, fallas en el suministro eléctrico o el sistema de enfriamiento, puede tener un impacto negativo en los servidores, lo que podría ocasionar pérdidas económicas o de la reputación de una empresa.

Gestión de riesgos, donde debemos considerar que a medida que las organizaciones adoptan gradualmente nuevas tecnologías de la información, transformando actividades, procesos y procedimientos antes mecánicos y manuales, surgen brechas de seguridad no contempladas que aumentan el riesgo de las operaciones y el control de procesos. Se puede definir como las "actividades coordinadas para dirigir y controlar la organización con relación al riesgo" con el propósito de gestionar el riesgo mediante el establecimiento de controles e indicadores que contribuyen a resguardar la información (Zevallos, 2019).

La seguridad de la información se define a la seguridad de la información como "aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada" (Briceño, 2021). Para comprender los fundamentos teóricos de la seguridad de la información en los centros de datos, es importante considerar diferentes enfoques y conceptos clave respaldados por la literatura especializada. Uno de los marcos más reconocidos en este campo es el modelo de seguridad de la información de la ISO/IEC 27001, que establece una serie de controles y buenas prácticas para la gestión de la seguridad de la información.

El cumplimiento normativo y el éxito empresarial dependen de la visibilidad y el control de una organización sobre los datos confidenciales que posee" (Check Point Software Technologies Ltd., 2024). Además de estos principios, es importante considerar otros aspectos relevantes, como la gestión de riesgos, el cumplimiento normativo, la concienciación del personal y la

monitorización constante de las amenazas emergentes (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2020).

2.2. Descripción de la propuesta

En un breve contexto, el desarrollo y aplicación de un instrumento de evaluación del nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información, basado en la Norma ISO 27001, representa un paso decisivo para la Universidad Central del Ecuador en su camino hacia la excelencia en seguridad de la información en su centro de datos, asegurando así la protección y confiabilidad de sus operaciones y servicios en favor de docentes, estudiantes, personal administrativo y de servicios como usuarios que demandan servicios tecnológicos de calidad en una infraestructura sólida y segura (Organización Internacional de Normalización (ISO), 2024).

a. Estructura general

En la esfera por la gestión de la seguridad de la información, la evaluación del nivel de madurez del cumplimiento de políticas es primordial para garantizar la protección adecuada de los activos de información en entornos críticos como los centros de datos de instituciones de educación superior. En este contexto la normativa ISO 27001 facilita una moldura concreta para el establecimiento, implementación, mantenimiento y mejora continua de un Sistema de Gestión de la Seguridad de la Información (SGSI).

En este contexto, la Universidad Central del Ecuador se enfrenta al desafío de garantizar la seguridad de la información en sus centros de datos, que albergan datos sensibles y críticos para su funcionamiento. Para abordar este desafío, se ha desarrollado un instrumento de evaluación del nivel de madurez de cumplimiento de políticas, basado en los requisitos de la Norma ISO 27001 y adaptado a las necesidades específicas de la institución.

Este instrumento de evaluación se centra en diversos aspectos clave, como la identificación de activos de información, la evaluación de riesgos, el establecimiento de controles de seguridad adecuados, la gestión de incidentes y la mejora continua. A través de un enfoque sistemático y estructurado, permite a la Universidad Central del Ecuador medir su nivel de cumplimiento con los requisitos establecidos por la norma internacional, identificar áreas de mejora para tomar acciones correctivas y preventivas pertinentes.

Al implementar este instrumento de evaluación, la Universidad Central del Ecuador como caso de estudio busca fortalecer su capacidad para proteger la confidencialidad, integridad y disponibilidad de la información, mitigar riesgos de seguridad y cumplir con las expectativas de

sus partes interesadas. Frente a este escenario la institución reconoce la importancia de proteger la información sensible y crítica alojada en su centro de datos, en su calidad de institución de prestigio en educación superior pública del país.

Para asegurar un nivel óptimo de seguridad de la información, la institución debe evaluar el grado de cumplimiento de políticas en sus Sistemas de Gestión de la Seguridad de la Información (SGSI) de acuerdo con la norma ISO 27001. La propuesta presentada aquí ofrece un enfoque integral para llevar a cabo esta evaluación, identificar áreas de mejora y fortalecer la postura de seguridad de la información a través de la implementación de un modelo de seguridad, tal como se ilustra en la figura 5.

Figura 5.
Modelo de Seguridad y Privacidad UCE

Nota: Propia, adaptación modelo PDSA

b. Explicación del aporte

La seguridad de la información se ha convertido en una prioridad estratégica para todas las organizaciones en la actualidad. Esto se debe a la diversidad y sensibilidad de los datos manejados, que incluyen información académica, administrativa y de investigación en el ámbito educativo. Es crucial contar con un Sistema de Gestión de la Seguridad de la Información (SGSI)

basado en la norma ISO 27001 para garantizar la confidencialidad, integridad y disponibilidad de la información de la comunidad académica.

Además, es fundamental evaluar periódicamente el cumplimiento de las políticas de seguridad de la información para mantener la efectividad del SGSI. Reconociendo la importancia de la investigación, resulta vital tener la capacidad de evaluar el nivel de madurez del cumplimiento de políticas, utilizando un instrumento diseñado específicamente con este propósito.

Una vez con el uso del instrumento o herramienta, podemos identificar áreas de mejora y brechas de cumplimiento con respecto a los requisitos establecidos en la norma ISO 27001 para la seguridad de la información del centro de datos del caso de estudio. Estos hechos nos permiten tener la visión de proporcionar recomendaciones específicas para implementar, fortalecer o mejorar el SGSI y aumentar el nivel de seguridad de la información en el entorno concentrado del centro de datos de la institución. Esto sin duda conlleva a realizar actividades usando una metodología para la evaluación utilizando un enfoque multifacético que incorpora:

- La revisión documental implica un análisis exhaustivo de las políticas, procedimientos y controles implementados en el Sistema de Gestión de Seguridad de la Información (SGSI), conforme a los estándares de la norma ISO 27001. Este proceso se lleva a cabo con el objetivo de evaluar la efectividad y el cumplimiento de las medidas de seguridad establecidas en la organización. Durante la revisión documental, se examinan detalladamente los documentos relevantes, como políticas de seguridad de la información, procedimientos operativos, registros de auditoría y evidencia de controles implementados. Este análisis proporciona una visión clara del estado actual del SGSI, identificando áreas de mejora y asegurando la alineación con los requisitos y principios de la norma ISO 27001.
- Las entrevistas representan un diálogo directo con el personal técnico encargado de la gestión y administración de la infraestructura tecnológica enclavada en el centro de datos. El propósito de estas conversaciones es comprender en profundidad el funcionamiento y la implementación de dicha infraestructura, con el objetivo de obtener una visión clara y de primera mano sobre el cumplimiento de las políticas establecidas. Durante las entrevistas, se exploran aspectos clave relacionados con los procesos, procedimientos y controles de seguridad implementados, así como cualquier desafío o área de mejora identificada. Estas interacciones proporcionan información

valiosa para evaluar la eficacia del Sistema de Gestión de Seguridad de la Información (SGSI) y garantizar la alineación con los estándares y requisitos establecidos.

- La evaluación in situ envuelve el poder llevar a cabo una inspección física de las instalaciones del centro de datos, complementando las actividades previas realizadas. El objetivo principal de esta evaluación es evaluar la implementación práctica de los controles de seguridad existentes. Durante esta fase, se realizan verificaciones directas de los controles físicos y tecnológicos establecidos para proteger la infraestructura de la información. Se examinan aspectos como el acceso físico a las instalaciones, la seguridad de los sistemas de seguridad física, la protección de equipos y datos, entre otros. Los resultados obtenidos de esta evaluación in situ proporcionan una parte concluyente del trabajo, brindando una visión completa y precisa del estado de seguridad del centro de datos.

Mediante la aplicación del instrumento, se obtiene una evaluación del nivel de madurez y cumplimiento de las políticas de seguridad. Esto permite adquirir una visión completa en el espectro legal y contractual, de acuerdo con lo reglamentado por la Ley Orgánica de Protección de Datos del Ecuador. Los resultados obtenidos son analizados en detalle, y en el informe se incluirán los siguientes aspectos:

a) **Cumplimiento normativo:** Se evaluará el grado de cumplimiento de las disposiciones legales y reglamentarias establecidas por la Ley Orgánica de Protección de Datos del Ecuador.
b) **Análisis contractual:** Se examinarán los contratos y acuerdos existentes para verificar el cumplimiento de las cláusulas relacionadas con la protección de datos y seguridad de la información.
c) **Identificación de brechas:** Se destacarán las áreas de mejora y las posibles brechas de cumplimiento en relación con la normativa de protección de datos.

Los entregables de la evaluación comprenden un informe resumido del cumplimiento de políticas, una presentación ejecutiva de los resultados y recomendaciones, así como la documentación de apoyo que incluye entrevistas y hallazgos recopilados durante la investigación in situ. Esta evaluación del nivel de madurez del Sistema de Gestión de la Seguridad de la Información (SGSI) del centro de datos de la Universidad Central del Ecuador ofrece una visión clara de su postura actual en seguridad de la información.

Al mismo tiempo, servirá como base para fortalecer su enfoque en la gestión de riesgos y el cumplimiento normativo. Estos entregables proporcionan una guía integral para la

implementación de mejoras y la adopción de medidas correctivas, contribuyendo así a reforzar la seguridad de la información en la universidad y garantizar el cumplimiento de los estándares legales y regulatorios vigentes.

c. Estrategias y/o técnicas

Bajo preceptos establecidos en la norma ISO 27001, se inicia con la revisión de los aspectos generales de la organización para el caso de estudio es la Universidad Central del Ecuador, donde se analizan ciertos aspectos generales en el contexto actual de la institución y su relación y conocimiento por el sistema de gestión de seguridad de la información, el objetivo de la norma ISO 27001 y los beneficios de esta.

Figura 6.
Tratamiento de las amenazas de ciberseguridad

Nota: Propia, adaptación de las principales actividades de la ciberseguridad

La figura 6, ofrece una visión comprensiva de las actividades para el tratamiento de amenazas, dado que en la actualidad todo está inmerso en el internet, y existe la posibilidad de encontrar información personal o de la organización en este entorno sin que los actores involucrados sean conscientes de ello. En este contexto, se hace hincapié en que la universidad

y la información generada internamente constituyen el activo más importante, por lo que proteger este activo resulta fundamental.

La seguridad de la información incluye la implementación y gestión de controles adecuados que tengan en cuenta una amplia variedad de amenazas, con el objetivo de garantizar el éxito y la continuidad del negocio para minimizar las consecuencias de las fallas en la seguridad de la información (Organización Internacional de Normalización (ISO), 2024). Para lo cual la norma ISO 27001 cumple con el objetivo de defender, proteger y gestionar la información como un activo de suma importancia para la Universidad Central del Ecuador.

El análisis de la norma señala la siguiente estructura que se debe tomar en cuenta en la organización y son:

ESTRUCTURA
0. Introducción
1. Objeto y campo de aplicación
2. Normas para consulta
3. Términos y definiciones
4. Contexto de la organización
5. Liderazgo
6. Planificación
7. Soporte
8. Operación
9. Evaluación del Desempeño
10. Mejora

Dentro de los aspectos contemplados en la norma, se incluyen otros apartados relacionados con los controles organizativos, controles sobre las personas, controles físicos y controles tecnológicos, los cuales se detallan a continuación (Organización Internacional de Normalización (ISO), 2024):

1. INTRODUCCION
0. Introducción
0.1 Generalidades
0.2 Compatibilidad con otros sistemas de gestión

2. OBJETO Y CAMPO DE APLICACIÓN
Norma aplicable a cualquier organización, cualquiera que sea su actividad y cualquiera que sea su tamaño.

