UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS "ESPOG"

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Resolución: RPC-SO-02-No.053-2021

PROYECTO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGISTER

Título del proyecto:
Propuesta de Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la 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:
Ing. Viteri Viteri Carlos Javier
Tutor/a:
Mgs. Toasa Guachi Renato Mauricio **Ph.D. Urdaneta Herrera Maryory**

Quito – Ecuador

2024

APROBACIÓN DEL TUTOR

Yo, Msc. Renato Mauricio Toasa Guachi con C.I: 1804724167 en mi calidad de Tutor del proyecto de investigación titulado: Propuesta de Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador.

Elaborado por: Carlos Javier Viteri Viteri, de C.I: 1712777968, 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:
RENATO MAURICIO
TOASA GUACHI

Msc. Renato Mauricio Toasa Guachi

APROBACIÓN DEL TUTOR

Yo, Ph.D. Urdaneta Herrera Maryory con C.I: 1759316126 en mi calidad de Tutora del proyecto de investigación titulado: Propuesta de Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador.

Elaborado por: Carlos Javier Viteri Viteri, de C.I: 1712777968, 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:
MARYORY URDANETA HERRERA

Ph.D. Urdaneta Herrera Maryory

DECLARACIÓN DE AUTORIZACIÓN POR PARTE DEL ESTUDIANTE

Yo, Carlos Javier Viteri Viteri con C.I: 1712777968, autor/a del proyecto de titulación denominado: Propuesta de Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador. Previo a la obtención del título de Magister en Seguridad.

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:
CARLOS JAVIER VITERI VITERI

Firma

Tabla de contenidos

Índice de tablas

Índice de figuras

INFORMACIÓN GENERAL

Contextualización del tema

La seguridad informática o ciberseguridad hace referencia a la protección de información encaminada a impedir la alteración de registros o métodos por parte terceras personas. El objetivo primordial es proteger a personas, dispositivos técnicos y registros de daños e intimidaciones. La seguridad informática es un cúmulo de acciones que tienen como fin proteger la integridad de equipos e información que contienen (UdeCataluña, 2023).

La seguridad de los sistemas es el concepto de aplicar lineamientos para garantizar que el software continúe funcionado (o se resista) a los ataques al crear seguridad. Esto significa que el software se somete a pruebas de seguridad para garantizar que pueda resistir ataques maliciosos antes de su lanzamiento al mercado (Thales, 2023).

El desarrollo de aplicaciones es una etapa crítica que necesita una planificación y ejecución cuidadosas. Para garantizar el éxito de su proyecto de software, es importante seguir las mejores prácticas de desarrollo de sistemas. Estas mejores prácticas incluyen el uso de las herramientas y la tecnología adecuadas, el cumplimiento de los estándares de codificación, la realización de pruebas periódicas y la garantía de calidad. Siguiendo estas mejores prácticas, los desarrolladores pueden crear aplicaciones de alto rendimiento que cubran los requerimientos y proporcione valor a los interesados (INNEVO CONSULTING, 2023).

La Universidad Central del Ecuador “tiene su sede en Quito, capital de la República del Ecuador, y es una comunidad de docentes, estudiantes, profesores y personal con personería jurídica, autónoma, pública y sin fines de lucro” (Universidad Central del Ecuador, 2019, p. 4).

La Dirección de Tecnologías de la Información y Comunicación (DTIC), se encargará de: “Regular, planificar los recursos tecnológicos orientados al uso y transferencia de la información de las personas que conforman la comunidad” (Universidad Central del Ecuador, 2019, p. 51).

El Desarrollo de Software en la DTIC, se encuentra bajo la normativa vigente, así como cuenta con la ejecución de acciones que derivan en un el desarrollo seguro de software.

La presente propuesta de políticas de seguridad informática para el desarrollo de sistemas web, aplicando la norma ISO 27002 2022, en la Universidad Central del Ecuador, pretende fomentar el uso de acciones en el desarrollo de software, certificando el uso actual de buenas prácticas y enmarcado a las normas vigentes, garantizando la integridad de los registros.

Problema de investigación

En la DTIC de la Universidad Central del Ecuador se desarrolla software con el propósito de brindar soluciones informáticas de acuerdo con los requerimientos de las Unidades de Planta Central y Facultades, de esta manera se realiza la "planificación, análisis, diseño, implementación, pruebas, instalación o despliegue y su uso y mantenimiento" (Universidad Central del Ecuador, 2019, p. 52).

En esta dirección, se realizan procesos que se encuentran enmarcados en la normativa legal vigente, como:

- "Ley Orgánica de Protección de Datos Personales" (DerechoEcuador.com, 2022).
- "ISO/IEC 17799 Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información" (ISO, 2024).
- Código Orgánico Integral Penal (Gob.ec, 2024).
- "Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que dispongan de Recursos Públicos" (CONTRALORÍA GENERAL DEL ESTADO, 2023).
- "Estatuto de la Universidad Central del Ecuador" (Universidad Central del Ecuador, 2019).

Actualmente la DTIC, no cuenta con un área especializada en la Seguridad de la Información, a pesar de que, en las áreas que componen esta Dirección, se realizan los procesos de manera segura, esto ocasiona que no existan políticas de seguridad informática en el desarrollo de software, estrictamente fundamentado en los requerimientos o "controles de la Norma ISO/IEC 27002:2022" (ISO, 2024).

Objetivo general

Elaborar la propuesta de políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador.

Objetivos específicos

1. Contextualizar los fundamentos teóricos sobre seguridad informática en el desarrollo de sistemas web.
2. Determinar los controles de la norma ISO/ICE 27002:2022 aplicables para el desarrollo de sistemas web.
3. Elaborar los instrumentos para el desarrollo de sistemas web aplicando los controles de la norma ISO 27002:2022.
4. Validar la propuesta mediante el criterio de especialistas.

Vinculación con la sociedad y beneficiarios directos:

La comunidad universitaria, integrada por Estudiantes, Docentes, Empleados y Trabajadores, serán los beneficiarios directos ya que podrán contar con la conectividad necesaria para desarrollar sus actividades académicas, así como, garantizar la integridad de la plataforma informática, por lo tanto, se propone políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, lo que contribuirá al cumplimiento de la misión Institucional, así como, para lograr el cuarto objetivo de desarrollo sostenible, que pide "garantizar una educación de calidad inclusiva y equitativa y promover oportunidades de aprendizaje permanente para todos" (ONU, 2023).

CAPÍTULO I: DESCRIPCIÓN DEL PROYECTO

1.1. Contextualización general del estado del arte

Con el proyecto se pretende proponer políticas de seguridad informática en el desarrollo de sistemas web, para la Universidad Central del Ecuador, cuyo fundamento se basa en la "norma ISO/IEC 27002:2022, Seguridad de la información, ciberseguridad y protección de la privacidad – controles de seguridad de la Información" (ISO, 2024).

Los trabajos investigados por que guardan similitud con la presente investigación son:

En la investigación para titulación, se concluye que, contextualizar las bases teóricas de las actividades para la integridad de los registros como los estándares ISO 27002 y CSF de NIST, proporciona una visión general de los lineamientos, medidas y salvaguardas que deben considerarse para garantizar la integridad, confidencialidad y disponibilidad de la información (Hernández & Recalde, 2023).

En el trabajo de investigación para obtener el grado de Magister, cita que "las políticas de seguridad informática son un cúmulo de reglas y lineamientos que garantizan la confidencialidad, integridad y disponibilidad de la información, reduciendo el riesgo de ser afectada" (Valencia & Recalde, 2023, p.1).

Las aplicaciones de software han evolucionado en las últimas décadas de tal manera que las empresas en la actualidad requieren al menos una aplicación que les permita reducir tiempos, gastos y mantener datos históricos que puedan servir de control para saber exactamente qué información se almacena. El software ha sido creado de manera inadecuada en todo aspecto, sin tener en consideración las etapas del ciclo de vida, lo que ha llevado a ataques a las empresas a través de las aplicaciones que han sido creadas para sí mismas, especialmente aquellas que se encuentran en la web. (Montalvo, 2017, p.1)

Se debe considerar que:

La seguridad de la información debe estar presente en todos los sectores, especialmente en las universidades, institutos y escuelas públicas y privadas. En algún momento, todas las instituciones pueden ser sujeto de estafa o ataque directo. (Chuqui y Orellana, 2023, p.15)

Mayra Gabriela Cordero Núñez en su proyecto de investigación creado en la Universidad Técnica de Ambato, cita que:

> Cooperativas como la Cooperativa de Ahorro y Crédito San Francisco Ltda. al paso del tiempo van creciendo y viéndose en la necesidad de proteger y reforzar la información sin embargo de que cuentan con Sistema de Gestión de Seguridad de la Información, el mismo que no se ha implementado de manera correcta, por lo que su actualización e implementación de políticas son necesarias para precautelar los activos de información. (Cordero, 2022, p.6)

En la publicación de GlobalSuite SOLUTIONS, afirma que "ISO 27002 es un estándar internacional que proporciona orientación sobre la implementación de controles de seguridad de la información" (GlobalSuite SOLUTIONS, 2023, p. 1).

Adriana Matei, en su trabajo de fin de grado concluye que:

> El desarrollo de aplicaciones seguras se ha transformado en un tema de alta prioridad. Esto es el resultado de la dependencia que tienen las empresas en sus aplicaciones y al apogeo de la seguridad de la información en la actualidad, por lo que es eminente garantizar el normal funcionamiento protegiéndolas de ataques internos y externos. (MATEI, 2015, p. 96).

La seguridad ya no es un atributo de calidad, existe en todas las capas de la arquitectura del software y por tanto no puede utilizarse como un elemento aislado, sino que es horizontal y multidimensional. Si se continúa desarrollando software de forma tradicional, siempre parecerá que los hackers están dos pasos por delante de las organizaciones (Joaquín & Abundis, 2013).

En su proyecto de investigación Jessica Janina Cabezas Quinto, señala que:

> Es habitual desarrollar políticas para proteger la seguridad de la información al mismo tiempo que se desarrollan planes de prevención. Estas empresas serán las encargadas de etiquetar todas las líneas de actuación relacionadas con la seguridad y definir medidas técnicas y procedimentales para asegurar los objetivos marcados en la política de seguridad a través de programas de prevención. (CABEZAS, 2023, p. 11)

La ejecución de un Sistema de Gestión de Seguridad de la Información suministra un modelo de mejoramiento continuo, que puede renovarse, contrarrestando las amenazas, con el uso de acciones preventivas y correctivas, que controlen cualquier incidente que implique la afectación de la Seguridad de la Información (Moron, 2023).

Otro autor concluye que:

> La revisión de código fuente para la seguridad es una actividad de buenas prácticas que contribuye a mejorar la seguridad del software. De igual manera, el diseño y las revisiones de código realizadas por pares pueden generar mejoras importantes en la seguridad del software. (Hernadez, 2020, p.108)

El aporte que brinda al proyecto de titulación, las referencias citadas, es muy valioso, la Seguridad Informática en el Desarrollo de aplicaciones tecnológicas, es cada vez más necesaria, con el avance tecnológico, las actividades que antes dependían estrictamente de la intervención del ser humano ahora son cada vez más reemplazadas por la invención tecnológica.

1.2. Proceso investigativo metodológico

En el tema objeto de estudio se va a aplicar el enfoque metodológico de investigación mixto, a fin de lograr una vista más amplia en la aplicación de herramientas, bases y seguridades informáticas, con las cuales se realiza el desarrollo de software en el área de Desarrollo de la DTIC de la Universidad Central del Ecuador.