3. NORMA PARA CONSULTA
ISO 27000:2014.

4. TÉRMINIOS Y DEFINICIONES
Recogidos en la Norma ISO 27000

5. CONTEXTO DE LA ORGANIZACIÓN
4.1 Comprensión de la organización y de su contexto
4.2 Comprensión de las necesidades y expectativas de las partes interesadas
4.3 Determinación del alcance del sistema de gestión de seguridad de la información (SGSI)
4.4 Sistema de gestión de seguridad de la información

6. LIDERAZGO
5.1 Liderazgo y compromiso
5.2 Política
5.3 Roles, responsabilidades y autoridades en la organización

7. PLANIFICACIÓN (PLAN)
6.1 Acciones para tratar los riesgos y oportunidades
6.1.1 Generalidades
6.1.2 Apreciación de riesgos de seguridad de la información
6.1.3 Tratamiento de los riesgos de seguridad de la información
6.2 Objetivos de seguridad de la información y planificación para su consecución
6.3 Planificación de los cambios

8. SOPORTE
7.1 Recursos

7.2 Competencias
7.3 Comunicación
7.4 Control de la información
7.5 Información documentada
7.5.1 Consideraciones generales
7.5.2 Creación y actualización
7.5.3 Control de información documentada

9. OPERACIÓN (DO)
8.1 Planificación y control operacional
8.2 Apreciación de los riesgos de seguridad de la información
8.3 Tratamiento de los riesgos de la seguridad de la información

10. EVALUACIÓN DEL DESEMPEÑO
9.1 Seguimiento, medición, análisis y evaluación
9.2 Auditoría interna
9.2.1 General
9.2.2 Programación de la auditoría interna
9.3 Revisión por la Dirección
9.3.1 General
9.3.2 Aportes a la revisión por dirección
9.3.3 Resultados de la revisión por dirección

11. MEJORA
10.1 Mejora
10.2 No conformidad de acciones correctivas

En la elaboración de esta herramienta, se toman en consideración los apartados del 1 al 4 de la norma ISO 27000, donde se establecen los requisitos del Sistema de Gestión de Seguridad de la Información (SGSI) para la universidad. En tanto que los apartados del 5 al 11 de la norma ISO 27000 no pueden ser excluidos, ya que representan requisitos obligatorios establecidos por la normativa. Es fundamental considerarlos en la construcción del instrumento, ya que

proporcionan directrices claras para el establecimiento y mantenimiento efectivo del Sistema de Gestión de Seguridad de la Información (SGSI) de la universidad.

Para el caso de estudio y considerando las particularidades de cada organización dentro de su contexto, existe la posibilidad de excluir controles que no sean aplicables en la herramienta. Sin embargo, es imperativo que estas exclusiones estén debidamente justificadas en la Declaración de Aplicabilidad (SOA). En este sentido, se toman en cuenta los apartados descritos en la norma relacionados con:

Contexto de la organización: Se puede definir como el entorno en el cual la organización para el caso de estudio la Universidad Central del Ecuador opera, tanto internamente como en su entorno, este ambiente afecta de forma positiva o negativa a los productos, servicios, metas y en general, al desarrollo de las actividades de la institución.

Liderazgo: Establecer requisitos de liderazgo de la alta dirección de la universidad y su participación del SGSI. Esto encierra la revisión de los roles y responsabilidades, comunicación de políticas de seguridad de la información y el establecer objetivos y planes de mejora continua para la institución.

Planificación: Refiere los requisitos de planificación del SGSI dentro del entorno universitario, incluida la identificación y evaluación de riesgos y oportunidades, la determinación de objetivos y requisitos de seguridad, la selección de controles de seguridad y el desarrollo de planes de implementación.

Soporte: Establece los requisitos de recursos necesarios para implementar y mantener el SGSI en la organización educativa, comprendidos los recursos humanos, la infraestructura y los recursos financieros. También encierra requisitos de capacidad, concientización e intercambio de información dentro de la universidad.

Operación: Describe los requisitos para implementar y operar un SGSI del establecimiento, incluida la gestión de riesgos, la seguridad de la información, el control de acceso, la continuidad del negocio y otros controles de seguridad. Igualmente encierra los requisitos para el control de documentos y registros que maneja la institución.

Evaluación del desempeño: Establece los requisitos para monitorear, medir, analizar y evaluar el desempeño del SGSI de la entidad educativa, esto involucra auditorías internas, revisiones de la gestión y controles de cumplimiento.

Mejora: En este apartado se abordan los requisitos necesarios para asegurar que las acciones correctivas sean adecuadas para prevenir los efectos de las no conformidades identificadas. Dónde también se contemplan los requisitos para la mejora continua del SGSI de la universidad.

Con base en los principios establecidos en la normativa, se elabora la matriz de cumplimiento que abarca cada eje temático. Dentro de esta matriz, se desarrollan indicadores que nos permiten asignar un valor según el grado de cumplimiento de las políticas, lo cual se refleja mediante una clasificación de semáforo.

NIVELES DE MADUREZ				
Valor	**Color**	**Porcentaje**		**Descripción**
1		0	20	No se cumple, no se conoce ni se aplica ninguna norma.
2		21	40	Se sabe de su existencia pero no se hace nada.
3		41	60	Se aplica empíricamente, sin estandarizar en un documento.
4		61	80	Estandarizado pero no implementado.
5		81	100	Documentado e implementado.

Este sistema de evaluación se compone de 5 niveles que abarcan desde el incumplimiento hasta el cumplimiento efectivo del parámetro evaluado, respaldado por documentación pertinente. Este enfoque permite asignar una puntuación a cada indicador de cumplimiento según la escala de semáforo establecida. Al finalizar, se realiza una suma de las puntuaciones en cada área para obtener un promedio que representa la aplicación general de la política. Este promedio se convierte en un porcentaje, el cual se visualiza a través de un gráfico de tela de araña, proporcionando una representación visual del nivel de madurez alcanzado en ese punto.

La representación gráfica obtenida muestra una figura que, si está correctamente construida, indica un nivel de cumplimiento adecuado o satisfactorio. Sin embargo, cualquier distorsión evidenciada en el graficado revela deficiencias en la aplicación o en la articulación de las políticas de seguridad, señalando áreas que requieren mejoras para fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI). Al concluir la herramienta, se presenta un resumen ejecutivo que comprende una gráfica de barras junto con una síntesis de todos los campos evaluados. Esta visión panorámica proporciona información integral sobre el estado de la organización en relación con las políticas implementadas y las áreas de mejora identificadas. Es de vital importancia que la alta gerencia tome en cuenta estos datos para elevar el nivel de seguridad y la reputación de la institución.

2.3. Validación de la propuesta

Basados en los criterios de los especialistas en seguridad de la información (anexo 3) que han brindado un valioso aporte y retroalimentación al trabajo de investigación, la propuesta recibe una evaluación general muy positiva en varios aspectos como estos:

- Alcance y representatividad: La propuesta se considera muy adecuada en términos de su alcance y su capacidad para generar valor. Esto sugiere que la propuesta aborda de manera efectiva las necesidades identificadas y tiene el potencial de ofrecer beneficios significativos.
- Capacidad de implementación: Se percibe que la propuesta tiene una buena capacidad de implementación, especialmente si los contenidos son aplicables. Esto sugiere que la propuesta es práctica y viable en el contexto de la organización.
- Base conceptual y teórica: La propuesta parece estar respaldada por una sólida base de conceptos y teorías, lo que indica un enfoque sistémico y articulado en su desarrollo.
- Consideración de procedimientos actuales y cambios tecnológicos: La propuesta ha tenido en cuenta los procedimientos actuales y los cambios científicos y tecnológicos relevantes, lo que sugiere una adaptación adecuada a las condiciones del entorno.
- Atributos cualitativos para satisfacer las expectativas: La propuesta se percibe como muy adecuada en términos de satisfacción de las expectativas de los beneficiarios, lo que indica que se han tenido en cuenta sus necesidades y preferencias.
- Utilización acorde a los recursos disponibles: La propuesta se considera muy adecuada en términos de su nivel de utilización por parte de la organización, lo que sugiere que se ha tenido en cuenta la disponibilidad de recursos para su implementación.
- Contundencia y conveniencia para solucionar el problema: Finalmente, la propuesta se evalúa como muy adecuada en términos de su capacidad para solucionar el problema planteado, lo que indica que se percibe como una solución efectiva y apropiada.

En resumen, podemos argumentar con el respaldo adecuado que la propuesta ha sido evaluada de manera positiva en varios aspectos por especialistas en seguridad de la información, lo que sugiere un alto potencial para el éxito y la satisfacción de la organización y sus beneficiarios.

2.4. Matriz de articulación de la propuesta

En la presente matriz se sintetiza la articulación del producto realizado con los sustentos teóricos, metodológicos, estratégicos-técnicos y tecnológicos empleados.

Tabla 1.

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
Seguridad de la Información	Seguridad y metodologías que proporcionan seguridad de la información en entornos organizacionales	Ciclo de Deming" o PDCA (Planificar, Hacer, Verificar, Actuar))	Análisis de mejores prácticas para implementar o mejorar la seguridad de la información en la organización	El adecuado manejo de la seguridad de la información proporciona a las organizaciones mejorar su reputación.	Word, Excel, lector de PDF, internet, normas y estándares internacionales.
ISO 27000	ISO/IEC 27001-2022 para establecer, implementar y mantener un SGSI	Ciclo de Deming" o PDCA (Planificar, Hacer, Verificar, Actuar)	Analizar y establecer un enfoque sistemático y metodológico para gestionar la seguridad de la información en una organización	Conocer la norma ISO 27001 para elaborar herramienta de cumplimiento de políticas de seguridad	Internet, normas y estándares internacionales.

Centro de Datos	**Disponibilidad y continuidad de servicios (integridad, confidencialidad y disponibilidad)**	Orientación sistemática para el diseño, implementación y gestión eficientemente la infraestructura de TI	Analizar el entorno seguro, eficiente y confiable para el almacenamiento, procesamiento y distribución de datos y servicios de TI en el centro de datos de las organizaciones	Conocer el entorno del centro de datos de la Universidad Central del Ecuador	Word, Excel, lector de PDF, internet, norma ISO/IEC 27001 2022
Analizar Requerimientos de la norma	ISO/IEC 27001-2022 para establecer, implementar y mantener un SGSI y documentación de la organización	Metodología de Investigación Científica Recopilación y análisis de datos	Análisis de documentación de la organización	Conocer el entorno organizacional de la institución educativa, las normas y políticas aplicadas al centro de datos, construcción de herramienta	Excel, lector pdf, norma ISO 27001
Definir Pruebas de herramienta	ISO/IEC 27001-2022 para establecer, implementar y mantener un SGSI y	Metodología de Investigación Científica Recopilación y análisis de datos	Analizar el entorno y los activos para correr herramienta para comprobar el nivel de madurez de políticas de seguridad	Correr la herramienta para comprobar su funcionamiento	Norma ISO 27001, herramienta.

	documentación de la organización				
Ejecutar pruebas con herramienta	SO/IEC 27001-2022 para establecer, implementar y mantener un SGSI y documentación de la organización	Metodología de Investigación Científica Recopilación y análisis de datos	Recolección de datos arrojados por la herramienta para su análisis.	Obtención de información del cumplimiento de políticas	Norma ISO 27001, Excel
Evaluar resultados	SO/IEC 27001-2022 para establecer, implementar y mantener un SGSI y documentación de la organización	Metodología de Investigación Científica, conclusiones y recomendaciones	Evaluar la información obtenida	Análisis y presentación de resultados	Word, Excel, lector PDF, herramienta de cumplimiento de políticas

Fuente: Elaboración propia

2.5. Análisis de resultados. Presentación y discusión

A continuación, se describen brevemente los resultados obtenidos en la aplicación de la lista de verificación y evaluación de cumplimiento de la norma ISO 27001 (herramienta de evaluación), respecto al estado situacional actual del Data Center de la Universidad Central del Ecuador en temas de cumplimiento de prácticas que posibiliten detectar que se hace y/o que hace falta por mejorar para alinearse a esta norma, la cual posibilita manejar estándares de seguridad de la información probados e implementados en otras organizaciones.

Basándose en los lineamientos proporcionados por la norma ISO/IEC 27001:2022 la aplicabilidad y límites del SGSI para el caso de estudio (DC-UCE) estarán determinados por los siguientes parámetros:

- Redes e infraestructura de TI.
- Servicio de Internet.
- Switch de Core y Distribución.
- Almacenamiento y respaldos de información.
- Seguridad Perimetral

4. ALCANCE DE SGSI

Figura 7.
Resultados en porcentaje de los niveles de madurez del Capítulo 4 (caso de estudio)

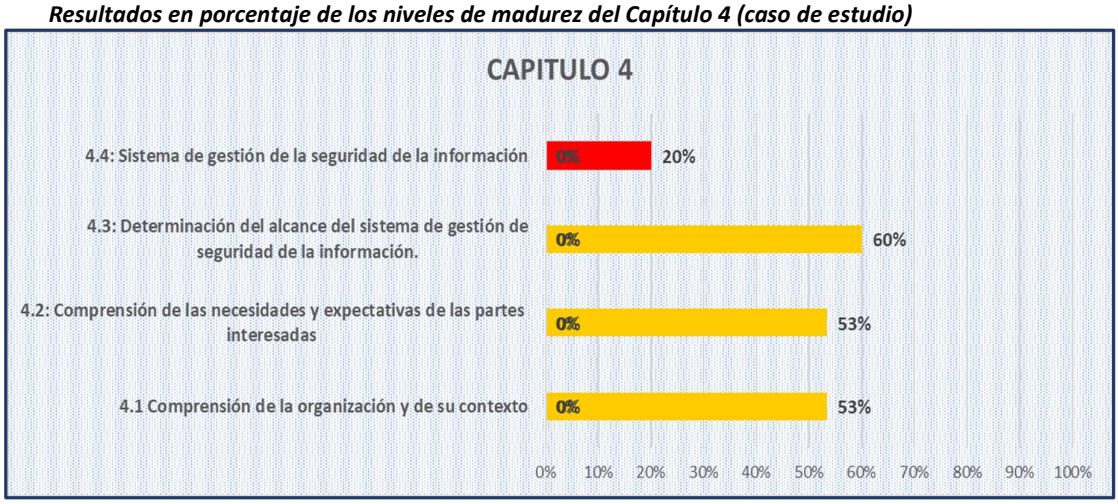
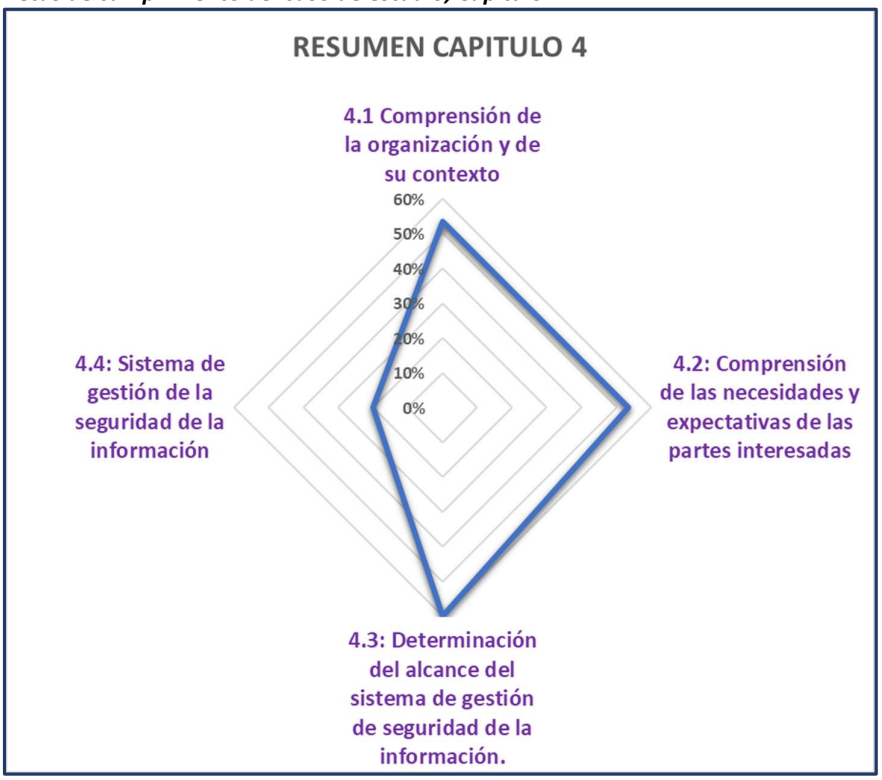


Figura 8.
Metas de cumplimiento del caso de estudio, Capítulo 4



Basándose en los lineamientos proporcionados por la norma ISO/IEC 27001:2022 la aplicabilidad y límites del SGSI (figuras 7 y 8), para el caso de estudio (DC-UCE) estarán determinados por los siguientes parámetros, las partes interesadas identificadas en el caso de estudio específico son:

- Proveedores de Servicio, por ejemplo, Servicio de Internet de CEDIA.
- Usuarios Internos, estudiantes, docentes y personal administrativo.
- Empresas con las que se están estableciendo la base de los proyectos de renovación tecnológica

Con respecto a la "Evaluación de riesgos de seguridad de la información", que incluye la identificación de dependencias de terceros, se han identificado algunas dependencias de terceros, como proveedores de servicios de internet y contratos con fabricantes (smartnet), lo cual es un paso importante en el cumplimiento de la norma. Sin embargo, el hecho de que no haya una documentación formal de esta evaluación de dependencia de terceros afecta el nivel de cumplimiento. La documentación es crucial en ISO 27001, ya que ayuda a garantizar la consistencia, la transparencia y la trazabilidad de los procesos de seguridad de la información.

El puntaje de 60% (caso de estudio DC-UCE) sugiere que hay un esfuerzo inicial en la identificación de dependencias de terceros, pero falta completar la documentación requerida para formalizar y asegurar adecuadamente este proceso. Para poder cumplir con este indicador, se recomendaría desarrollar y mantener una documentación clara y completa que detalle las evaluaciones de dependencia de terceros, incluyendo los criterios utilizados, los resultados obtenidos y cualquier acción tomada para mitigar los riesgos identificados.

Con respecto a la "Gestión de riesgos de seguridad de la información", este es un aspecto crítico en el cumplimiento de la norma, ya que implica la identificación, evaluación y tratamiento de los riesgos de seguridad de la información. Al no existir una implementación de la norma, es comprensible que el puntaje para este punto sea bajo (20%). Sin una implementación de la norma, es poco probable que exista una gestión adecuada de los riesgos de seguridad de la información según los estándares de la ISO 27001.

Para mejorar este aspecto, es necesario iniciar un análisis exhaustivo de los riesgos de seguridad a los que se enfrenta la organización, establecer controles y medidas adecuadas para mitigar estos riesgos, y documentar todo el proceso de gestión de riesgos de seguridad de la información de acuerdo con los requisitos de la norma. Es importante destacar que la implementación de la norma ISO 27001 es un proceso que requiere compromiso, recursos y tiempo, pero puede proporcionar importantes beneficios en términos de mejora de la seguridad de la información y la gestión de riesgos en la organización.

5. LIDERAZGO Y COMPROMISO

Figura 9.
Resultados en porcentaje de los niveles de madurez del Capítulo 5 (caso de estudio)

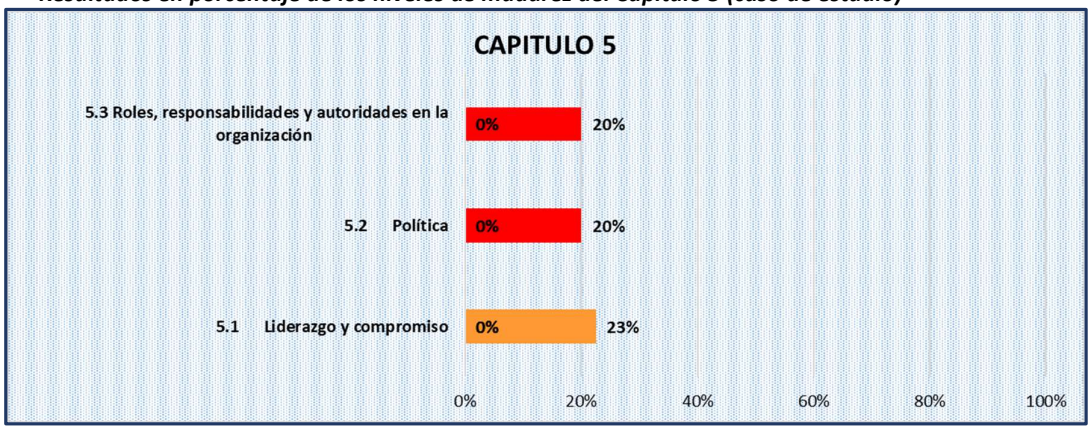
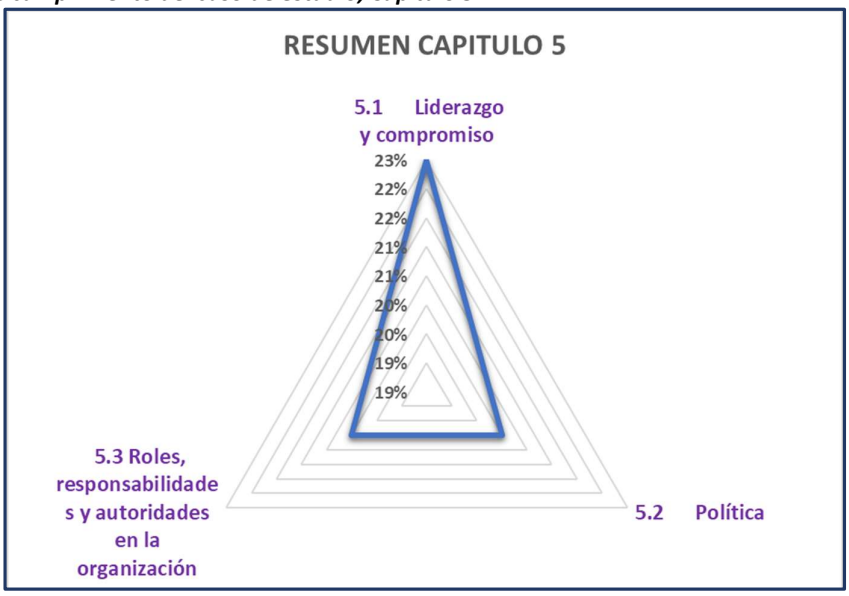


Figura 10.

Metas de cumplimiento del caso de estudio, Capítulo 5



Basado en los resultados obtenidos (figuras 9 y 10) del nivel de madurez del cumplimiento de las políticas de seguridad según la norma ISO 27001, se observa que la UCE carece de una definición formal de la "Política de Seguridad de la Información". Aunque se realiza cierta difusión y sensibilización en este ámbito, esta actividad no cumple con los estándares formales requeridos por la norma ISO 27001. En tal sentido se asigna una puntuación de 40% a esta área debido a los esfuerzos de sensibilización, pero es importante destacar que no existe una política formal y consistente.

También resalta que no se ha establecido una Política de Seguridad de la Información de manera formal en la institución. Esta política no ha sido aprobada por las autoridades pertinentes, lo que representa una brecha significativa en el cumplimiento de la norma ISO 27001 en esta área. Importante resaltar que no se ha designado un responsable específico de la Seguridad de la Información, aunque el área de infraestructura se encarga de los activos descritos en el alcance, los procedimientos no se ajustan a un Sistema de Gestión de Seguridad de la Información (SGSI), lo que refleja una falta de estructura y responsabilidad clara en este aspecto.

Finalmente, los resultados muestran que la Universidad Central del Ecuador enfrenta deficiencias significativas en cuanto al cumplimiento de las políticas de seguridad según la norma ISO 27001, especialmente en lo que respecta al liderazgo, la definición de políticas y la asignación de roles específicos en la gestión de la seguridad de la información. Estas áreas requieren una atención inmediata y acciones correctivas para mejorar el nivel de madurez del cumplimiento de la seguridad de la información en la organización.

6. PLANIFICACIÓN

Figura 11.