La propuesta de políticas de seguridad informática pretende verificar la aplicación de la norma ISO 27002:2022 en el desarrollo de software, avalando la confidencialidad, integridad y disponibilidad de la información.

Los métodos mixtos son “procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta” (Hernandéz-Sampieri & Mendoza, 2018, p. 612).

Las principales características del enfoque mixto de la investigación son: “Se usan métodos del enfoque cualitativo y cuantitativo, es posible la conversión de datos, desde el planteamiento del problema estimula el uso de lógica inductiva y deductiva” (Hernandéz-Sampieri & Mendoza, 2018, p. 612).

En la investigación se usan técnicas como:

Revisión bibliográfica:

Para todo tipo de investigación se requiere una revisión bibliográfica para determinar el contexto del estudio y el estado actual del tema de análisis en el campo científico. La investigación bibliográfica es ágil y económica comparada con otros métodos y puede contener registros informáticos, documentos comerciales y académicos, y más (Lifeder, 2020). En este proyecto de investigación se realizó el análisis de la normativa interna como: Estatuto, políticas y procesos.

Entrevistas:

Con el propósito de fortalecer la investigación se hizo uso de la técnica e instrumento de entrevista, mediante entrevistas focalizadas realizadas al Director de la DTIC y a los Coordinadores de las Áreas de Desarrollo e Infraestructura, se ha podido obtener una muestra del grado de cumplimiento de los controles que comprenden la “norma ISO/IEC 27002:2022” (ISO, 2024), considerando los siguientes criterios:

- Amplia experiencia y conocimiento del personal entrevistado.
- Especificidad en la elaboración de las preguntas enmarcadas en los “controles de la norma ISO/IEC 27002:2022” (ISO, 2024).
- Profundidad en el contenido de las preguntas lo que ha permitido obtener información relevante de la situación actual en el desarrollo de aplicaciones.

Para el desarrollo de la entrevista se ha elaborado la matriz de situación inicial en la cual se establece el cumplimiento completo, parcial o incumplimiento de los “controles de la norma ISO/IEC 27002:2022” (ISO, 2024).

1.3. Análisis de resultados

El análisis constituye un resumen de toda la información recopilada en base a las respuestas obtenidas mediante las entrevistas aplicadas al Director, al Coordinador del Área de Desarrollo de Sistemas y al Coordinador del Área de Infraestructura de la DTIC de la Universidad Central del Ecuador ver Anexo 1, se realiza el respectivo análisis.

Se consolida la información obtenida mediante las respuestas de los entrevistados con el propósito de establecer un análisis cuantitativo, que se registra en la MATRIZ PONDERADA DE SITUACIÓN INICIAL DE REQUISITOS DE LA NORMA ISO 27002:2022, ver Anexo 2.

Para su valoración se establece el siguiente parámetro: dos puntos para los controles que se cumplen; un punto para los controles que se cumplen de manera parcial; y, cero puntos para los controles que no se cumplen.

Las respuestas a las preguntas sobre el cumplimiento de los controles de la cláusula 5 (Controles Organizacionales) de la norma ISO/IEC 27002:2022, indican que se encuentra en un 81,08% desarrollado y en un 18,92% por desarrollar, como se presenta en la Tabla 1:

Tabla 1

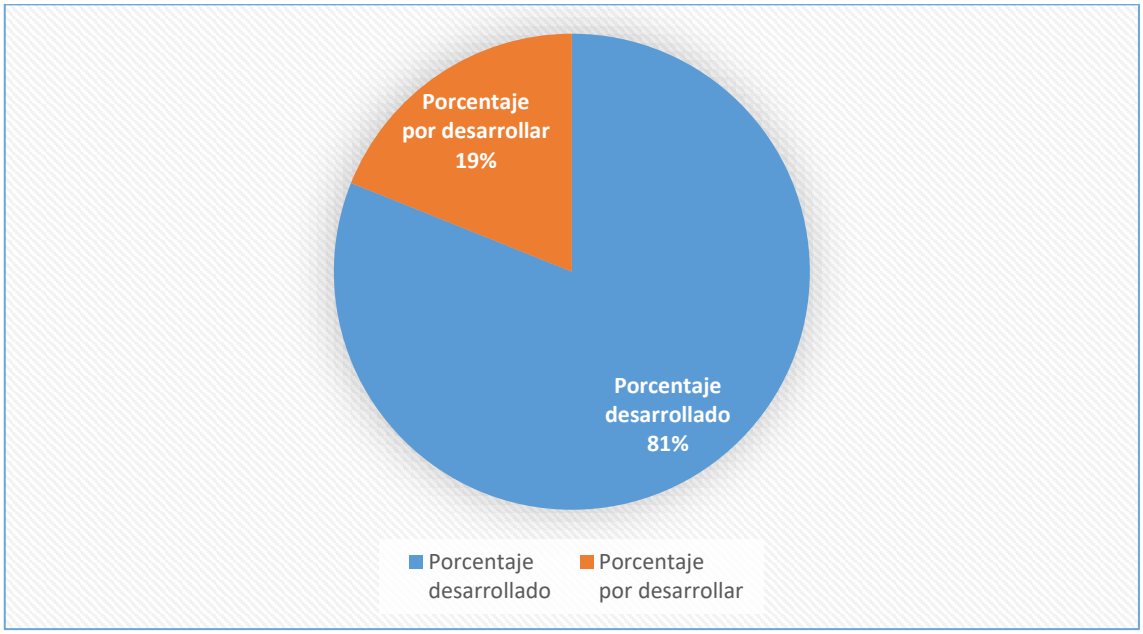
Clausula 5 Controles Organizacionales

Calificación	Controles	Total Ponderado	Porcentaje desarrollado	Porcentaje por desarrollar
Cumple	24	48	64,86	
Cumple Parcial	12	12	16,22	
Incumple	1	0	0,00	
TOTAL	37	60	81,08	18,92

Se puede observar en la Figura 1 que, el 81,08% se encuentra desarrollado y 18,92% por desarrollar.

Figura 1

Porcentajes de cumplimiento Cláusula 5



Las respuestas sobre el cumplimiento de los controles de la cláusula 6 (Controles Personales) de la "norma ISO/IEC 27002:2022" (ISO, 2024), indican que el cumplimiento es del 93,75% y 6,25% por cumplir, como se detalla en la Tabla 2:

Tabla 2

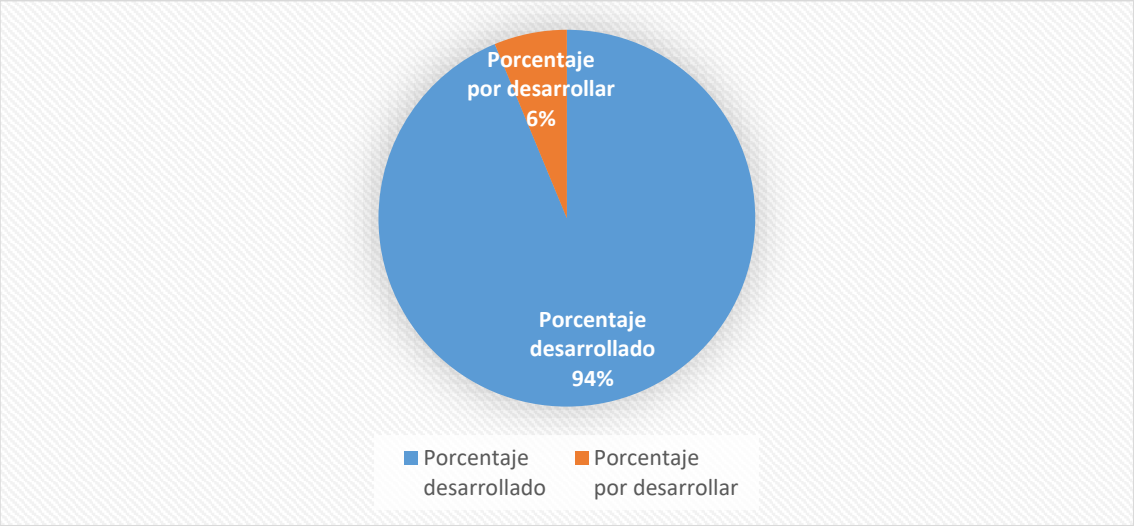
Cláusula 6 Controles Personales

Calificación	Controles	Total Ponderado	Porcentaje desarrollado	Porcentaje por desarrollar
Cumple	7	14	87,50	
Cumple Parcial	1	1	6,25	
Incumple	0	0	0,00	
TOTAL	8	15	93,75	6,25

Se puede observar en la Figura 2 que, el 93,75% se encuentra desarrollado y 6,25% por desarrollar.

Figura 2

Porcentajes de cumplimiento Cláusula 6



En cuanto a las respuestas sobre el cumplimiento de los controles de la cláusula 7 (Controles Físicos) de la "norma ISO/IEC 27002:2022" (ISO, 2024), expresan un total de 85,71% de cumplimiento y 14,29% por cumplir, como se detalla en la Tabla 3:

Tabla 3

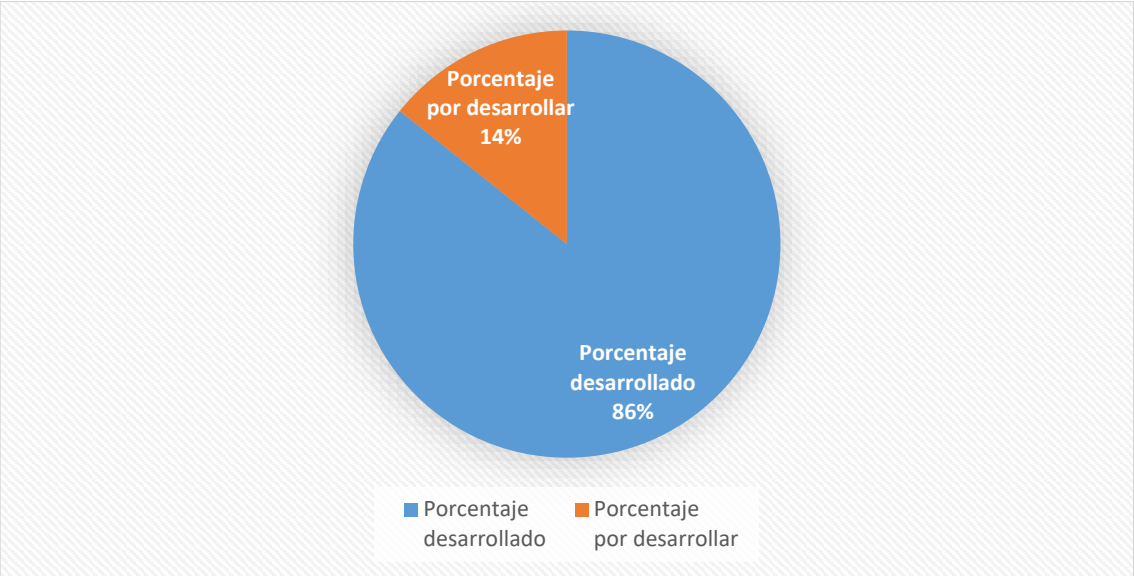
Clausula 7 Controles Físicos

Calificación	Controles	Total Ponderado	Porcentaje desarrollado	Porcentaje por desarrollar
Cumple	10	20	71,43	
Cumple Parcial	4	4	14,29	
Incumple	0	0	0,00	
TOTAL	14	24	85,71	14,29

En la Figura 3 se puede observar que, el 85,71% se encuentra desarrollado y 14,29% por desarrollar.