Resultados en porcentaje de los niveles de madurez del Capítulo 6 (caso de estudio)

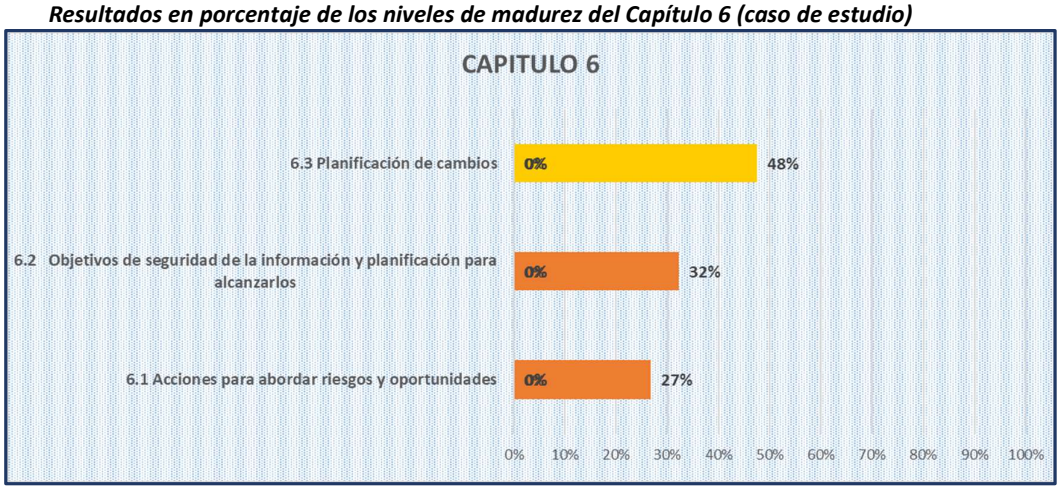
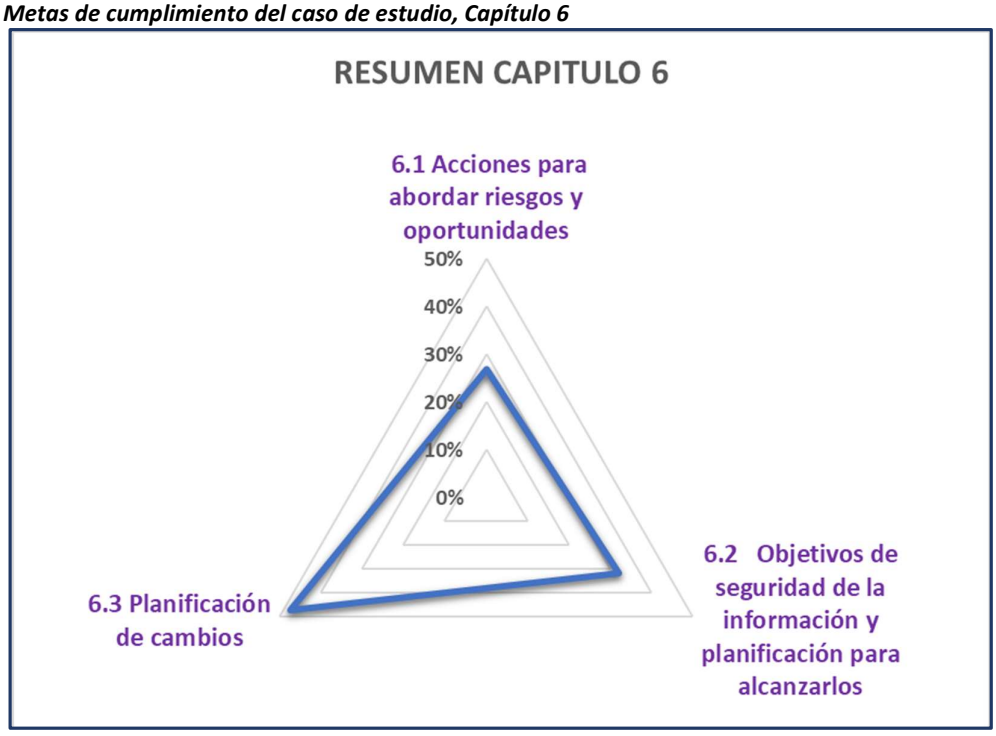


Figura 12.

Metas de cumplimiento del caso de estudio, Capítulo 6



El análisis del nivel de madurez del cumplimiento de las políticas de seguridad (figuras 12 y 13) según la norma ISO 27001 revela varios puntos críticos. En cuanto a las acciones para tratar riesgos y oportunidades, se ha alcanzado un 27% de cumplimiento debido a la implementación parcial de medidas de seguridad y una medición de incidentes relativamente efectiva. Sin embargo, la ausencia de un procedimiento formal de evaluación de riesgos es una limitación

importante. A pesar de identificar la mayoría de los riesgos y tomar medidas para abordarlos, la falta de procedimientos documentados según la norma ISO 27001 es una brecha significativa en el cumplimiento de los requisitos.

La medición de objetivos de seguridad de la información y los planes para alcanzarlos obtuvo un resultado del 32%, reflejando actividad en esta área. Sin embargo, la falta de objetivos alineados con un Sistema de Gestión de Seguridad de la Información (SGSI) y la comunicación inadecuada de estos objetivos representan limitaciones clave. Las políticas documentadas requieren actualización para reflejar los estándares y requisitos actuales, mientras que la asignación de recursos para medidas de seguridad carece de alineación con el SGSI, lo que puede resultar en una distribución inadecuada de recursos.

En la planificación de cambios, la falta de documentación adecuada y la integración insuficiente con el SGSI conducen a una evaluación del proceso del 48%, comprometiendo la trazabilidad y la gestión coherente de los cambios. En resumen, se necesitan mejoras en la documentación, la alineación con la normativa y la integración con el SGSI en varias áreas evaluadas para fortalecer el cumplimiento de las políticas de seguridad de la información. Estas áreas deben abordarse mediante acciones correctivas para mejorar el nivel de madurez del cumplimiento en la organización.

7. SOPORTE

Figura 13.
Resultados en porcentaje de los niveles de madurez del Capítulo 7 (caso de estudio)

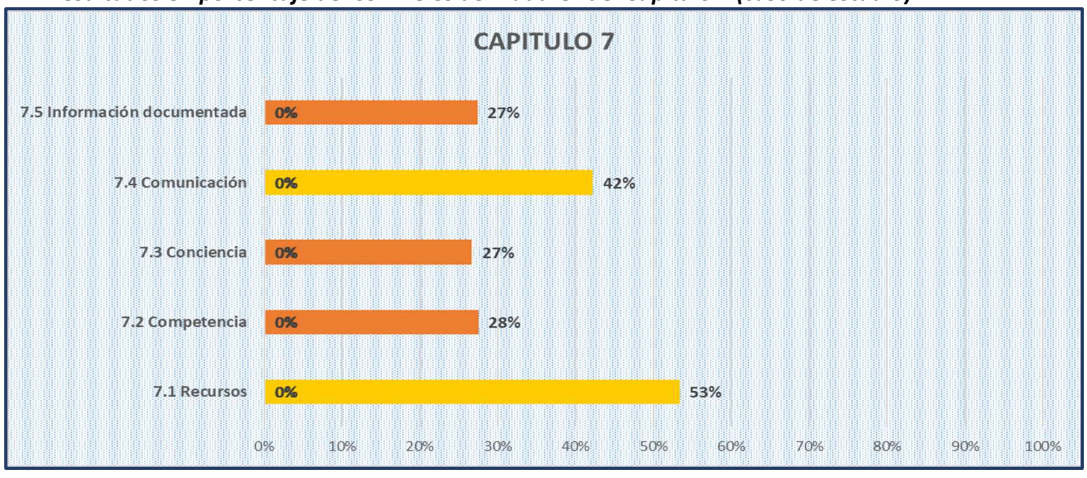
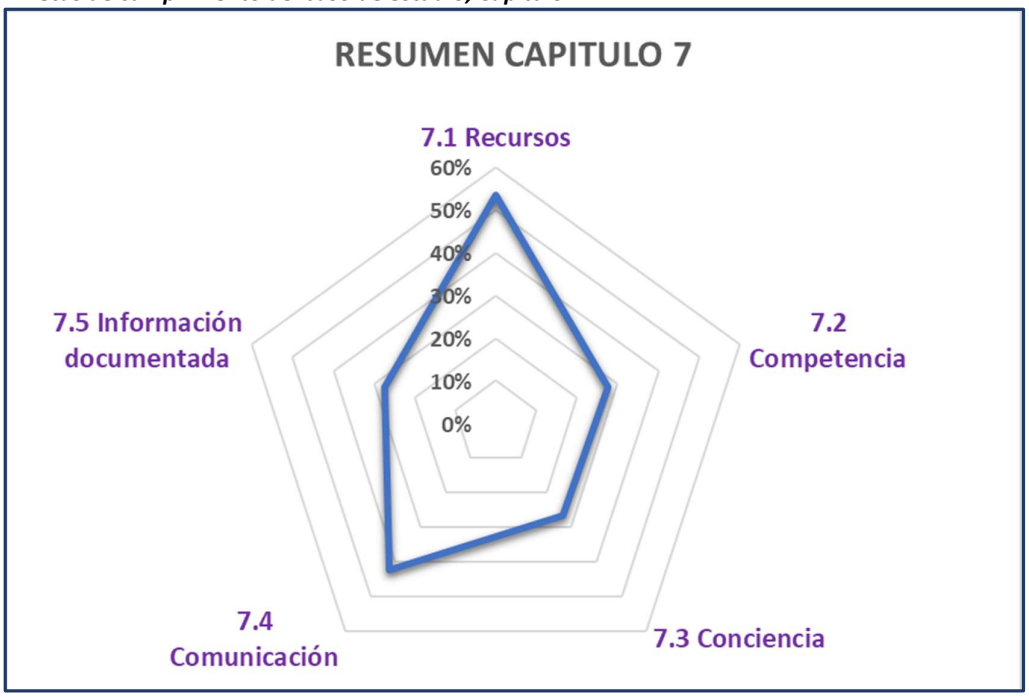


Figura 14.
Metas de cumplimiento del caso de estudio, Capítulo 7



En cuanto al apartado 7 de la norma ISO 27001 los resultados (figuras 13 y 14) manifiestan que el análisis de los recursos alcanza una ponderación del 53%. Si bien los recursos están bien definidos y documentados a través del proceso de aprobación de proyectos (PAP), su eficiencia se ve comprometida debido a la dependencia de otras áreas de la institución. Esto subraya la necesidad de mejorar la coordinación entre departamentos y optimizar el uso de los recursos asignados para mejorar la efectividad en seguridad de la información.

En cuanto a la competencia, se obtiene una calificación del 28%. Se identifica una falta de procedimientos definidos para la capacitación en seguridad de la información, lo que sugiere la necesidad de implementar un proceso estructurado. Además, la falta de evaluación de competencias y actualización continua del personal destaca la importancia de establecer un sistema de evaluación formal y brindar oportunidades de formación continua. La conciencia sobre la política de seguridad obtiene una calificación del 27%. La falta de definición de la política de seguridad impacta negativamente en la conciencia y participación de los empleados. Aunque se realizan sesiones de concientización, la falta de encuestas relacionadas con la conciencia y la participación en seguridad de la información limita la evaluación precisa de la efectividad de estas iniciativas.

En todo lo que se relaciona a la comunicación, se alcanza un cumplimiento del 42%. Se informa cualquier cambio a la comunidad universitaria, pero la falta de retroalimentación limita la efectividad del proceso. Se reconoce la necesidad de mejorar la identificación de partes interesadas y establecer canales de comunicación bidireccionales para mejorar la efectividad general de la comunicación. El análisis de la información documentada revela un nivel de madurez del 27%. Aunque existe información documentada, no cumple plenamente con los requisitos de la norma. Se necesita una mejora en el control de la información documentada, incluyendo un monitoreo efectivo de accesos y una mejor identificación de fuentes externas.

Los resultados muestran la importancia de mejorar la documentación, la capacitación, la conciencia sobre la política de seguridad, la comunicación y el control de la información para fortalecer el sistema de seguridad de la organización. Esto es fundamental para asegurar un entorno más seguro para los activos de información y cumplir con los estándares de seguridad necesarios.