Figura 3

Porcentajes de cumplimiento Cláusula 7



Los resultados sobre el cumplimiento de los controles de la cláusula 8 (Controles Tecnológicos) de la norma ISO/IEC 27002:2022, expresan un 58,82% desarrollado o cumplido y 41,18 % por desarrollar o incumplido, como se detalla en la Tabla 4:

Tabla 4

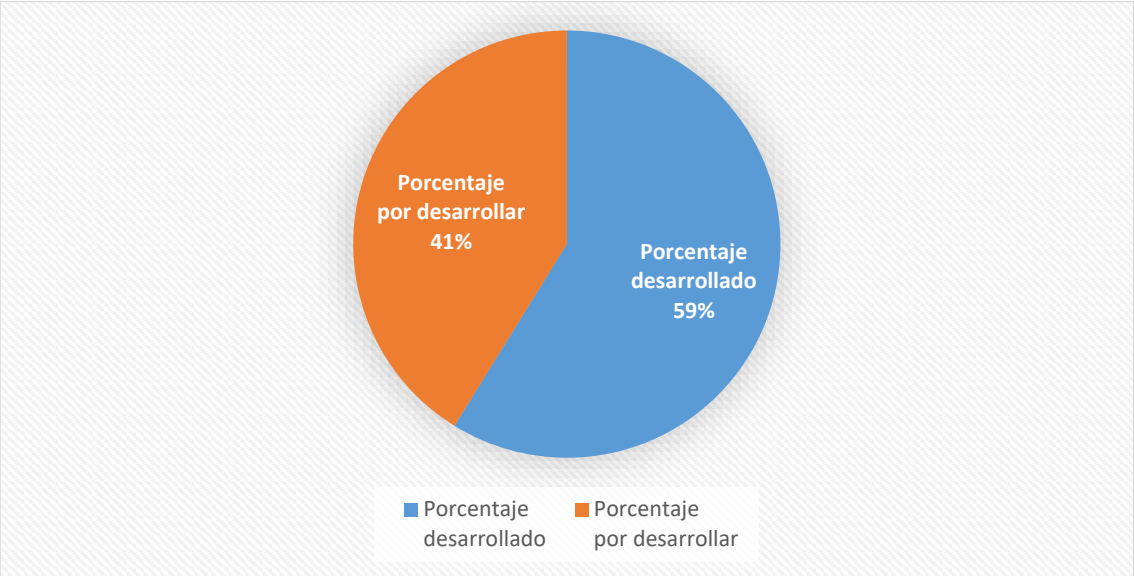
Cláusula 8 Controles Tecnológicos

Calificación	Controles	Total Ponderado	Porcentaje desarrollado	Porcentaje por desarrollar
Cumple	12	24	35,29	
Cumple Parcial	16	16	23,53	
Incumple	6	0	0,00	
TOTAL	34	40	58,82	41,18

En la Figura 4 se puede observar que, el 58,82% se encuentra desarrollado y 41,18% por desarrollar.

Figura 4

Porcentajes de cumplimiento Cláusula 8



Como análisis general el cumplimiento Cláusulas de la "norma ISO/IEC 27002:2022" (ISO, 2024), se calcula sumando la calificación obtenida en los controles de cada uno, dividido para el total de la ponderación establecida y multiplicado por 100, obteniendo como resultado el porcentaje de cumplimiento por Cláusula, como se detalla en la Tabla 5, información que permite analizar e identificar el estado del cumplimiento.

Tabla 5

Resultados generales de las Cláusulas

Cláusulas	**Porcentaje desarrollado**	**Porcentaje por desarrollar**
Organizacionales	81,08	18,92
Personas	93,75	6,25
Físicos	90,00	10,00
Tecnológicos	58,82	41,18

En la Figura 5, se puede observar que en la Cláusula 8 Controles Tecnológicos, se cuenta con un mayor porcentaje de controles por desarrollar.

Figura 5

Porcentajes generales de cumplimiento de las Cláusulas


18,92
81,08
6,25
93,75
10,00
90,00
41,18
58,82
ORGANIZACIONALES
PERSONAS
FÍSICOS
TECNOLÓGICOS
Porcentaje desarrollado
Porcentaje por desarrollar

CAPÍTULO II: PROPUESTA

2.1. Fundamentos teóricos aplicados

2.1.1. Políticas de seguridad informática

Consiste en una serie de normas y directrices que permiten garantizar la confidencialidad, integridad y disponibilidad de la información y minimizar los riesgos que le afectan (unir LA UNIVERSIDAD EN INTERNET, 2020).

Existen varias definiciones que se pueden citar como:

Un conjunto de directrices y procedimientos diseñados para proteger los datos confidenciales y críticos de una institución. Las políticas son indispensables para la seguridad de la información, reducir los riesgos y cumplir con la normativa (ADQA, 2024).

2.1.2. Desarrollo de Software Seguro

El desarrollo seguro de software es una metodología cuya meta es considerar la seguridad de las aplicaciones a lo largo de todo su ciclo de vida, iniciando desde la propia definición de requisitos de estas (ITCL CENTRO TECNOLOGICO, 2022).

2.1.3. Normas ISO Organización Internacional de Normalización

Se conoce que, “Es una organización mundial independiente y no gubernamental. Reúne a expertos de todo el mundo para acordar las mejores formas de hacer las cosas, desde la gestión de la calidad hasta la inteligencia artificial” (ISO, 2024).

Los estándares internacionales permiten que los bienes y servicios que se usan todos los días sean idóneos, confiables y de alta eficiencia. También ayudan a las instituciones a adoptar prácticas éticas y sostenibles para ayudar a crear un futuro en el que su suministro no solo funcione bien, sino que también proteja nuestro planeta (ISO, 2024).

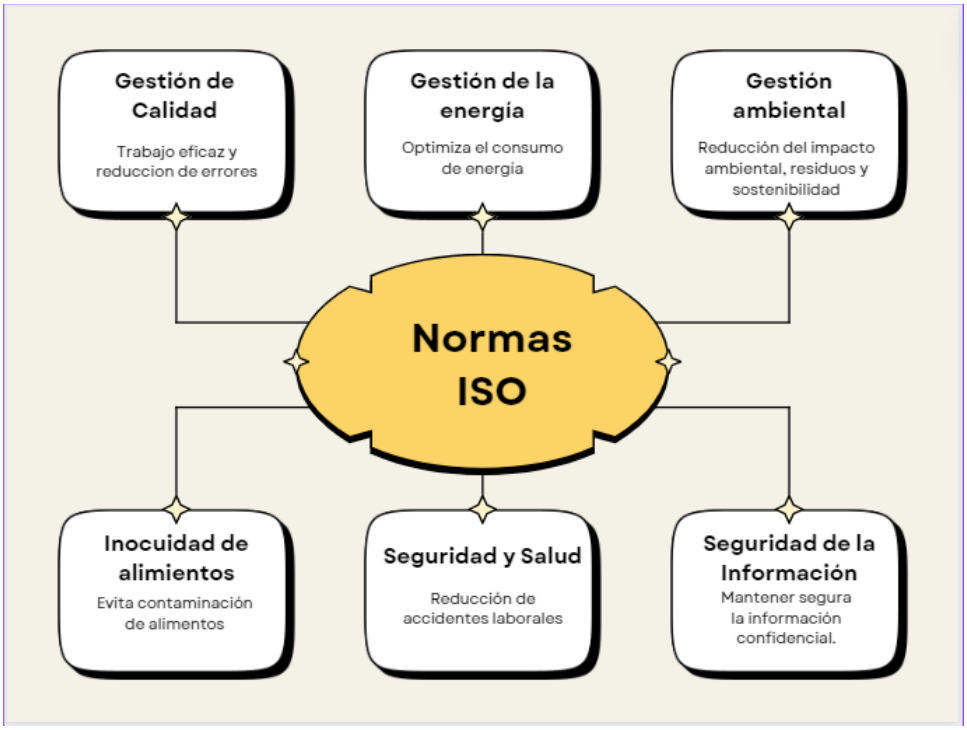
“Normas mundiales para bienes y servicios de confianza precisan lo que es eficiente, referenciando puntos coherentes tanto para las empresas como para los

consumidores, garantizando así la fiabilidad, generando confianza y simplificando las opciones" (ISO, 2024, p. 1).

Las Normas ISO abarcan varios sectores, por ejemplo, los que se describen en la Figura 6:

Figura 6

Sectores de las Normas ISO



Nota. Fuente: Organización Internacional de Normalización

2.1.4. ISO/IEC 27002:2022

2.1.4.1. Generalidades

La Organización Internacional de Normalización establece que: "la norma ISO/IEC 27002:2022 ofrece buenas prácticas y objetivos de control relacionados con aspectos clave de la ciberseguridad, como el control de acceso, la criptografía, la seguridad de los recursos humanos y la respuesta ante incidentes" (ISO, 2024, p. 1).

Esta norma sirve para las organizaciones como: “modelo práctico para proteger eficazmente sus activos de información contra las ciberamenazas. Al seguir las directrices, pueden adoptar un enfoque proactivo de la gestión de riesgos de ciberseguridad y proteger la información crítica del acceso no autorizado y la pérdida” (ISO, 2024, p. 1).

2.1.4.2. Alcance

Toda organización de cualquier tamaño, tipo o industria tienen la posibilidad de aplicar la Norma ISO/IEC 27002:2022. Las organizaciones se benefician al seleccionar e implementar controles de seguridad acoplados a los riesgos propios que los afectan (GlobalSuite SOLUTIONS, 2023).

2.1.4.3. Controles

La norma está compuesta de cuatro cláusulas:

Controles Organizacionales (Cláusula 5): cuenta con 37 controles que “proporcionan un esquema operativo enfocado en la definición de estructuras de gobernabilidad y roles, establecimiento de políticas claras, asegurar el cumplimiento regulatorio, gestión proactiva de riesgos, adaptabilidad ante el cambio e incentivar una búsqueda constante de mejora” (GlobalSuite SOLUTIONS, 2023).

Controles de Personas (Cláusula 6): cuenta con 8 controles que “reconocen la importancia del factor humano, se centran en la concientización y formación del personal, procesos de reclutamiento seguros, definición de responsabilidades en la contratación, evaluaciones periódicas y disciplina en caso de incumplimientos y protocolos de terminación de empleo” (GlobalSuite SOLUTIONS, 2023).

Controles Físicos (Cláusula 7): son 14 controles que “se encargan de la protección tangible, se enfocan en la salvaguarda de equipos y dispositivos, protección de medios de almacenamiento, seguridad de las instalaciones físicas, y medidas preventivas contra incidentes, ya sean naturales o intencionados” (GlobalSuite SOLUTIONS, 2023).