8. OPERACIÓN

Figura 15.
Resultados en porcentaje de los niveles de madurez del Capítulo 8 (caso de estudio)

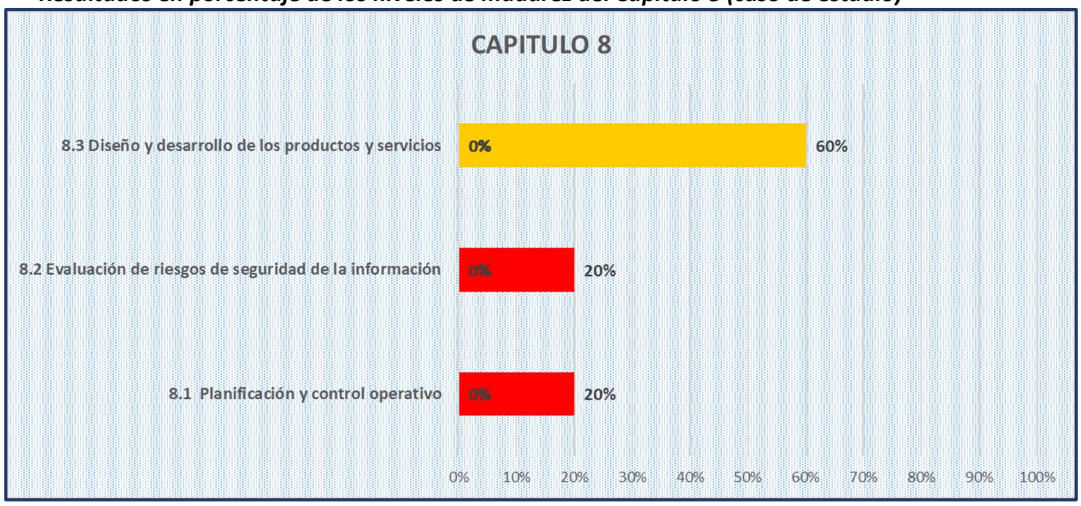
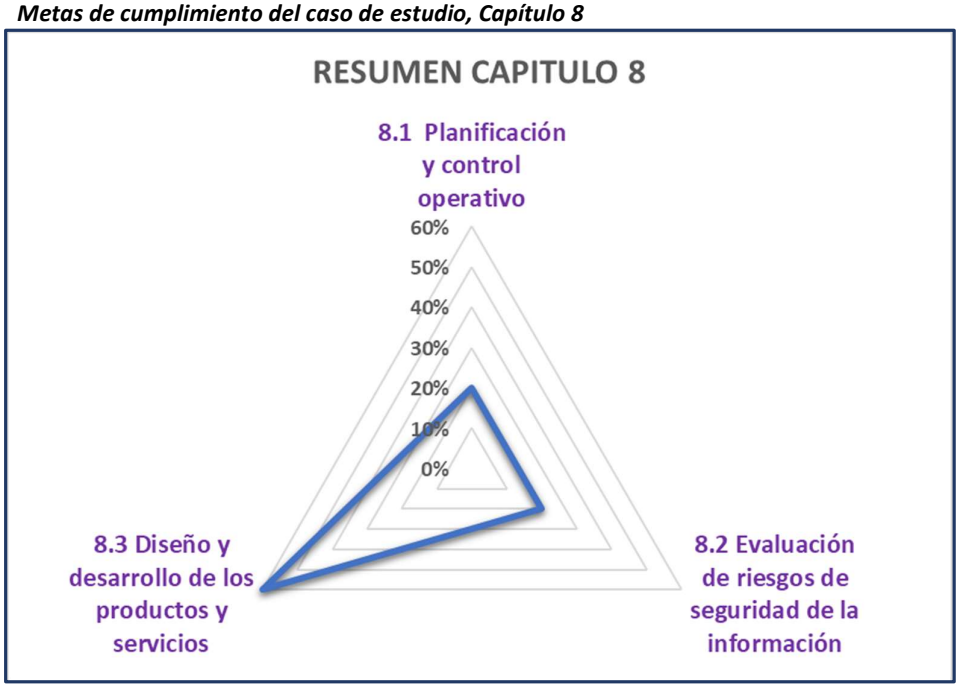


Figura 16.
Metas de cumplimiento del caso de estudio, Capítulo 8



En relación con la planificación y el control operativo (figuras 15 y 16), se observa una baja madurez con un puntaje del 20%. La falta de procesos alineados con los requisitos de la norma ISO 27001 representa un desafío significativo en términos de cumplimiento normativo y gestión efectiva de riesgos. Es crucial implementar procesos adecuados para mejorar el nivel de madurez en esta área clave de seguridad de la información. Respecto a la evaluación de riesgos de seguridad de la información, también se observa un bajo nivel de madurez con un puntaje del 20%. La falta de evaluaciones de riesgos efectivas puede exponer a la organización a amenazas significativas de seguridad de la información. Es fundamental implementar procesos adecuados de evaluación de riesgos que cumplan con los estándares requeridos por la norma ISO 27001.

En cuanto a la planificación y el control operacional, se observa una práctica aceptable con un puntaje del 60%. Aunque se aplican correctivos ante brechas de seguridad y se registra la información relacionada con estos eventos, estas acciones no están totalmente alineadas con los requisitos específicos de la norma ISO 27001. Sin embargo, la existencia de una base de datos de eventos registrados constituye una medida positiva para evitar problemas futuros. Para el diseño y desarrollo de productos y servicios, se ha alcanzado un puntaje aceptable. Aunque se aplican correctivos ante brechas de seguridad identificadas y se lleva a cabo un registro

exhaustivo de estos eventos, es importante reconocer que estas prácticas no cumplen completamente con los estándares establecidos por la norma ISO 27001.

El desenlace de este capítulo muestra que la planificación y el control operativo revelan cierto nivel de madurez, el control operativo y la evaluación de riesgos de seguridad de la información presentan deficiencias importantes que necesitan ser abordadas urgentemente para mejorar el cumplimiento normativo y garantizar la seguridad de la información de la organización.

9. EVALUACIÓN DEL DESEMPEÑO

Figura 17.
Resultados en porcentaje de los niveles de madurez del Capítulo 9 (caso de estudio)

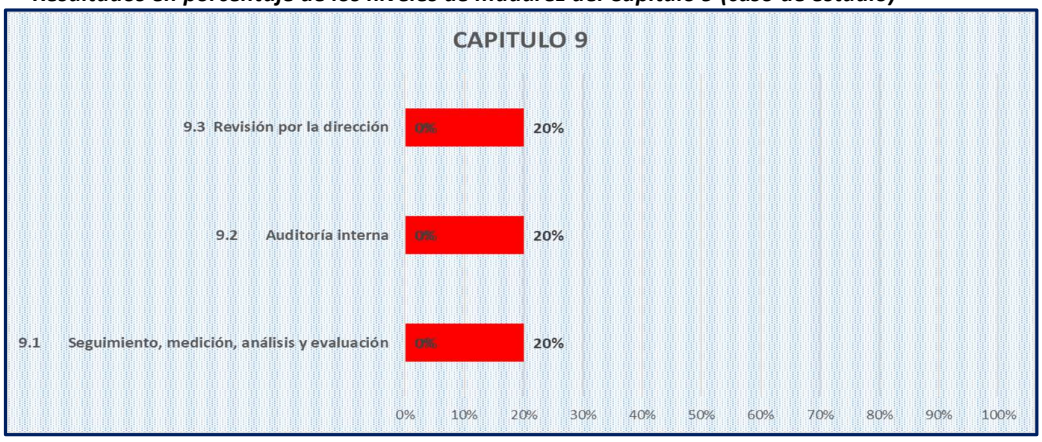
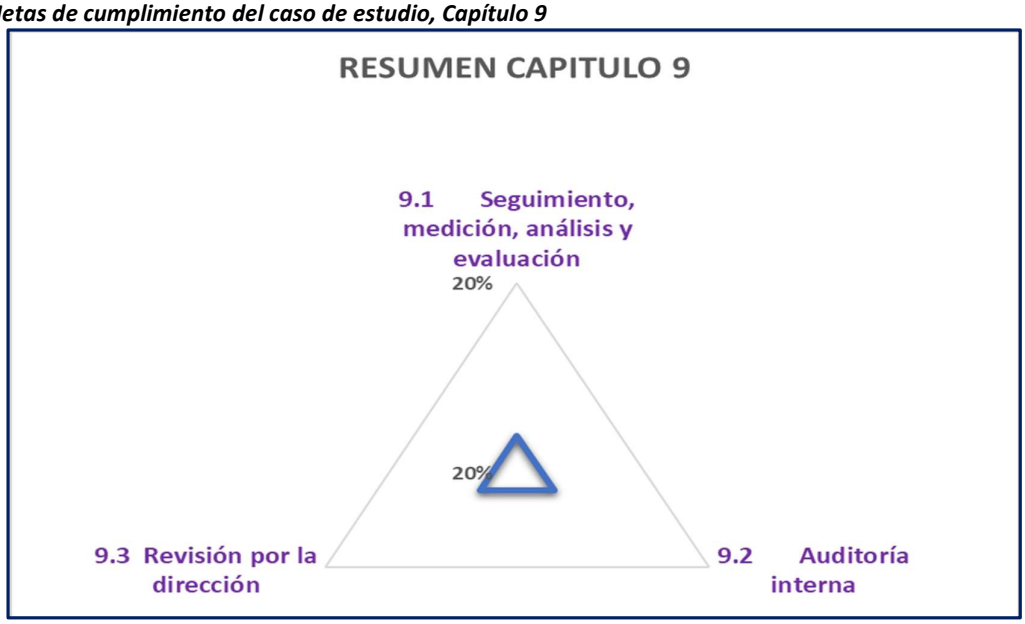


Figura 18.
Metas de cumplimiento del caso de estudio, Capítulo 9



En cuanto a la Evaluación del desempeño los resultados obtenidos (figuras 17 y 18) exponen, el seguimiento, medición, análisis y evaluación con un resultado del 20%, reflejando una baja madurez debido a la falta de implementación de un plan de tratamiento de riesgos en la universidad. Esta carencia impide a la organización identificar, evaluar y tratar los riesgos de seguridad de la información de manera sistemática y efectiva, comprometiendo su capacidad para monitorear, medir, analizar y evaluar el desempeño en seguridad de la información. Es esencial desarrollar e implementar un plan de tratamiento de riesgos que cumpla con los estándares de la norma ISO 27001 para mejorar el nivel de madurez en esta área y garantizar la protección adecuada de la información sensible.

En cuanto a la Auditoría Interna, se observa una baja madurez con un cumplimiento del 20% debido a la falta de registros de las auditorías internas realizadas en la universidad. Esta carencia limita la capacidad de la organización para evaluar de manera sistemática y regular el cumplimiento de los controles de seguridad de la información y para identificar áreas potenciales de mejora.

La revisión por la dirección donde la universidad muestra una baja madurez en este aspecto, con un puntaje del 20%. La ausencia de una política formal para llevar a cabo revisiones por la dirección limita la capacidad de la organización para evaluar de manera sistemática y regular la efectividad del sistema de gestión de seguridad de la información y tomar decisiones informadas sobre posibles mejoras. Es esencial desarrollar e implementar una política de revisión por la dirección que cumpla con los requisitos de la norma ISO 27001 para mejorar el nivel de madurez en esta área y garantizar la eficacia continua del sistema de gestión de seguridad de la información.

Es fundamental establecer e implementar un programa sólido y periódico de auditoría interna que cumpla con los requisitos de la norma ISO 27001 para mejorar el nivel de madurez en esta área y garantizar la efectividad de los controles de seguridad de la información. Tambien hay que señalar que la falta de una política de revisión por la dirección refleja una baja madurez en la capacidad de la universidad para evaluar y mejorar continuamente su sistema de gestión de seguridad de la información. Es necesario establecer una política formal de revisión por la dirección para mejorar la gestión de la seguridad de la información y cumplir con los requisitos de la norma ISO 27001.