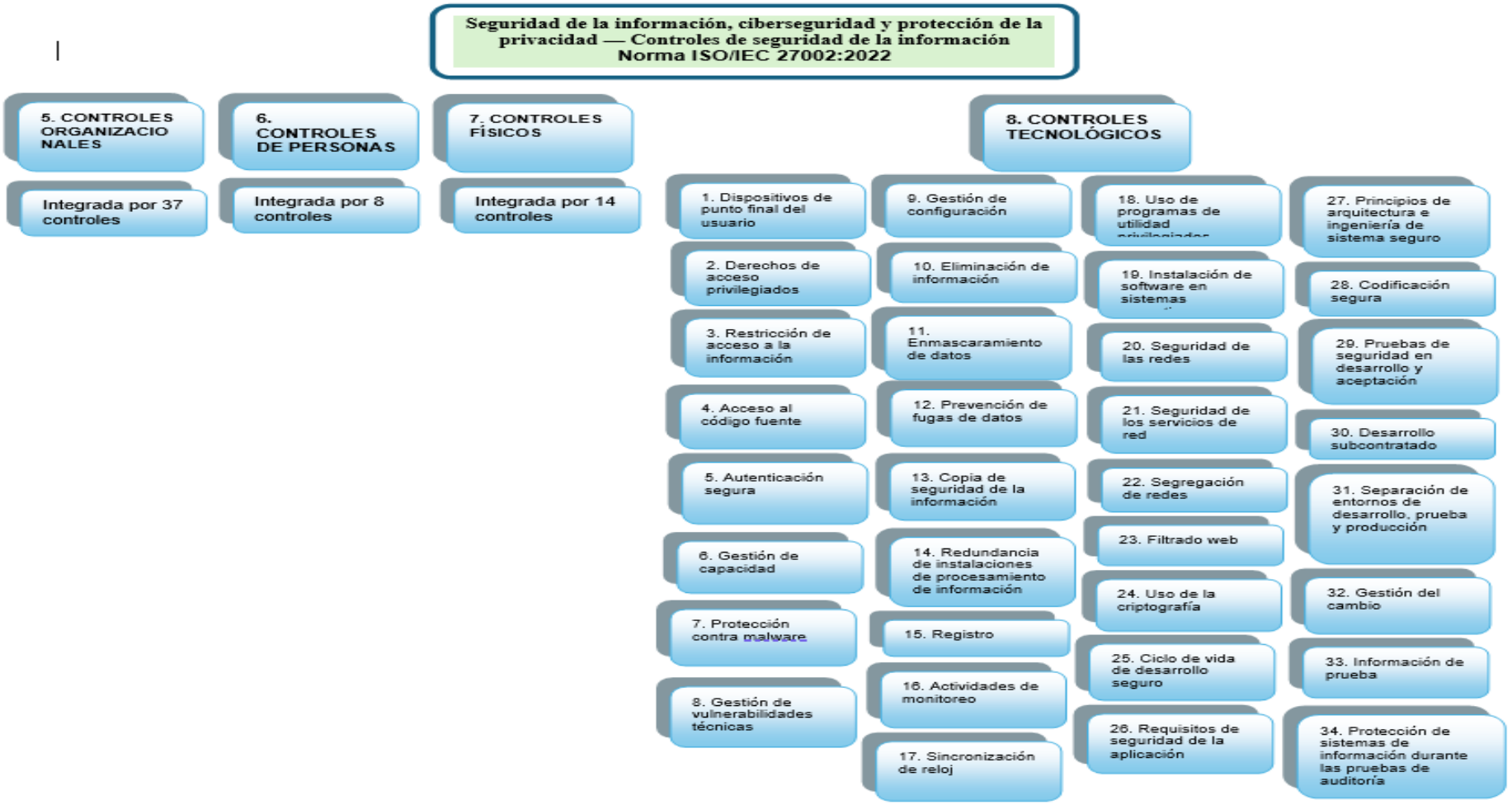
Controles Tecnológicos (Cláusula 8): con 34 controles y su enfoque es “la infraestructura tecnológica, se centran en los procesos seguros desde el diseño hasta la implementación de sistemas, mantenimiento y configuración de redes, monitoreo constante, análisis y pruebas periódicas y procedimientos de auditoría y recuperación en caso de incidentes” (GlobalSuite SOLUTIONS, 2023).

2.1.4.4. Esquema de la Norma ISO/IEC 27002:2022

A continuación, se detalla en la Figura 7, “el esquema de la Norma ISO /IEC 27002:2022 Seguridad de la información, ciberseguridad y protección de la privacidad — Controles de seguridad de la información” (ISO, 2024), de conformidad al objetivo propuesto para la presente investigación:

Figura 7

Esquema de la "Norma ISO /IEC 27002:2022 Seguridad de la información" (ISO, 2024).



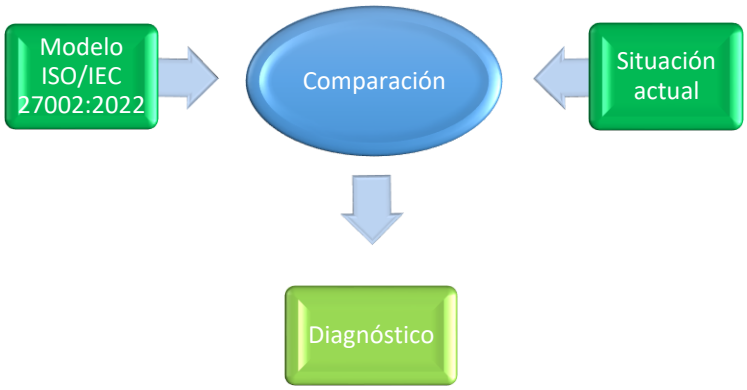
2.2. Descripción de la propuesta

2.2.1 Diagnostico de situación inicial.

Se realiza la comparación entre la situación actual de la DTIC con la “norma ISO/IEC 27002:2022” (ISO, 2024), la cual se ilustra en la Figura 8, obteniendo del diagnóstico situacional inicial, que es la línea base para la propuesta de esta investigación.

Figura 8

Comparación de la situación actual



Nota. El gráfico representa la comparación entre los requisitos de la norma vs la situación actual del área y como resultado obtenemos el diagnostico de situación inicial.

El diagnostico resultado de la metodología aplicada en la recolección de la información permite evaluar el cumplimiento (C), cumplimiento parcial (CI) o incumplimiento (I), de cada uno de los controles que componen la “norma ISO/IEC 27002:2022” (ISO, 2024), es pertinente mencionar que los primeros puntos de la norma son de carácter introductorio, ver Anexo 3.

a. Estructura general

En la Figura 9 se ilustra la estructura del objeto de esta investigación.

Figura 9

Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador

b. Explicación del aporte

1. TEMA

Propuesta de políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002:2022, para la Universidad Central del Ecuador.

2. JUSTIFICACIÓN

"La Organización Internacional de Normalización ha desarrollado la norma internacional ISO/IEC 27002:2022, que brinda orientación a las organizaciones que desean establecer, implantar y mejorar un sistema de gestión de seguridad de la información centrado a la seguridad informática" (ISO, 2024).

En la actualidad las instituciones de Educación Superior como la Universidad Central del Ecuador, cuenta con plataformas tecnológicas en las que se almacena información referente a la academia y administración, que deben contar con normas, políticas y procedimientos que permitan garantizar su confidencialidad, integridad y disponibilidad.

La DTIC, cuenta con el área de Desarrollo de Software, la cual no dispone de políticas de seguridad informática aplicando la norma ISO/IEC 27002:2022, que permita brindar las directrices y procedimientos, a fin de proteger eficazmente los activos de información y reducir las vulnerabilidades en sus sistemas.

En tal virtud se propone desarrollar las políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002.

3. OBJETIVOS DE LAS POLÍTICAS DE SEGURIDAD

3.1. OBJETIVO GENERAL

Desarrollar las políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO/IEC 27002:2022

3.2. OBJETIVOS ESPECIFICOS

3.2.1 Establecer los controles tecnológicos en la Clausula 8 de la norma ISO/IEC 27002:2022, necesarios para precautelar la información en el desarrollo de software.

3.2.2 Diseñar las actividades e instrumentos basados en los controles tecnológicos de la Clausula 8 de la norma ISO 27002:2022.

4. ALCANCE

Las políticas de seguridad informática propuestas se encuentran enfocadas al área de desarrollo de sistemas, cuyas actividades y procedimientos podrían ser aplicadas en todas las áreas que conforman la DTIC.

5. POLITICAS

Las autoridades de la institución deben proveer de los recursos humanos, tecnológicos, económicos y de la infraestructura, que permita el cumplimiento de las políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO/IEC 27002:2022.

El Director y Coordinadores de la DTIC deben socializar y capacitar al personal que interviene en las actividades de las políticas de seguridad informática en el desarrollo de sistemas web, fundamentado en el cumplimiento de los controles de la norma ISO/IEC 27002:2022.

El personal del área de Desarrollo de Software de la DTIC debe aplicar las directrices, basadas en los controles tecnológicos de la Clausula 8 de la norma ISO/IEC 27002:2022, que constan las políticas de seguridad informática en el desarrollo de sistemas web, para la ejecución de los proyectos inherentes al cumplimiento de sus funciones.

El Coordinador del área de Desarrollo de Software debe realizar el seguimiento y control en la ejecución de las políticas de seguridad informática en el desarrollo de software.

Para la ejecución de estas políticas el Coordinador dispone de los instrumentos elaborados por cada control de la norma ISO/IEC 27002:2022, aplicables al desarrollo de software.

6. PRESUPUESTO Y CRONOGRAMA

6.1. PRESUPUESTO

Las presentes políticas de seguridad informática en el desarrollo de sistemas web, son financiadas por el autor, de acuerdo con el detalle de la Tabla 6:

Tabla 6

Recursos financieros

Descripción	Valor
Laptop	$ 650,00
Servicio de internet por 3 meses	$ 90,00
Recolección de datos	$ 250,00
TOTAL	$ 990,00

6.2. CRONOGRAMA DE ACTIVIDADES

Las presentes políticas de seguridad informática en el desarrollo de sistemas web, se realiza según el cronograma de la Tabla 7:

Tabla 7

Cronograma

Actividad	Inicio	Fin	Diciembre 2023				Enero 2024				Febrero 2024			
			1	2	3	4	1	2	3	4	1	2	3	4
Recolección y análisis de la información	1/12/2023	22/12/2023												
Elaboración del Diagnostico Situacional	2/1/2024	21/1/2024												
Análisis de resultados	22/1/2024	26/1/2024												
Desarrollo	1/2/2024	28/2/2024												

7. DESARROLLO DE LOS CONTROLES DE LA NORMA ISO 27002:2022

Para el desarrollo de las actividades de las políticas, se consideran los controles de la norma, que son aplicables al desarrollo de software.

Fase 1: Acceso al código fuente:

Responsable: Coordinador del área de Desarrollo de Software.

Control del acceso a los datos sensibles de las herramientas de desarrollo y código fuentes (isms.online, 2023).