10. MEJORA

Figura 19
Resultados en porcentaje de los niveles de madurez del Capítulo 10 (caso de estudio)

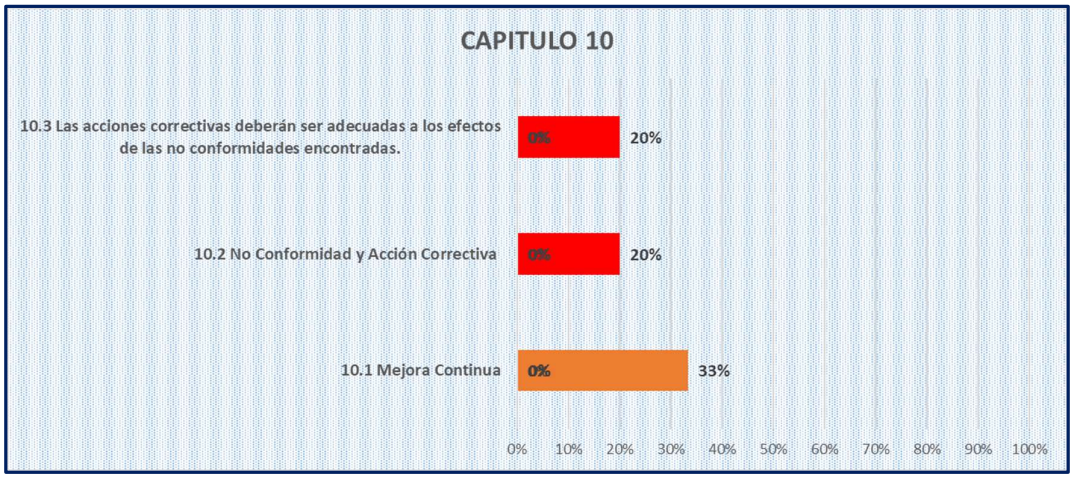
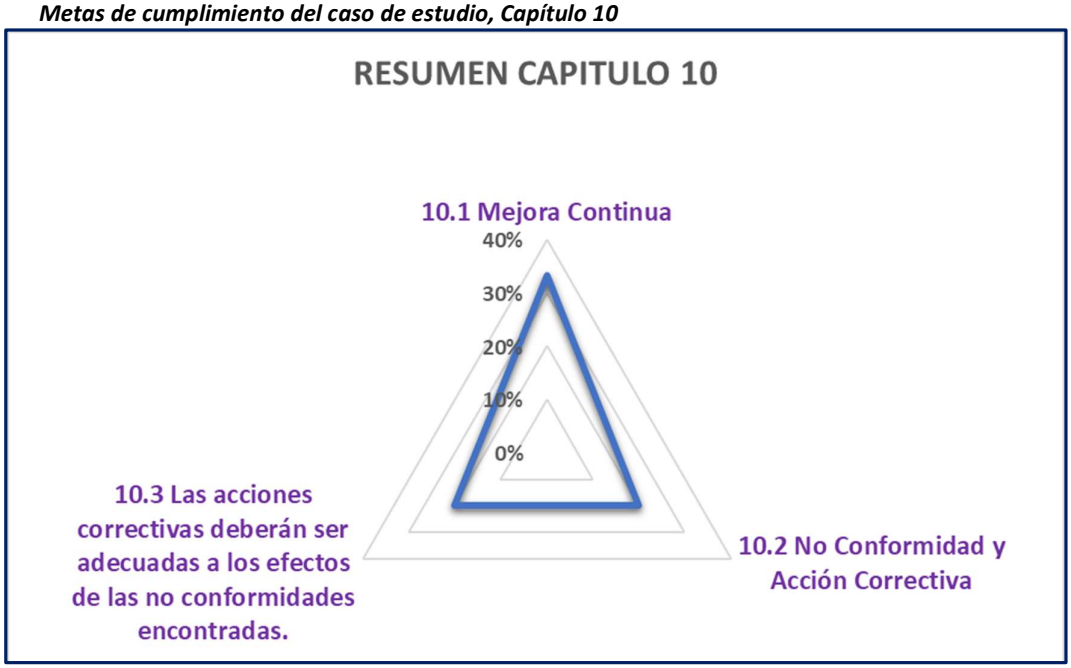


Figura 20
Metas de cumplimiento del caso de estudio, Capítulo 10



En cuanto a la mejora continua (figuras 19 y 20), la universidad alcanza una madurez del 33%, destacando su capacidad para identificar áreas de mejora, lo cual refleja un compromiso positivo con la mejora continua en seguridad de la información. Sin embargo, la falta de implementación y evaluación conforme a normativas establecidas limita la efectividad de este proceso. Es esencial desarrollar e implementar un proceso formal que cumpla con los requisitos de la norma

ISO 27001 para evaluar y abordar sistemáticamente las áreas de mejora identificadas, asegurando una mejora continua efectiva en el sistema de gestión de seguridad de la información.

En cuanto a la No Conformidad y Acción Correctiva, con una madurez del 20%, la universidad muestra una baja madurez debido a la falta de implementación de la normativa relacionada con la no conformidad y acción correctiva. Esto compromete su capacidad para identificar, registrar y abordar adecuadamente las no conformidades en el sistema de gestión de seguridad de la información. Es urgente implementar medidas adecuadas para abordar las no conformidades y llevar a cabo acciones correctivas, según lo requiere la norma ISO 27001.

En relación con las acciones correctivas para no conformidades, también con una madurez del 20%, la universidad muestra un bajo discernimiento debido a la falta de implementación de la normativa relacionada con la acción correctiva para abordar las no conformidades encontradas. Esta falta de acción correctiva representa un riesgo significativo para la seguridad de la información de la institución. Es crucial implementar medidas para abordar estas deficiencias y mejorar la capacidad de la universidad para identificar, abordar y corregir las no conformidades de manera efectiva, garantizando un sistema de gestión de seguridad de la información sólido y robusto.

Los resultados de la evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador, se resumen en las figuras 21 y 22.

Figura 21
Resultados en porcentaje de los niveles de madurez de los capítulos (caso de estudio)

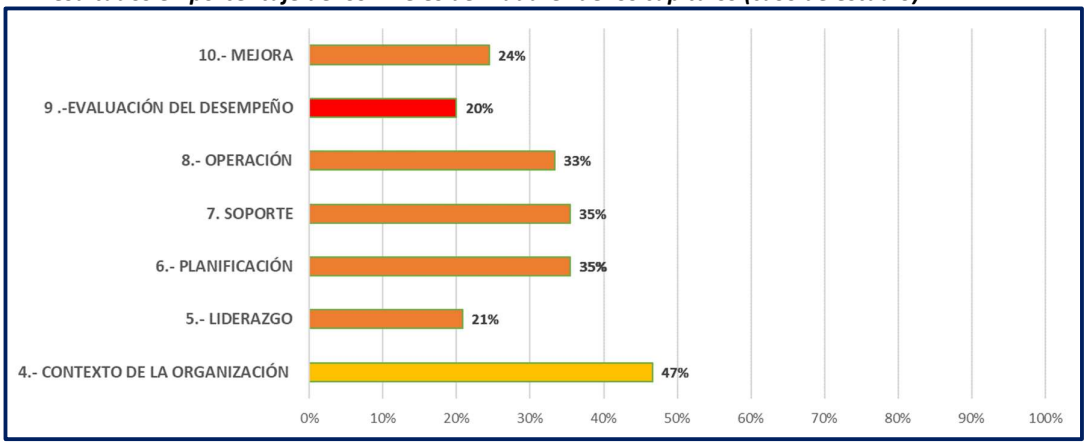
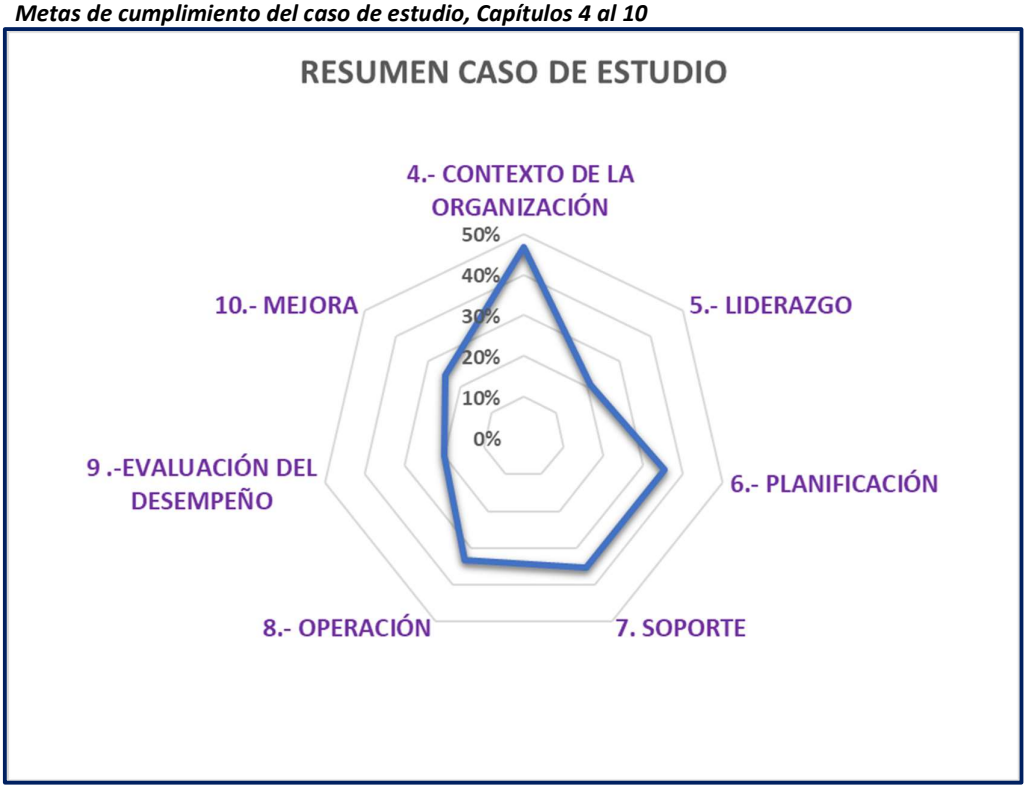


Figura 22
Metas de cumplimiento del caso de estudio, Capítulos 4 al 10



1. **Contexto de la organización (47%):** Este porcentaje indica un nivel moderado de madurez en comprender el entorno en el que opera la Universidad Central del Ecuador en términos de seguridad de la información. Sin embargo, aún hay margen para mejorar la comprensión de los factores internos y externos que pueden afectar a la seguridad de la información de la institución.
2. **Liderazgo (21%):** El bajo puntaje en liderazgo sugiere que puede haber deficiencias en el compromiso y la participación de la alta dirección en el establecimiento de una cultura de seguridad de la información sólida. Se necesita un mayor liderazgo para promover la importancia de la seguridad de la información en todos los niveles de la organización.
3. **Planificación (35%):** Aunque este puntaje muestra un nivel moderado de madurez en la planificación de la seguridad de la información, aún hay áreas que requieren atención. Es crucial desarrollar planes sólidos para gestionar y mitigar los riesgos de seguridad de la información de manera proactiva.
4. **Soporte (35%):** Un nivel moderado de madurez en el soporte indica que se han establecido algunos recursos y procesos para respaldar la implementación de medidas de seguridad de la información. Sin embargo, es importante fortalecer estos recursos y procesos para garantizar un soporte efectivo a largo plazo.

5. **Operación (33%):** Este puntaje sugiere que la ejecución de las operaciones relacionadas con la seguridad de la información puede ser inconsistente o no estar completamente alineada con los estándares de la norma ISO 27001. Se necesitan mejoras en la implementación de controles y procedimientos operativos para garantizar la seguridad de la información de manera efectiva.
6. **Evaluación del desempeño (20%):** El bajo puntaje en evaluación del desempeño indica que puede haber deficiencias en la medición y análisis del rendimiento de los controles de seguridad de la información. Es crucial implementar procesos de evaluación sólidos para identificar áreas de mejora y tomar medidas correctivas según sea necesario.
7. **Mejora (24%):** Un puntaje relativamente bajo en mejora sugiere que puede haber limitaciones en la capacidad de la universidad para identificar y abordar oportunidades de mejora en su SGSI de manera efectiva. Se necesitan acciones correctivas y procesos de mejora continua más sólidos para fortalecer el SGSI.

En resumen, mientras que la Universidad Central del Ecuador ha logrado cierto nivel de madurez en algunas áreas de su SGSI, como el contexto de la organización, la planificación y el soporte, aún enfrenta desafíos significativos en áreas clave como el liderazgo, la evaluación del desempeño y la mejora. Es fundamental abordar estas áreas de mejora para garantizar la efectividad y la robustez del SGSI en la institución.

CONCLUSIONES

La herramienta de evaluación basada en la norma ISO 27001 representa un avance significativo en la seguridad de la información para el centro de datos de la Universidad Central del Ecuador como institución de educación superior pública. Al adherirse a los estándares de la ISO 27001, se establece un marco objetivo para medir el nivel de cumplimiento de políticas de seguridad. Esta herramienta ofrece una visión clara del estado de seguridad actual, identificando áreas de mejora y fortaleciendo las prácticas de protección de datos.

El diagnóstico del estado actual de las políticas de seguridad de la información en el Centro de Datos de la Universidad Central del Ecuador revela tanto áreas de cumplimiento satisfactorio como oportunidades de mejora significativas. Se ha identificado un conjunto de políticas y procedimientos que proporcionan un sustento concreto para la protección de la información sensible, sin embargo, existen ciertas deficiencias y lagunas que deben abordarse para fortalecer la postura de seguridad en su totalidad.

El análisis del proceso de aplicación de políticas y normativas relacionadas con la seguridad de la información en el ámbito de las universidades públicas como es el caso de la UCE revela una evolución histórica significativa. A lo largo del tiempo, se ha observado un cambio hacia un enfoque más estructurado y proactivo en la gestión de la seguridad de la información, con la implementación de políticas y normativas más rigurosas y específicas. Este proceso ha sido impulsado por una mayor conciencia sobre los riesgos de seguridad, avances tecnológicos y regulaciones gubernamentales cada vez más estrictas.