Las actividades que se ejecutan en la actualidad en el área de desarrollo son:

1. El coordinador del área entrega al personal el software para su instalación:
    - TortoiseSVN
    - Eclipse IDE
    - DBVisualizer
    - SQL Developer
2. El coordinador del área crea las credenciales para el acceso al sistema TortoiseSVN
3. El coordinador del área configura el acceso a las bases de datos

Para contribuir a la adecuada administración se ha desarrollado los siguientes formatos:

Formato para el Control como lo muestra la Figura 10:

Figura 10

Formato para el Control de acceso

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

FORMATO PARA EL CONTROL DE ACCESO DE LECTURA Y ESCRITURA AL CODIGO FUENTE

Codigo: AL-FO-001
Versión: 1

Área:
Responsable del Control:

Fecha de creación	Nombre del Sistema	Nombres y apellidos del funcionario	Numero de cedula	Usuario	Contraseña

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Control de herramientas de desarrollo de software como lo muestra la Figura 11:

Figura 11

Formato para el Control de herramientas de desarrollo

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

FORMATO PARA EL CONTROL DE HERRAMIENTAS DE DESARROLLO

Codigo: AL-FO-002
Versión: 1

Área:
Responsable del Control:

Nombre	Descripción	Tipo	Version	Tipo de Licencia

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Control de biblioteca de software como lo muestra la Figura 12:

Figura 12

Formato para el Control de biblioteca de software

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

FORMATO PARA EL CONTROL DE BIBLIOTECA DE SOFTWARE

		Codigo:	AL-FO-003
Área:		Versión:	1
Responsable del Control:			

Fecha	Nombre	Descripción	Tipo	Version	Tipo de Licencia

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Fase 2: Gestión de configuración:

Responsable: Director de la DTIC.

Es una tarea administrativa que comprende el mantenimiento y monitoreo de la información y los datos que se reposan en dispositivos y aplicaciones (isms.online, 2023).

Propiedades: Las propiedades de este control se detallan a continuación en la Figura 13:

Figura 13

Propiedades del control 8,9 Gestión de configuración (isms.online, 2023).

27002:2022	Descripción	Tipo	Propiedades	Concepto	C Operacional	Dominios
8,9	Gestión de configuración	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Configuración segura	Gobernanza y Ecosistema Protección

Nota. Fuente Organización Internacional de Normalización (ISO).

Las actividades que se ejecutan en la actualidad en el área de desarrollo son:

- Los equipos y sistemas se configuran de acuerdo con las especificaciones técnicas del proveedor y a la documentación publica cuando es de código abierto.
- Procedimiento de mantenimiento periódico de hardware y software.
- Procedimiento para actualizaciones de hardware y software.
- Políticas de manejo de usuarios y contraseñas.

Para complementar las actividades que se cumplen con respecto a este control en el área de desarrollo se elabora la matriz (check list) para su monitoreo, revisión y control, como se detalla en la Figura 14:

Figura 14

Formato para el Monitoreo, revisión y control.

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

CHECK LIST PARA EL MONITOREO, CONTROL Y REVISION GESTION DE CONFIGURACIÓN

		Codigo:	GC-FO-001
Área:		Versión:	1
Responsable del Control:			
Usuario:			
Cargo:			
Proyecto:			

		✓ X	Realizado / Pendiente
HARDWARE:			
	Configuraciones generales		
	Mantenimiento periódico		
	Actualizaciones		
SOFTWARE			
	Configuraciones generales		
	Mantenimiento periódico		
	Actualizaciones		
USUARIO			
	Validacion permiso de administrador		
	Cambio de contraseñas		
	Caducidad de sesiones		

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Fase 3: Principios de arquitectura e ingeniería de sistema seguro:

Responsable: En el caso de la DTIC de la Universidad Central del Ecuador, la seguridad de la información está distribuida en las áreas existentes, en este caso la responsabilidad recae sobre el Coordinador del área de Desarrollo de Sistemas.

Instituir los lineamientos de ingeniería de sistemas seguros, en el desarrollo de software dentro de su diseño, implementación y operación (isms.online, 2023).

Propiedades: Las propiedades de este control se detallan a continuación en la Figura 15:

Figura 15

Propiedades del control 8,27.

27002:2022	Descripción	Tipo	Propiedades	Concepto	C Operacional	Dominios
8,27	Principios de arquitectura e ingeniería de sistema seguro	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad del sistema y red Seguridad aplicación	Protección

Nota. Fuente Organización Internacional de Normalización (ISO).

Las actividades que se ejecutan en la actualidad en el área de desarrollo son:

El coordinador del área de Desarrollo de Software dispone para la creación de proyectos los siguientes lineamientos:

- Tutorial para la CREACION DE PROYECTO JEE, en el que se establece la arquitectura que se debe aplicar en la creación de proyectos (Collaguazo, 2016).
- Aplicación del MVC Modelo-Vista-Controlador (Collaguazo, 2016).
- Aplicación del marco de trabajo Spring Security (Collaguazo, 2016, p. 45).

Para complementar las actividades que se cumplen con respecto a este control en el área de desarrollo de sistemas se propone aplicar la Matriz (check list) de

seguimiento y control de la arquitectura en el desarrollo de software, como se expresa en la Figura 16:

Figura 16

Check List de Seguimiento y Control de Arquitectura en el Desarrollo de Software

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

CHECK LIST DE SEQUIMIENTO Y CONTROL DE ARQUITECTURA EN EL DESARROLLO DE SOFTWARE

			Codigo:	PA-FO-001
Área:			Versión:	1
Responsable del Control:				
Usuario:				
Cargo:				
Proyecto:				

			✓ X	Realizado / Pendiente
ARQUITECTURA				
	Moldelo Multicapa			
	Estandares base			
		Paquetes		
		Carpetas		
		Clases		
		Metodos		
		Atributos		
		Variables		
		Constantes		
	Librerias			
ESTRUCTURA				
	JPA			
	EJB			
	WEB			
	EAR			
SEGURIDAD	Spring Security			

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Fase 4: Pruebas de seguridad en desarrollo y aceptación:

Responsable: En este caso la responsabilidad es del Coordinador del área de Desarrollo de Sistemas.

Implementación de pruebas de seguridad a las que, las nuevas aplicaciones son sometidas durante su desarrollo y antes de entrar en producción (isms.online, 2023).

Propiedades: Las propiedades de este control se detallan a continuación en la Figura 17:

Figura 17

Propiedades del control 8,29

27002:2022	Descripción	Tipo	Propiedades	Concepto	C Operacional	Dominios
8,29	Pruebas de seguridad en desarrollo y aceptación	Preventivo	Confidencialidad Integridad Disponibilidad	Detectar	Seguridad del sistema y red Seguridad aplicación Seguridad de información	Protección

Nota. Fuente: Organización Internacional de Normalización (ISO).

Las actividades que se ejecutan en la actualidad en el área de desarrollo son:

- Autenticación de los usuarios
- Acceso controlado a los registros
- Uso de criptografía
- Procedimiento de mantenimiento y actualización de hardware y software

Con respecto a este control en el área de desarrollo de sistemas se propone aplicar la Matriz de cumplimiento de pruebas de seguridad en el desarrollo de software, como se expresa en la Figura 18:

Figura 18

Matriz de Cumplimiento Pruebas de Seguridad

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

MATRIZ DE CUMPLIMIENTO PRUEBAS DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE						
					Codigo:	PS-FO-001
Área:					Versión:	1
Responsable del Control:						
Fecha	**Nombre del Proyecto**	**Descripción**	**Responsable del Proyecto**	**Etapa**	**Prueba**	**Observaciones**

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Fase 5: Separación de entornos de desarrollo, prueba y producción:

Responsable: Oficial de Seguridad de la Información. La responsabilidad es del Coordinador del área de Desarrollo de Sistemas y de su equipo de trabajo.

Aplicación de procedimientos, controles y políticas específicas para cada entorno de desarrollo, prueba y producción (isms.online, 2023).

Propiedades: Las propiedades de este control se detallan a continuación en la Figura 19:

Figura 19

Propiedades del control.

27002:2022	Descripción	Tipo	Propiedades	Concepto	C Operacional	Dominios
8,31	Separación de entornos de desarrollo, prueba y producción	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad del sistema y red Seguridad aplicación	Protección

Nota. Fuente Organización Internacional de Normalización (ISO).

En torno a este control en la actualidad se realizan las siguientes actividades:

- Actualización y parcheo de herramientas de desarrollo de forma periódica.
- Los equipos y sistemas se configuran de acuerdo con las especificaciones técnicas del proveedor y a la documentación publica cuando es de código abierto.
- Control de acceso al ambiente de desarrollo
- Respaldo del entorno de desarrollo
- Monitore y revisión del entono de desarrollo

De acuerdo con el control 8,31 es de suma importancia contar con un documento que evidencie el cumplimiento de las actividades realizadas por lo que se propone aplicar la Matriz de aplicación de procedimientos y controles en el área de desarrollo de software, como se expresa en la Figura 20:

Figura 20

Matriz de Aplicación de Controles y Procedimientos

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

MATRIZ DE APLICACIÓN DE CONTROLES Y PROCEDIMIENTOS POR ÁREA				
				SE-FO-001
Área:				1
Responsable del Control:				
Fecha	**Acción**	**Tipo (Control / Procedimiento)**	**Responsable**	**Observaciones**

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

Fase 6: Gestión de cambio:

Responsable: La responsabilidad es del Coordinador del área de Desarrollo de Sistemas.

Implementación de reglas de gestión de cambios (isms.online, 2023).

Propiedades: Las propiedades de este control se detallan a continuación en la Figura 21:

Figura 21

Propiedades del control

27002:2022	Descripción	Tipo	Propiedades	Concepto	C Operacional	Dominios
8,32	Gestión del cambio	Preventivo	Confidencialidad Integridad Disponibilidad	Proteger	Seguridad del sistema y red Seguridad aplicación	Protección

Nota. Fuente: Organización Internacional de Normalización (ISO).

Actividades:

- El Director de Tecnologías dispone al Coordinador el cambio requerido por el área pertinente.
- El Coordinador delega al responsable del proyecto el cambio solicitado.
- El responsable del proyecto procede con lo solicitado.

En este control se propone realizar un registro de los cambios en la Matriz de Registro para Gestión de Cambios en Desarrollo de Software, como consta en la Figura 21:

Figura 22

Matriz de Registro para Gestión de Cambios en Desarrollo de Software

UNIVERSIDAD CENTRAL DEL ECUADOR
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

MATRIZ DE REGISTRO PARA GESTION DE CAMBIOS EN DESARROLLO DE SOFTWARE	
	GA-FO-001
	1
Área:	
Nombre del Proyecto:	
Responsable del Proyecto:	
Solicitado por:	
Cargo:	
Autorizado por:	
Cargo:	
Cambio Propuesto:	
Motivo del Cambio:	
Resultado Previsto:	
Plazo estimado:	

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Firma	Firma	Firma

8. IMPLEMENTACIÓN DE LAS POLÍTICAS

Para la implementación de las Políticas, es necesario considerar aspectos como:

Recursos Económicos: Todos los recursos económicos se obtienen del Presupuesto asignado a la Institución y se deben constar en la planificación anual.

Responsabilidades: El responsable de la implementación de las Políticas es el Director de Tecnologías de la Información y Comunicación.

El responsable del seguimiento y control del cumplimiento de las Políticas es el Coordinador del área de Desarrollo de Software

Indicadores: Se ha definido los siguientes indicadores:

1. (Número de funcionarios capacitados en la ejecución de las Políticas / Numero de funcionarios de DTIC inmersos en el cumplimiento de las Políticas) * 100
2. (Número de actividades ejecutadas de las Políticas / Número de actividades establecidas en las Políticas) * 100

Tiempo de implementación: Se considera para la implementación de las Políticas un año.

c. Estrategias y/o técnicas

Se consideró los controles de la Cláusula 8 (Controles Tecnológicos), para propuesta de las políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador.

Se desarrolló instrumentos que permiten realizar el seguimiento y control de las actividades y lineamientos que se ejecutan en el desarrollo de sistemas web.

2.3. Validación de la propuesta

Para la validación del presente proyecto de investigación se cuenta con el aporte de:

La Señorita Ing. Nora Catalina Quimbita Caiza Msc. Directora Administrativa (e) de la Universidad Central del Ecuador.

El Señor Ing. Luis Alfredo Gualoto, Analista de Tecnologías 1 de la Universidad Central del Ecuador.

La propuesta se valida a través del método de criterios del especialista. (ver Anexos)

El criterio emitido por quienes valoraron el presente proyecto exponen que es apropiado y contribuye al cumplimiento de la norma en el desarrollo de sistemas web en la Universidad Central del Ecuador.

2.4. Matriz de articulación de la propuesta

Tabla 8

Matriz de articulación

EJES O PARTES PRINCIPALES	SUSTENTO TEÓRICO	SUSTENTO METODOLÓGICO	ESTRATEGIAS / TÉCNICAS	DESCRIPCIÓN DE RESULTADOS	INSTRUMENTOS APLICADOS
ISO/IEC 27002:2022	Guía para la aplicación de controles enfocados en la seguridad de la información	En el tema objeto de estudio se va a aplicar el enfoque metodológico de investigación mixto, a fin de lograr una vista más amplia en la aplicación de herramientas, bases y seguridades informáticas, con las cuales se realiza el desarrollo de software en el área de Desarrollo de la DTIC de la UCE.	Fuentes bibliográficas Entrevistas	Se desarrolló instrumentos que permiten realizar el seguimiento y control de las actividades y procedimientos que se ejecutan en el desarrollo de sistemas web.	Documentación e información de la DTIC – UCE. Artículos publicados en la web.
Acceso al código fuente	Control del acceso a los datos sensibles de las herramientas de desarrollo y código fuentes	Metodológico de investigación mixta	Fuentes bibliográficas Entrevistas	Desarrollo de instrumentos que permiten realizar una adecuada administración.	Documentación e información de la DTIC – UCE. Artículos publicados en la web.
Gestión de configuración	Mantenimiento y monitoreo de la información y los datos que se	Metodológico de investigación mixta	Fuentes bibliográficas Entrevistas	Elaboración de la matriz (check list) para su monitoreo, revisión y control	Documentación e información de la DTIC – UCE. Artículos publicados en la web.

	reposan en dispositivos y aplicaciones				
Principios de arquitectura e ingeniería de sistema seguro	Aplicados al desarrollo de software dentro de su diseño, implementación y operación	Metodológico de investigación mixta	Fuentes bibliográficas Entrevistas	Aplicar la Matriz (check list) de seguimiento y control de la arquitectura en el desarrollo de software	Documentación e información de la DTIC – UCE. Artículos publicados en la web.
Pruebas de seguridad en desarrollo y aceptación	Implementación de pruebas de seguridad a las que, las nuevas aplicaciones son sometidas durante su desarrollo y antes de entrar en producción	Metodológico de investigación mixta	Fuentes bibliográficas Entrevistas	Aplicar la Matriz de cumplimiento de pruebas de seguridad en el desarrollo de software	Documentación e información de la DTIC – UCE. Artículos publicados en la web.
Separación de entornos de desarrollo, prueba y producción	Aplicación de procedimientos, controles y políticas específicas para cada entorno.	Metodológico de investigación mixta	Fuentes bibliográficas Entrevistas	Aplicar la Matriz de aplicación de procedimientos y controles en el área de desarrollo de software	Documentación e información de la DTIC – UCE. Artículos publicados en la web.
Gestión de cambio	Implementación de reglas de gestión de cambios	Metodológico de investigación mixta	Fuentes bibliográficas Entrevistas	Registro de cambios en la Matriz de Registro para Gestión de Cambios en Desarrollo de Software	Documentación e información de la DTIC – UCE. Artículos publicados en la web.

CONCLUSIONES

De la investigación se concluye que existe una amplia información de los fundamentos teóricos sobre seguridad informática en el desarrollo de sistemas web, así como la emisión de normas internacionales que han evolucionado con los avances tecnológicos como la norma ISO/ICE 27002:2022.

Se realiza la comparación entre la situación actual de la DTIC con la norma ISO/IEC 27002:2022, de lo cual se determinó el diagnóstico situacional de los controles de la norma aplicables para el desarrollo de aplicaciones web.

Se ha elaborado los instrumentos para el desarrollo de sistemas web aplicando los controles de la norma ISO 27002:2022, lo que contribuye a la integridad, confidencialidad y disponibilidad de la información que se maneja en el área de Desarrollo de Sistemas de la DTIC.

La validación del experto concluye que el tema de investigación propuesto se enmarca en lo establecido en los controles de la norma ISO/IEC 27002:2022 que permitirá contribuir al mejoramiento del desarrollo de sistemas web en la Universidad Central del Ecuador.

Con la elaboración de las políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, se ha logrado establecer los mecanismos que permitirán mejorar la seguridad de la información en los proyectos desarrollados en el área de Desarrollo de Software, para las áreas académicas y administrativas de la Universidad Central del Ecuador.

RECOMENDACIONES

Promover que las futuras investigaciones se orienten a la aplicación de las normas internacionales que garanticen la seguridad de la información en especial a las normas ISO/IEC 27000.

Socializar y capacitar al personal que interviene en las actividades a desarrollarse en las políticas de seguridad informática en el desarrollo de sistemas web.

Proveer de los recursos humanos, tecnológicos, económicos y de la infraestructura, que permita el cumplimiento de las políticas de seguridad informática en el desarrollo de sistemas web.

Implementar las políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, en el área de Desarrollo de Software de la DTIC de la Universidad Central del Ecuador.

Realizar el seguimiento y control en la ejecución de las políticas de seguridad informática en el desarrollo de software.

BIBLIOGRAFÍA

ADQA. (01 de 03 de 2024). *Definición de políticas de seguridad*. ADQA: https://www.adqa.com/ciberseguridad/tecnologias-y-servicios/definicion-de-politicas-de-seguridad/

CABEZAS QUINTO, J. (12 de 01 de 2023). ANÁLISIS DE UN PLAN CON ESTRATEGIAS DE SEGURIDAD DE LA . pág. 11. https://repositorio.unemi.edu.ec/bitstream/123456789/6852/1/PEREZ%20ALVAREZ%20SEGUNDO%20ARTURO.pdf

Collaguazo, D. (2016). *CREACION PROYECTO JEE.* UNIVERSIDAD CENTRAL DEL ECUADOR.

CONTRALORÍA GENERAL DEL ESTADO. (14 de 12 de 2018). *Base legal y normativa*. www.contraloria.gob.ec: https://www.contraloria.gob.ec/Normatividad/BaseLegal

CONTRALORÍA GENERAL DEL ESTADO. (27 de 02 de 2023). *Base legal y normativa*. www.contraloria.gob.ec: https://www.contraloria.gob.ec/Normatividad/BaseLegal

DerechoEcuador.com. (24 de 01 de 2022). *LEY ORGÁNICA DE PROTECCIÓN DE DATOS PERSONALES*. https://derechoecuador.com/ley-organica-de-proteccion-de-datos-personales/

Droege, U. (05 de 06 de 2023). *¿Qué es una estructura de alto nivel?* dqs: https://www.dqsglobal.com/es-mx/aprenda/centro-de-conocimientos-dqs/que-es-una-estructura-de-alto-nivel

GlobalSuite SOLUTIONS. (17 de 10 de 2023). ¿Qué es la norma ISO 27002 y para qué sirve? https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27002-y-para-que-sirve/

GlobalSuite SOLUTIONS. (17 de 10 de 2023). *¿Qué es la norma ISO 27002 y para qué sirve?* https://www.globalsuitesolutions.com/es/que-es-la-norma-iso-27002-y-para-que-sirve/

Gob.ec. (07 de 03 de 2024). *CÓDIGO ORGÁNICO INTEGRAL PENAL COIP*. https://www.gob.ec/regulaciones/codigo-organico-integral-penal-coip

Hernadez Bejarano, M. (2020). *Ciclo de vida de desarrollo ágil de software serguro.* Fundación Universitaria Los Libertadores.

Hernandéz-Sampieri, R., & Mendoza Torres, C. P. (2018). *METODOLOGÍA DE LA INVESTIGACIÓN: LAS RUTAS CUANTITATIVA, CUALITATIVA Y MIXTA.* McGRAW-HILL INTERAMERICANA EDITORES, S.A. de C. V.

INNEVO CONSULTING. (2023). *20 Mejores Prácticas de Desarrollo de Software para Optimizar tus Proyectos*. Retrieved 27 de 10 de 2023, from https://blog.innevo.com/mejores-practicas-desarrollo-software

isms.online. (14 de 12 de 2023). *ISO 27002:2022, Control 8.4 – Acceso al código fuente*. es.isms.online: https://es.isms.online/iso-27002/control-8-4-access-to-source-code/

isms.online. (2023). *ISO 27002:2022, Control 8.9 – Gestión de la configuración*. CONFIGURATION MANAGEMENT: https://es.isms.online/iso-27002/control-8-9-configuration-management/

isms.online. (14 de 12 de 2023). *ISO 27002:2022, Control 8.9 – Gestión de la configuración*. es.isms.online: https://es.isms.online/iso-27002/control-8-9-configuration-management/

ISO. (07 de 03 de 2024). *ISO 17779:2021*. https://www.iso.org/es/contents/data/standard/07/64/76481.html

ISO. (2024). *ISO/IEC 27002:2022*. ISO: https://www.iso.org/es/contents/data/standard/07/56/75652.html

ISO. (22 de 02 de 2024). ISO: Normas mundiales para bienes y servicios de confianza. https://www.iso.org/es/home

ISO. (22 de 02 de 2024). ISO: Normas mundiales para bienes y servicios de confianza. https://www.iso.org/es/home

ISO. (22 de 02 de 2024). ISO: Normas mundiales para bienes y servicios de confianza. https://www.iso.org/es/home

ISO. (s.f.). ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection*. https://www.iso.org/es/contents/data/standard/07/56/75652.html

ISO. (s.f.). ISO/IEC 27002:2022. *Information security, cybersecurity and privacy protection*. https://www.iso.org/es/contents/data/standard/07/56/75652.html

ISOTools. (s.f.). Nueva ISO/IEC 27002:2022: cambios con respecto a la versión de 2013. https://www.isotools.us/2022/07/22/nueva-iso-iec-270022022-cambios-con-respecto-a-la-version-de-2013/

ITCL CENTRO TECNOLOGICO. (30 de 05 de 2022). Desarrollo seguro de software. https://itcl.es/blog/desarrollo-seguro-de-software/

Lifeder. (2020). *Investigación explicativa: características, técnicas, ejemplos*. Retrieved 02 de 11 de 2023, from https://www.lifeder.com/investigacion-explicativa/

Lifeder. (2020). *Investigación explicativa: características, técnicas, ejemplos*. Retrieved 02 de 11 de 2023, from https://www.lifeder.com/investigacion-explicativa/

MATEI, A. (07 de 01 de 2015). Guía para el desarrollo de Software Seguro.