El diseño de esta herramienta para evaluar y medir el nivel de madurez de cumplimiento de políticas en sistemas de gestión de seguridad, enfocado en el centro de datos de una universidad pública y con base en la norma ISO 27001, representa un paso crucial hacia la mejora continua de la seguridad de la información en este entorno. Al seguir los principios y directrices establecidos por esta norma, esta herramienta proporcionará un soporte objetivo para evaluar el grado de cumplimiento de las políticas de seguridad, identificando áreas de fortaleza y oportunidades de mejora.

La validación de la herramienta para establecer el nivel de cumplimiento de normativas de seguridad de la información en el Centro de Datos de la Universidad Central del Ecuador ha sido un paso fundamental para evaluar la postura actual de seguridad de la institución. Mediante el uso de esta herramienta, se ha obtenido una evaluación objetiva y estructurada del cumplimiento de las normativas, permitiendo identificar áreas de fortaleza y oportunidades de mejora en esta materia.

RECOMENDACIONES

La creación de una herramienta de evaluación basada en la norma ISO 27001 es decisivo para reforzar la seguridad de la información en el centro de datos de la Universidad Central del Ecuador y otras instituciones. Esta herramienta proporciona una metodología completa para evaluar el cumplimiento de las políticas de seguridad, identificar áreas de mejora y establecer acciones correctivas y preventivas según sea necesario.

En este sentido, se recomienda para el caso de estudio, el uso de este tipo de herramientas según las necesidades específicas de la institución lo que asegura su relevancia y utilidad práctica para fortalecer la seguridad. Al tener en cuenta las particularidades y desafíos propios de este entorno, se garantiza que la evaluación sea precisa y efectiva, lo que permite mejorar significativamente su postura de seguridad. En este sentido, se proponen las siguientes recomendaciones para el caso de estudio en concreto.

1. Promover la adopción y uso continuo de la herramienta de evaluación en temas de seguridad por parte de las instituciones de educación superior pública en nuestro país, mediante la realización de sesiones de capacitación y la difusión de material informativo sobre su importancia y beneficios.
2. Establecer un proceso de revisión y actualización periódica de la herramienta, con el fin de incorporar nuevos requisitos y controles de seguridad de la información en la universidad, así como adaptaciones necesarias en función de cambios en el entorno tecnológico y normativo.
3. Fomentar la colaboración y el intercambio de buenas prácticas entre las instituciones de educación superior tanto públicas como privadas, con el objetivo de enriquecer el conocimiento y la experiencia en materia de seguridad de la información de sus centros de datos. Esto puede facilitarse mediante la creación de comunidades de práctica o la organización de eventos y conferencias especializadas en estos temas.
4. Realizar auditorías periódicas y revisiones internas por medio del uso de este tipo de herramientas de evaluación, con el fin de valorar el progreso en materia de seguridad de la información y asegurar el cumplimiento continuo de las políticas y estándares establecidos dentro de la Universidad Central del Ecuador u otras instituciones.
5. Considerar la posibilidad de obtener certificaciones o acreditaciones externas en seguridad de la información, como la certificación ISO 27001, como un medio para validar y reconocer el compromiso de la Universidad Central del Ecuador con la protección de la información.

BIBLIOGRAFÍA

Aguilera, P. (2019). *Seguridad Informática.* Madrid, España: Editex S. A. Retrieved 12 de 02 de 2024, from https://books.google.com.ec/books?id=Mgvm3AYIT64C&printsec=copyright&hl=es#v=onepage&q&f=false

ANUIES. (11 de 2018). ESTADO ACTUAL DE LAS TECNOLOGÍAS DE. (Primera Edición). Ciudad de México, México: ANUIES. http://publicaciones.anuies.mx/pdfs/libros/Libro240.pdf

AWS. (2023). *Amazon Web Services*. Retrieved 17 de Octubre de 2023, from https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,cliente%20y%20cumplir%20la%20normativa.

AXENTIO. (1 de 4 de 2023). https://www.axentio.com/que-es-cpd/

Barros, B. C. (15 de 05 de 2020). *DIGIBUG.* (U. d. Granada, Ed.) https://doi.org/doi:10.30827/publicaciones.v50i2.13952

Briceño, E. V. (2021). *Seguridad de la Información.* 3Ciencias. https://doi.org/https://doi.org/10.17993/tics.2021.4

Centro Criptológico Nacional CCN-CERT. (14 de 02 de 2024). *CCN-CERT*. https://www.ccn-cert.cni.es/es/

CEPAL. (2021). *www.cepal.org.* https://www.cepal.org/sites/default/files/publication/files/46766/S2000991_es.pdf

CEPAL. (01 de 09 de 2024). *Biblioguías - Biblioteca de la CEPAL*. https://biblioguias.cepal.org/TIC/Infraestructura

CEPAL. (05 de 01 de 2024). *CEPAL.org*. https://biblioguias.cepal.org/c.php?g=495473&p=4398118

Check Point Software Technologies Ltd. (2024). *Check Point Software Technologies.* https://www.checkpoint.com/es/cyber-hub/cyber-security/what-is-data-center/data-center-threats-and-vulnerabilities/

DATA CENTER MARKET. (8 de 1 de 2024). *www.datacentermarket.es*. (L. Bonilla, Editor) https://www.datacentermarket.es/dcm-xl/por-que-es-importante-la-seguridad-fisica-de-un-data-center/

EcuaCERT. (2024). *EcuaCERT*. Retrieved 15 de Diciembre de 2023, from https://www.ecucert.gob.ec/centro-de-respuesta-a-incidentes-informaticos-del-ecuador/

García, A. M. (2023). https://burjcdigital.urjc.es/bitstream/handle/10115/23388/2022-23-ETSII-A-2059-2059037-a.garciamayo-MEMORIA.pdf?sequence=-1&isAllowed=y

García, A. M. (20 de 07 de 2023). BURJC DIGITAL. *SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS DE INTELIGENCIA ARTIFICIAL*. https://burjcdigital.urjc.es/bitstream/handle/10115/23388/2022-23-ETSII-A-2059-2059037-a.garciamayo-MEMORIA.pdf?sequence=-1&isAllowed=y

Google. (2024). *Google Cloud*. https://cloud.google.com/learn/what-is-iaas?hl=es

Hernández, C. (2022). Monitorización de Amenazas en Centros de Datos: Herramientas y Técnicas Avanzadas. *Conferencia Internacional sobre Seguridad Informática*, 30-38.

IBM. (2023). *www.ibm.com*. https://www.ibm.com/es-es/topics/identity-access-management

Kaspersky. (2024). *2024 AO Kaspersky Lab*. https://latam.kaspersky.com/resource-center/definitions/encryption

Medina Garzón, M. A. (30 de 01 de 2020). *Repositorio Institucional Universidad Estatal Francisco José de Caldas.* https://repository.udistrital.edu.co/bitstream/handle/11349/29845/VasquezRodriguezYiseth2020.pdf?sequence=1&isAllowed=y

Ministerio de Telecomunicaciones y de la Sociedad de la Información. (04 de 2020). *Gobierno Electrónico, GUÍA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.* Retrieved 2024, from https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

MINTEL. (26 de 05 de 2021). *www.telecomunicaciones.gob.ec.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2023/11/LOPDP-LEXIS.pdf

Naciones Unidas. (5 de 2018). *www.unjiu.org.* Retrieved 24 de 02 de 2024, from https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2018_5_spanish.pdf

Obama, J. (2022). *Universidad de Valladolid Repositorio Documental.* https://uvadoc.uva.es/handle/10324/57275

ODATA. (9 de 9 de 2022). *ODATACOLOCATION.COM*. (E. Andrade, Productor, y ODATA) https://odatacolocation.com/es/blog/infraestructura-del-data-center-el-corazon-tecnologico-de-cada-empresa/

Organización de los Estados Americanos (OEA). (2020). *www.oas.org.* (OEA, Ed.) https://www.oas.org/es/sms/cicte/docs/20200925-ESP-White-Paper-Educacion-en-Ciberseguridad.pdf

Organización Internacional de Normalización (ISO). (14 de 02 de 2024). *ISO Org*. https://www.iso.org/es/contents/data/standard/08/28/82875.html

Ortega, J. M. (2021). *CIBERSEGURIDAD Manual Práctico.* Ediciones Paraninfo. https://books.google.es/books?id=QsROEAAAQBAJ&lpg=PP1&hl=es&pg=PR4#v=onepage&q&f=false

Pacio, G. (2014). *Data centers hoy. Protección y administración de datos en la empresa.* Alpha Editorial. https://www.google.com.ec/books/edition/_/43xNDAAAQBAJ?hl=es&gbpv=1#pli=1

Pereyra, L. (2022). *Metodología de la investigación.* Klik. Retrieved 20 de 02 de 2024, from https://books.google.es/books?id=6e-KEAAAQBAJ&dq=m%C3%A9todolog%C3%ADa+de+la+investigacion&lr=lang_es&hl=es&source=gbs_navlinks_s

Ramirez, A. O. (2011). Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. *UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS, 16*(2), 56-66. file:///C:/Users/Ren%C3%A9%20Camacho/Downloads/Dialnet-GestionDeRiesgosTecnologicosBasadaEnISO31000EISO27-4797252.pdf

Red Hat. (04 de 08 de 2023). *Red Hat*. https://www.redhat.com/es/topics/cloud-native-apps/what-is-service-oriented-architecture

Secretaria de Educación Suerior, Ciencia, Tecnología e Innovación. (2020). *SENESCYT.* Retrieved 22 de 02 de 2024, from http://www.educacionsuperior.gob.ec/

Servicio Ecuatoriano de Normalización INEN. (2024). *www.normalizacion.gob.ec*. https://www.normalizacion.gob.ec/el-inen-fomenta-el-avance-tecnologico-a-traves-de-la-adopcion-de-normas-en-tecnologias-de-la-informacion-y-comunicacion/

SISSA Monitoring. (9 de 10 de 2023). Las 6 capas de seguridad en Data Centers: soluciones para garantizar una protección integral. https://www.linkedin.com/pulse/las-6-capas-de-seguridad-en-data-centers-soluciones-para-garantizar/?originalSubdomain=es

Sistema Oficial de Contratación Pública. (2015). *Sistema Oficial de Contratación Pública*. https://www.compraspublicas.gob.ec/ProcesoContratacion/compras/PC/informacionProcesoContratacion2.cpe?idSoliCompra=5gvD82LPxsCCF8NZTpTHFNFqzWHEWv5lUqCPy66L2q8,

Thales. (2024). *www.thalesgroup.com.*

Unión Internacional de Telecomunicaciones (UIT). (2024). *ITU*. https://www.itu.int/es/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx

Universidad Central del Ecuador. (2019). Estatuto Universidad Central del Ecuador. Quito, Pichincha, Ecuador. Retrieved 18 de 10 de 2023, from https://drive.google.com/file/d/1YYR1d-ryEwhTXl4TkJ6OOMeyPTujp09I/view

Universidad Central del Ecuador. (2024). *UCE*. https://reportes.uce.edu.ec/Academico/Estudiantes/Matriculados.aspx

VISTAZO. (26 de 4 de 2022). *Datacenters proponen un almacenamiento ágil y seguro*. https://www.vistazo.com/enfoque/datacenters-almacenamiento-agil-y-seguro-GH1669833

World Economic Forum. (2024). *World Economic Forum.* Retrieved 23 de 02 de 2024, from https://www.weforum.org/publications/global-risks-report-2024/

Zevallos, N. M. (02 de 2019). *Universidad Nacional Mayor de San Marcos, Facultad de Ingeniería de Sistemas e Informática. Lima, Perú.* https://core.ac.uk/download/pdf/304901839.pdf

ANEXOS

ANEXO 1

FORMATO DE ENCUESTA

UNIVERSIDAD TECNOLÓGICA ISRAEL

MAESTRÍA EN SEGURIDAD INFORMÁTICA

PROYECTO DE TITULACIÓN AL GRADO DE MAGISTER

Título del proyecto:

"Evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador"

ENCUESTA ANÓNIMA PARA ENCARGADOS DE LA ADMINISTRACIÓN DEL CENTRO DE DATOS RELACIONADO A LA POLITICA DE SEGURIDAD

OBJETIVO:

Elaborar un instrumento para medir la madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27000.