Moron Peredo, K. (31 de 01 de 2023). Diseño e implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27002 para mejorar el nivel de seguridad informática en la empresa Rash Perú S.A.C. https://repositorio.uss.edu.pe/handle/20.500.12802/10629?show=full

QuestionPro. (2023). *Tipos de investigación y sus características*. Retrieved 02 de 11 de 2023, from https://www.questionpro.com/blog/es/tipos-de-investigacion-de-mercados/

SANCHO NÚÑEZ, J. (30 de 10 de 2020). Implementación de un Modelo de Desarrollo. https://dehesa.unex.es:8443/bitstream/10662/12316/1/TDUEX_2021_Sancho_Nunez.pdf

Thales. (2023). *¿Qué es la seguridad del software y por qué es tan importante ahora?* Retrieved 27 de 10 de 2023, from https://cpl.thalesgroup.com/es/software-monetization/what-is-software-security

UdeCataluña. (2023). *Seguridad informática: La importancia y lo que debe saber*. Retrieved 27 de 10 de 2023, from https://www.ucatalunya.edu.co/blog/seguridad-informatica-la-importancia-y-lo-que-debe-saber#:~:text=La%20seguridad%20inform%C3%A1tica%20o%20ciberseguridad,procesos%20por%20personas%20no%20autorizadas.

unir LA UNIVERSIDAD EN INTERNET. (14 de 05 de 2020). *Claves de las políticas de seguridad informática*. https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

Universidad Central del Ecuador. (2019). *DTIC*. Retrieved 01 de 11 de 2023, from uce.edu.ec: https://www.uce.edu.ec/administrativos

Universidad Central del Ecuador. (2019). *ESTATUTO*. Retrieved 01 de 11 de 2023, from https://drive.google.com/file/d/1YYR1d-ryEwhTXl4TkJ6OOMeyPTujp09I/view

Hernández Mera, D. A., & Recalde Varela, P. M. (2023). *UNIVERSIDAD TECNOLÓGICA ISRAEL*.

Joaquín, C., & Abundis, B. (n.d.). *Metodologías para desarrollar software seguro Methodologies for software security development*.

Valencia Lomas, G. A., & Recalde Varela, P. M. (2023). *UNIVERSIDAD TECNOLÓGICA ISRAEL*.

ANEXOS

ANEXO 1

FORMATO DE ENTREVISTA

Objetivo: Recopilar información mediante el planteamiento de preguntas cerradas, en base a los controles de la norma ISO/IEC 27002:2022
dirigidas a el Director, Coordinador del Área de Desarrollo de Software y Coordinador del Área de Infraestructura de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador, para el proyecto de investigación "Propuesta de políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador."

Datos de la entrevista:

Fecha de entrevista:	15/12/2023
Tiempo estimado de entrevista:	60 minutos
Lugar:	Dirección de Tecnologías de la Información y Comunicación

27002:2022 Cláusula 5	CONTROL	Cumple (C)	Cumple Parcialmente (CP)	Incumple (I)
1	Políticas para la seguridad de la información		-	
2	Roles y responsabilidades de seguridad de la información			
3	Segregación de deberes			
4	Responsabilidades de gestión (la dirección)			
5	Contacto con las autoridades			
6	Contacto con grupos de interés especial			
7	Inteligencia de amenazas			
8	Seguridad de la información en la gestión de proyectos			
9	Inventario de información y otros activos asociados			
10	Uso aceptable de información y otros activos asociados			
11	Retorno de los activos			
12	Clasificación de información			
13	Etiquetado de información			
14	Transferencia de información			
15	Control de acceso			
16	Gestión de identidad			
17	Información de autenticación			
18	Derechos de acceso			
19	Seguridad de la información en las relaciones con los proveedores			
20	Abordar la seguridad de la información dentro de los acuerdos de proveedores			
21	Gestión de la seguridad de la información en la cadena de suministro de las TIC			
22	Monitoreo, revisión y gestión de cambios de servicios de proveedores			
23	Seguridad de la información para el uso de servicios en la nube			
24	Gestión de incidentes de seguridad de la información Planificación y preparación			
25	Evaluación y decisión sobre eventos de seguridad de la información			
26	Respuesta a incidentes de seguridad de la información			
27	Aprender de los incidentes de seguridad de la información			
28	Recopilación de evidencia			
29	Seguridad de la información durante eventos disruptivos			
30	Preparación para las TIC para la continuidad del negocio			
31	Requisitos legales, legales, regulatorios y contractuales			
32	Derechos de propiedad intelectual			
33	Protección de registros			
34	Privacidad y protección de PII			
35	Revisión independiente de la seguridad de la información			
36	Cumplimiento de las políticas, reglas y estándares para la seguridad de la información			
37	Procedimientos operativos documentados			

Objetivo: Recopilar información mediante el planteamiento de preguntas cerradas, en base a los controles de la norma ISO/IEC 27002:2022 dirigidas a el Director, Coordinador del Área de Desarrollo de Software y Coordinador del Área de Infraestructura de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador, para el proyecto de investigación "Propuesta de políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador."				
Datos de la entrevista:				
Fecha de entrevista: **Tiempo estimado de entrevista:** **Lugar:**		15/12/2023 60 minutos Dirección de Tecnologías de la Información y Comunicación		
27002:2022 Cláusula 6	**CONTROL**	**Cumple (C)**	**Cumple Parcialmente (CP)**	**Incumple (I)**
1	Selección			
2	Términos y condiciones de empleo			
3	Conciencia de seguridad, educación y capacitación de la información			
4	Proceso Disciplinario			
5	Responsabilidades después de la terminación o cambio de empleo			
6	Acuerdos de confidencialidad o no divulgación			
7	Trabajo remoto			
8	Informes de eventos de seguridad de la información			

Objetivo: Recopilar información mediante el planteamiento de preguntas cerradas, en base a los controles de la norma ISO/IEC 27002:2022 dirigidas a el Director, Coordinador del Área de Desarrollo de Software y Coordinador del Área de Infraestructura de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador, para el proyecto de investigación "Propuesta de políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador."				
Datos de la entrevista:				
Fecha de entrevista: **Tiempo estimado de entrevista:** **Lugar:**		15/12/2023 60 minutos Dirección de Tecnologías de la Información y Comunicación		
27002:2022 Cláusula 7	**CONTROL**	**Cumple (C)**	**Cumple Parcialmente (CP)**	**Incumple (I)**
1	Perímetros de seguridad física			
2	Entrada física			
3	Asegurar oficinas, habitaciones e instalaciones			
4	Monitoreo de seguridad física			
5	Protección contra amenazas físicas y ambientales			
6	Trabajando en áreas seguras			
7	Descripción de la pantalla y pantalla clara			
8	Manejo de equipos y protección			
9	Seguridad de activos fuera de las instalaciones			
10	Medios de almacenamiento			
11	Soporte de servicios públicos			
12	Cableado de seguridad			
13	Mantenimiento de equipo			
14	Eliminación o reutilización segura del equipo			

Objetivo: Recopilar información mediante el planteamiento de preguntas cerradas, en base a los controles de la norma ISO/IEC 27002:2022
dirigidas a el Director, Coordinador del Área de Desarrollo de Software y Coordinador del Área de Infraestructura de la Dirección de Tecnologías de la Información y Comunicación de la Universidad Central del Ecuador, para el proyecto de investigación "Propuesta de políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la Universidad Central del Ecuador."

Datos de la entrevista:

Fecha de entrevista:	15/12/2023
Tiempo estimado de entrevista:	60 minutos
Lugar:	Dirección de Tecnologías de la Información y Comunicación

27002:2022 Cláusula 8	CONTROL	Cumple (C)	Cumple Parcialmente (CP)	Incumple (I)
1	Dispositivos de punto final del usuario			
2	Derechos de acceso privilegiados			
3	Restricción de acceso a la información			
4	Acceso al código fuente			
5	Autenticación segura			
6	Gestión de capacidad			
7	Protección contra malware			
8	Gestión de vulnerabilidades técnicas			
9	Gestión de configuración			
10	Eliminación de información			
11	Enmascaramiento de datos			
12	Prevención de fugas de datos			
13	Copia de seguridad de la información			
14	Redundancia de instalaciones de procesamiento de información			
15	Registro			
16	Actividades de monitoreo			
17	Sincronización de reloj			
18	Uso de programas de utilidad privilegiados			
19	Instalación de software en sistemas operativos			
20	Seguridad de las redes			
21	Seguridad de los servicios de red			
22	Segregación de redes			
23	Filtrado web			
24	Uso de la criptografía			
25	Ciclo de vida de desarrollo seguro			
26	Requisitos de seguridad de la aplicación			
27	Principios de arquitectura e ingeniería de sistema seguro			
28	Codificación segura			
29	Pruebas de seguridad en desarrollo y aceptación			
30	Desarrollo subcontratado			
31	Separación de entornos de desarrollo, prueba y producción			
32	Gestión del cambio			
33	Información de prueba			
34	Protección de sistemas de información durante las pruebas de auditoría			

ANEXO 2

MATRIZ PONDERA DE SITUACIÓN INICIAL DE REQUISITOS DE LA NORMA ISO 27002:2022

MATRIZ PONDERADA DE SITUACIÓN INICIAL DE REQUISITOS DE LA NORMA ISO 27002:2022

UNIVERSIDAD CENTRAL DEL ECUADOR

DIRECCION DE TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN

FECHA: 17 de Febrero del 2024

27002:2022	CONTROL	PONDERACION	CALIFICACION CUMPLE = 2 CUMPLE PARCIAL=1 INCUMPLE=0
5,1	Políticas para la seguridad de la información	2	0
5,2	Roles y responsabilidades de seguridad de la información	2	2
5,3	Segregación de deberes	2	2
5,4	Responsabilidades de gestión (la dirección)	2	1
5,5	Contacto con las autoridades	2	2
5,6	Contacto con grupos de interés especial	2	2
5,7	Inteligencia de amenazas	2	2
5,8	Seguridad de la información en la gestión de proyectos	2	2
5,9	Inventario de información y otros activos asociados	2	2
5.10	Uso aceptable de información y otros activos asociados	2	1
5,11	Retorno de los activos	2	2
5,12	Clasificación de información	2	2
5,13	Etiquetado de información	2	2
5,14	Transferencia de información	2	1
5,15	Control de acceso	2	2
5,16	Gestión de identidad	2	1
5,17	Información de autenticación	2	2
5,18	Derechos de acceso	2	2
5,19	Seguridad de la información en las relaciones con los proveedores	2	2
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	2	2

27002:2022	CONTROL	PONDERACION	CALIFICACION CUMPLE = 2 CUMPLE PARCIAL=1 INCUMPLE=0
5,16	Gestión de identidad	2	1
5,17	Información de autenticación	2	2
5,18	Derechos de acceso	2	2
5,19	Seguridad de la información en las relaciones con los proveedores	2	2
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	2	2
5,21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	2	2
5,22	Monitoreo, revisión y gestión de cambios de servicios de proveedores	2	1
5,23	Seguridad de la información para el uso de servicios en la nube	2	2
5,24	Gestión de incidentes de seguridad de la información Planificación y preparación	2	1
5,25	Evaluación y decisión sobre eventos de seguridad de la información	2	1
5,26	Respuesta a incidentes de seguridad de la información	2	1
5,27	Aprender de los incidentes de seguridad de la información	2	1
5,28	Recopilación de evidencia	2	2
5,29	Seguridad de la información durante eventos disruptivos	2	2
5.30	Preparación para las TIC para la continuidad del negocio	2	2
5,31	Requisitos legales, legales, regulatorios y contractuales	2	1
5,32	Derechos de propiedad intelectual	2	2
5,33	Protección de registros	2	2
5,34	Privacidad y protección de PII	2	2
5,35	Revisión independiente de la seguridad de la información	2	2
5,36	Cumplimiento de las políticas, reglas y estándares para la seguridad de la información	2	1
5,37	Procedimientos operativos documentados	2	1
		74	**60**