UNIVERSIDAD TECNOLÓGICA ISRAEL

1. ¿Su centro de datos cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI) implementado conforme a alguna norma existente y reconocida, describa brevemente su respuesta?

2. ¿Qué medidas de seguridad física (accesos a centro de datos, ubicación equipos, equipamiento eléctrico, aspectos ambientales, etc.) se han implementado en el centro de datos para proteger la infraestructura y los recursos críticos de información?

3. ¿su departamento realiza regularmente una evaluación de riesgos de seguridad de la información enfocado al centro de datos?

4. ¿Existe un proceso para la gestión de incidentes de seguridad de la información relacionados a eventos ocasionados en el centro de datos?

5. ¿su departamento realiza periódicamente auditorías internas para evaluar el cumplimiento de las políticas de seguridad de la información relacionadas al centro de datos?

6. ¿El personal responsable de la supervisión y mantenimiento del centro de datos recibe formación y capacitación regular sobre seguridad de la información y políticas que deberían implementarse para minimizar riesgos de seguridad?

7. ¿Se han establecido y documentado políticas y procedimientos claros para el control de acceso físico y/o lógico relacionado al normal funcionamiento del centro de datos?

8. ¿Se realizan frecuentemente pruebas de seguridad, tales como: pruebas de penetración simulacros de incidentes, gestión de identidad, protección y detección de incendios entre otras en el centro de datos, que permita identificar posibles brechas de seguridad?

9. ¿Existe un proceso formal de mejora continua para fortalecer la seguridad de la información en el centro de datos, basado en los resultados de las evaluaciones y auditorías previas realizadas?

ANEXO 2

RESULTADOS DE ENCUESTA

ENCUESTA ANÓNIMA DIRIGIDA PARA ENCARGADOS DE LA ADMINISTRACIÓN DEL CENTRO DE DATOS

	Pregunta 01	Pregunta 02	Pregunta 03	Pregunta 04	Pregunta 05	Pregunta 06	Pregunta 07	Pregunta 08	Pregunta 09
	¿Su centro de datos cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI) implementado conforme a alguna norma existente y reconocida, describa brevemente su respuesta?	¿Qué medidas de seguridad física (accesos a centro de datos, ubicación equipos, equipamiento eléctrico, aspectos ambientales, etc.) se han implementado en el centro de datos para proteger la infraestructura y los recursos críticos de información?	¿Su departamento realiza regularmente una evaluación de riesgos de seguridad de la información enfocado al centro de datos?	¿Existe un proceso para la gestión de incidentes de seguridad de la información relacionados a eventos ocasionados en el centro de datos?	¿Su departamento realiza periódicamente auditorías internas para evaluar el cumplimiento de las políticas de seguridad de la información relacionadas al centro de datos?	¿El personal responsable de la supervisión y mantenimiento del centro de datos recibe formación y capacitación regular sobre seguridad de la información y políticas que deberían implementarse para minimizar riesgos de seguridad?	¿Se han establecido y documentado políticas y procedimientos claros para el control de acceso físico y/o lógico relacionado al normal funcionamiento del centro de datos?	¿Se realizan frecuentemente pruebas de seguridad, tales como: pruebas de penetración simulacros de incidentes, gestión de identidad, protección y detección de incendios entre otras en el centro de datos, que permita identificar posibles brechas de seguridad?	¿Existe un proceso formal de mejora continua para fortalecer la seguridad de la información en el centro de datos, basado en los resultados de las evaluaciones y auditorías previas realizadas?
Funcionario 01	No cuenta con SGSI aprobado por algun comité o autoridad	En el Centro de Datos donde labore, se tienen accesos de tipo biométrico solo para cuatro funcionarios y redundancia a nivel eléctrico, con lo que respecta a seguridad física.	No se realiza evalauciones peródicas, cuando se va a hacer alguna implementacion dentro del centro se realiza ese revisión de riesgos sin dejar documentado	No hay un proceso definido, por el proveedor del servicio de internet se tiene alertas de vulnerabilidades de los sistemas o incidentes	No hay auditorias internas periódicas sobe el cumplimiento de políticas de SGSI	No hay programas de capacitación o formacion en temas de segruirad informática, el aprendizaje es autónomo	Ciertos procesos se encuentran documentados en sus políticas para el acceso físico y/o logico del DC	No se realizan este tipo de test con regularidad, se los ejecuta de vez en cuando con la ayuda del provedor del servicio de inetrnet sin responder a una planificación	No se tiene un procedimiento formal, se realizan correctivos o mejoras como respuesta a un incidente o evento sin responder a un plan
Funcionario 02	Lamentablemente en el Centro de Datos donde laboro no se encuentra implementado un SGSI, pero se tiene proyecto implementarlo.	acceso biométrico de doble factor, respaldo y redundancia eléctrica, malla de tierra, sistema anti-incendios.	Lamentablemente no se ha realizado un procedimiento con lo que respecta a la evaluación de riesgos de la seguridad de la información.	Existe un procedimiento, pero no está definido como una política a nivel de seguridad de la información.	No se han realizado auditorías internas.	Debido a problemas presupuestarios, la organización no ha proporcionado recursos para capacitación en los últimos cuatro años.	Existen algunos procedimientos documentados, sin embargo, no existe una política formal en cuanto a control de acceso físico y/o lógico.	No se realizan estos procedimientos con regularidad.	No se tiene un procedimiento formal, sin embargo, si se ha considerado la implementación de procesos de mejora continua.
Funcionario 03	Se cuenta parcialmente, debido a que hay documentación pero no formalmente aprobada por un comité de seguridad	Control de acceso biométrico, videovigilancia mediante cámaras ubicadas estratégicamente, protección antiincendios, protección sobrevoltajes y caídas de tensión mediante UPS y continuidad de energía con generador eléctrico	Solo cuando existen nuevas adquisiciones de hardware/software se evalúa la seguridad de la información, no periódicamente	Existe un proceso externo, a través del proveedor de internet que con sus herramientas externas controla la red pública, evaluando las vulnerabilidades y notificando cuando existen correcciones a efectuarse dentro de la administración de red y servidores	No existen auditorías internas, unicamente se realiza protección de los sistemas con los medios con los que se cuenta	No se cuenta con formación y capacitación permanente relacionada a seguridad de la información	No existe documentación formal y aprobada para el acceso físico/lógico al centro de datos	A través del proveedor de internet se cuenta con hacking ético periódico y notificaciones de vulnerabilidades activas en la red pública de la institución	No existe ningún proceso para la mejora de la seguridad de la información
Funcionario 04	No, el centro de datos pese a tener políticas que den una cierta seguridad no cuenta con un sistema de gestión, ni tampoco se apega a una norma específica, más bien se diría una adopción de alguna medida de seguridad por si acaso.	Se tiene ciertos elementos físicos de seguridad como control de acceso biométrico, sensores de humo, cámaras sistemas contra incendios, energía regulada, sistema de enfriamiento y con un generador eléctrico, pero no se tiene contratos de mantenimiento vigentes de estos equipos.	Si, se evalúan riesgos de manera oral sin dejar documentado. Estas evaluaciones nos dejan en el mismo punto por no contar con una gestión ante las autoridades.	No existe, la gestión de incidentes no tiene un plan o un proceso definido, se actúa o se toma acciones de acuerdo al evento lo que ocasiona mal estar, sin embargo, hay ciertos incidentes que son conocidos y en cierta forma se conocen y se actúa para responder y retomar servicios en el menor tiempo posible.	No se tiene una política definida, existe un área de auditoría interna que está en constates auditorías a los sistemas y a otras áreas más, no hay una enfocada en el centro de datos de la institución	No, uno de los mayores problemas a nivel del sector público es la falta de capacitación dentro de la organización, existen cursos que se dan por convenio, pero no es accesible o no es llamativo para todos.	Existen controles de acceso a nivel físico y lógico hacia la infraestructura dentro del centro de datos.	No existen pruebas frecuentes, se han realizado, pero sin base a una planificación	No hay un proceso formal de mejora. Es de suma importancia trabajar en este aspecto, es importante visibilizar este tema a las autoridades y así tomar acciones correctivas.

ANEXO 3

VALIDACIÓN DE EXPERTOS

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: "Evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador".

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Alex Eduardo Caizapanta Gonzalez, MSc.

Título obtenido
Máster Universitario en Seguridad Informática / Internal Auditor en la Norma ISO27001:2022
Cédula de Identidad
1714940671
E- mail
aecaizapanta@uce.edu.ec
Institución de Trabajo
Universidad Central del Ecuador
Cargo
Analista de Tecnologías de la Información y Comunicación
Años de experiencia en el área
10 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: "Evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador".

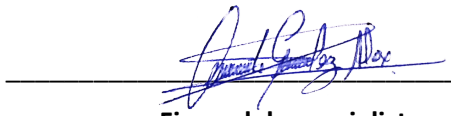
Indicador	*Descripción*	Muy adecuado	Bastante Adecuado	Adecuado	Poco adecuado	Inadecuado
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*	*X*				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		***X***			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*		***X***			
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***X***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*	***X***				
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	*X*				
Total						

Observaciones: La propuesta del proyecto se considera fundamental para una evaluación e implementación efectiva de cada uno de los parámetros correspondientes a un sistema de gestión de la Seguridad de la Información en la Institución según la norma ISO 27001:2022.

Recomendaciones

Ninguna, estoy de acuerdo con la plantilla y la metodología de evaluación planteada en el proyecto.

Lugar, fecha de validación: Quito, 6 de marzo de 2024



Firma del especialista

INSTRUMENTO DE VALIDACIÓN

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

INSTRUMENTO PARA VALIDACIÓN DE LA PROPUESTA

Estimado colega:

Se solicita su valiosa cooperación para evaluar la siguiente propuesta del proyecto de titulación: "Evaluación de nivel de madurez de cumplimiento de políticas en Sistemas de Gestión de la Seguridad de la Información en centros de datos de instituciones de educación superior, basado en la norma ISO 27001, Caso de estudio: Universidad Central del Ecuador".

Sus criterios son de suma importancia para la realización de este trabajo, por lo que se le pide brinde su cooperación contestando las preguntas que se realizan a continuación.

Datos informativos

Validado por: Ing. Francisco Xavier Valverde Alulema

Título obtenido
PhD. Informática
Cédula de Identidad
1712156684
E- mail
fvalverde@uce.edu.ec
Institución de Trabajo
Universidad Central del Ecuador
Cargo
Docente del Área de Informática de la Facultad de Ciencias Económicas
Años de experiencia en el área
15 años

Instructivo:

- Responda cada criterio con la máxima sincera del caso;
- Revisar, observar y analizar la propuesta del proyecto de titulación; y,
- Coloque **una X** en cada indicador, tomando en cuenta que Muy adecuado equivale a 5, Bastante Adecuado equivale a 4, Adecuado equivale a 3, Poco Adecuado equivale a 2 e Inadecuado equivale a 1.

Tema: Propuesta de automatización de procesos administrativos en una Institución de Educación Superior mediante el uso de Inteligencia Artificial.

Indicador	*Descripción*	**Muy adecuado**	**Bastante Adecuado**	**Adecuado**	**Poco adecuado**	**Inadecuado**
Impacto	*El alcance que tendrá la propuesta y su representatividad en la generación de valor*		*X*			
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*			***X***		
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	***X***				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	***X***				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	***X***				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*			***X***		
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*		*X*			
Total						

Observaciones: En la actualidad la aplicación de normas de seguridad que permitan brindar protección a los datos de cualquier organización, siempre será un aporte importante y de alta prioridad a implementarse, las tecnologías de la información vinieron a quedarse, los datos no dejaran de ser digitales y por tanto se requieren iniciativas que apoyen a cuidar lo más importante que en la actualidad tienen las organizaciones y en particular las universidades sean estas públicas o privadas y eso tan importante es su información

Recomendaciones

Ir mejorando y complementando el aporte con nuevos estudios que integren nuevos aspectos no considerados en la propuesta, de esta forma en el tiempo se irá consolidando un instrumento importante y relevante que puede ser usado por cualquier organización, recordando que estamos en un mundo en donde las buenas practicas deben ser tomadas en consideración para probarse y mejorarse continuamente hacia la calidad total

Lugar, fecha de validación: Quito, 6 de marzo de 2024

Firma del especialista