27002:2022	CONTROL	PONDERACION	CALIFICACION
6,1	Selección	2	2
6,2	Términos y condiciones de empleo	2	1
6,3	Conciencia de seguridad, educación y capacitación de la información	2	2
6,4	Proceso Disciplinario	2	2
6,5	Responsabilidades después de la terminación o cambio de empleo	2	2
6,6	Acuerdos de confidencialidad o no divulgación	2	2
6,7	Trabajo remoto	2	2
6,8	Informes de eventos de seguridad de la información	2	2
		16	**15**

27002:2022	CONTROL	PONDERACION	CALIFICACION
7,1	Perímetros de seguridad física	2	2
7,2	Entrada física	2	2
7,3	Asegurar oficinas, habitaciones e instalaciones	2	2
7,4	Monitoreo de seguridad física	2	2
7,5	Protección contra amenazas físicas y ambientales	2	2
7,6	Trabajando en áreas seguras	2	1
7,7	Descripción de la pantalla y pantalla clara	2	1
7,8	Manejo de equipos y protección	2	2
7,9	Seguridad de activos fuera de las instalaciones	2	2
7.10	Medios de almacenamiento	2	1
7,11	Soporte de servicios públicos	2	2
7,12	Cableado de seguridad	2	2
7,13	Mantenimiento de equipo	2	2
7,14	Eliminación o reutilización segura del equipo	2	1
		60	**54**

27002:2022	CONTROL	PONDERACION	CALIFICACION
8,1	Dispositivos de punto final del usuario	2	2
8,2	Derechos de acceso privilegiados	2	2
8,3	Restricción de acceso a la información	2	2
8,4	Acceso al código fuente	2	1
8,5	Autenticación segura	2	2
8,6	Gestión de capacidad	2	1
8,7	Protección contra malware	2	1
8,8	Gestión de vulnerabilidades técnicas	2	1
8,9	Gestión de configuración	2	1
8.10	Eliminación de información	2	1
8,11	Enmascaramiento de datos	2	2
8,12	Prevención de fugas de datos	2	2
8,13	Copia de seguridad de la información	2	2
8,14	Redundancia de instalaciones de procesamiento de información	2	1
8,15	Registro	2	2
8,16	Actividades de monitoreo	2	1
8,17	Sincronización de reloj	2	2
8,18	Uso de programas de utilidad privilegiados	2	1
8,19	Instalación de software en sistemas operativos	2	0
8.20	Seguridad de las redes	2	1
8,21	Seguridad de los servicios de red	2	1
8,22	Segregación de redes	2	1
8,23	Filtrado web	2	1
8,24	Uso de la criptografía	2	2
8,25	Ciclo de vida de desarrollo seguro	2	0
8,26	Requisitos de seguridad de la aplicación	2	0
8,27	Principios de arquitectura e ingeniería de sistema seguro	2	1
8,28	Codificación segura	2	2
8,29	Pruebas de seguridad en desarrollo y aceptación	2	1
8.30	Desarrollo subcontratado	2	2
8,31	Separación de entornos de desarrollo, prueba y producción	2	1
8,32	Gestión del cambio	2	0
8,33	Información de prueba	2	0
8,34	Protección de sistemas de información durante las pruebas de audit	2	0

ANEXO 3

MATRIZ DE SITUACION INICIAL DE LOS REQUISITOS DE LA NORMA ISO/IEC 27002:2022

27002:2022	CONTROL	C	CP	I
5,1	Políticas para la seguridad de la información			X
5,2	Roles y responsabilidades de seguridad de la información	X		
5,3	Segregación de deberes	X		
5,4	Responsabilidades de gestión (la dirección)		X	
5,5	Contacto con las autoridades	X		
5,6	Contacto con grupos de interés especial	X		
5,7	Inteligencia de amenazas	X		
5,8	Seguridad de la información en la gestión de proyectos	X		
5,9	Inventario de información y otros activos asociados	X		
5.10	Uso aceptable de información y otros activos asociados		X	
5,11	Retorno de los activos	X		
5,12	Clasificación de información	X		
5,13	Etiquetado de información	X		
5,14	Transferencia de información		X	
5,15	Control de acceso	X		
5,16	Gestión de identidad		X	
5,17	Información de autenticación	X		
5,18	Derechos de acceso	X		
5,19	Seguridad de la información en las relaciones con los proveedores	X		
5.20	Abordar la seguridad de la información dentro de los acuerdos de proveedores	X		
5,21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	X		
5,22	Monitoreo, revisión y gestión de cambios de servicios de proveedores		X	
5,23	Seguridad de la información para el uso de servicios en la nube	X		
5,24	Gestión de incidentes de seguridad de la información Planificación y preparación		X	
5,25	Evaluación y decisión sobre eventos de seguridad de la información		X	
5,26	Respuesta a incidentes de seguridad de la información		X	
5,27	Aprender de los incidentes de seguridad de la información		X	
5,28	Recopilación de evidencia	X		
5,29	Seguridad de la información durante eventos disruptivos	X		
5.30	Preparación para las TIC para la continuidad del negocio	X		
5,31	Requisitos legales, legales, regulatorios y contractuales		X	

27002:2022	CONTROL	C	CP	I
5,32	Derechos de propiedad intelectual	X		
5,33	Protección de registros	X		
5,34	Privacidad y protección de PII	X		
5,35	Revisión independiente de la seguridad de la información	X		
5,36	Cumplimiento de las políticas, reglas y estándares para la seguridad de la información		X	
5,37	Procedimientos operativos documentados		X	
6,1	Selección	X		
6,2	Términos y condiciones de empleo		X	
6,3	Conciencia de seguridad, educación y capacitación de la información	X		
6,4	Proceso Disciplinario	X		
6,5	Responsabilidades después de la terminación o cambio de empleo	X		
6,6	Acuerdos de confidencialidad o no divulgación	X		
6,7	Trabajo remoto	X		
6,8	Informes de eventos de seguridad de la información	X		
7,1	Perímetros de seguridad física	X		
7,2	Entrada física	X		
7,3	Asegurar oficinas, habitaciones e instalaciones	X		
7,4	Monitoreo de seguridad física	X		
7,5	Protección contra amenazas físicas y ambientales	X		
7,6	Trabajando en áreas seguras		X	
7,7	Descripción de la pantalla y pantalla clara		X	
7,8	Manejo de equipos y protección	X		
7,9	Seguridad de activos fuera de las instalaciones	X		
7.10	Medios de almacenamiento		X	
7,11	Soporte de servicios públicos	X		
7,12	Cableado de seguridad	X		
7,13	Mantenimiento de equipo	X		
7,14	Eliminación o reutilización segura del equipo		X	
8,1	Dispositivos de punto final del usuario	X		
8,2	Derechos de acceso privilegiados	X		
8,3	Restricción de acceso a la información	X		
8,4	Acceso al código fuente		X	
8,5	Autenticación segura	X		
8,8	Gestión de vulnerabilidades técnicas		X	

27002:2022	CONTROL	C	CP	I
8,9	Gestión de configuración		X	
8.10	Eliminación de información		X	
8,11	Enmascaramiento de datos	X		
8,12	Prevención de fugas de datos	X		
8,13	Copia de seguridad de la información	X		
8,14	Redundancia de instalaciones de procesamiento de información		X	
8,15	Registro	X		
8,16	Actividades de monitoreo		X	
8,17	Sincronización de reloj	X		
8,18	Uso de programas de utilidad privilegiados		X	
8,19	Instalación de software en sistemas operativos			X
8.20	Seguridad de las redes		X	
8,21	Seguridad de los servicios de red		X	
8,22	Segregación de redes		X	
8,23	Filtrado web		X	
8,24	Uso de la criptografía	X		
8,25	Ciclo de vida de desarrollo seguro			X
8,26	Requisitos de seguridad de la aplicación			X
8,27	Principios de arquitectura e ingeniería de sistema seguro		X	
8,28	Codificación segura	X		
8,29	Pruebas de seguridad en desarrollo y aceptación		X	
8.30	Desarrollo subcontratado	X		
8,31	Separación de entornos de desarrollo, prueba y producción		X	
8,32	Gestión del cambio			X
8,33	Información de prueba			X
8,34	Protección de sistemas de información durante las pruebas de auditoría			X

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: Propuesta de Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la 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. Nora Catalina Quimbita Caiza Msc.

Título obtenido
MAGISTER EN SISTEMAS DE GESTIÓN INTEGRADOS
Cédula de Identidad
1712407269
E- mail
nquimbita@uce.edu.ec
Institución de Trabajo
UNIVERSIDAD CENTRAL DEL ECUADOR
Cargo
DIRECTORA ADMINISTRATIVA (e)
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: Propuesta de Políticas de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la 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*	5				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*		4			
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	5				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	5				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	5				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		4			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	5				
Total		33				

Observaciones:

El proyecto de investigación contribuye a que el desarrollo de sistemas web en la Universidad Central del Ecuador, cuente con un instrumento que permita garantizar la seguridad de la información enmarcado en la norma ISO/IEC 27002:2022.

Recomendaciones

Este tipo de investigaciones contribuye al mejoramiento en la ejecución de los procesos académicos y administrativos, que se ejecutan en la institución, para el cumplimiento de sus objetivos, por tanto, se recomienda la implementación, así como el seguimiento y control del cumplimiento de las Políticas.

Lugar, fecha de validación: Quito, 7 de marzo del 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: Propuesta del plan de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la 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. Luis Alfredo Gualoto Guachamin.

Título obtenido
INGENIERO EN SISTEMAS DE LA INFORMACIÓN
Cédula de Identidad
1715759724
E- mail
lagualoto@uce.edu.ec
Institución de Trabajo
UNIVERSIDAD CENTRAL DEL ECUADOR
Cargo
ANALISTA DE TECNOLOGÍAS 1
Años de experiencia en el área
8 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 del plan de seguridad informática en el desarrollo de sistemas web, aplicando la norma ISO 27002, para la 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*	5				
Aplicabilidad	*La capacidad de implementación de la propuesta considerando que los contenidos sean aplicables*	5				
Conceptualización	*La base de conceptos y teorías propias de la propuesta de manera sistémica y articulada*	5				
Actualidad	*Los procedimientos actuales y los cambios científicos y tecnológicos considerados en la propuesta*	5				
Calidad Técnica	*Los atributos cualitativos del contenido de la propuesta para satisfacer las expectativas de sus beneficiarios*	5				
Factibilidad	*El nivel de utilización de la propuesta por parte de la organización acorde a los recursos disponibles*		4			
Pertinencia	*La contundencia y conveniencia de la propuesta para solucionar el problema planteado.*	5				
Total		34				

Observaciones:

El tema de investigación constituye un aporte significativo para la ejecución de actividades que permitan garantizar la confidencialidad, integridad y disponibilidad en el manejo de la información en el desarrollo de sistemas web en la Universidad Central del Ecuador.

Recomendaciones

Para complementar la investigación de este proyecto, se debe considerar ampliar su alcance, con el desarrollo de todos los controles que integran la norma ISO/27002:2022 extendiéndose a las diferentes áreas que integran la Dirección de Tecnologías de la Información y Comunicación.

Lugar, fecha de validación: Quito, 7 de marzo del 2024

Firmado electrónicamente por:
LUIS ALFREDO GUALOTO GUACHAMIN

Firma del especialista