REPÚBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE POSGRADO

MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA

TEMA:

PROPUESTA PARA LA CREACIÓN DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS (CSIRT) EN LA UNIVERSIDAD CENTRAL DEL ECUADOR

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

AUTOR: Ing. Jorge Luis Rivera Guaman

DIRECTOR: Ing. Yoo Sang Guun, Ph.D.

ASESOR: Ing. Alexander Guevara Vega MSc.

IBARRA - ECUADOR

2025

AGRADECIMIENTO

Quisiera expresar mi más sincero agradecimiento a todas las personas que me han apoyado a lo largo de este camino. En primer lugar, a mi familia, cuyos valores y amor incondicional me han dado la fuerza para seguir adelante. A mis padres, por su constante aliento y por enseñarme la importancia de la dedicación y el esfuerzo. A mis hermanos, por ser mis mejores aliados y por siempre estar a mi lado, brindándome su apoyo inquebrantable.

A mi querida hija, Victoria, gracias por tu paciencia y por ser la luz de mi vida. Tu sonrisa me ha dado fuerzas en los momentos más desafiantes y es un recordatorio constante de por qué he trabajado tan arduamente.

Quiero agradecer también a mis docentes, quienes me han guiado y me han brindado su conocimiento y apoyo a lo largo de esta travesía académica. Su dedicación y pasión por la enseñanza han sido una fuente de inspiración.

Por último, pero no menos importante, a mis amigos, que siempre han estado allí, animándome y brindándome su apoyo incondicional. Sin su compañía y aliento, este proceso habría sido mucho más difícil.

A todos ustedes, gracias por ser parte de este viaje. No podría haber llegado hasta aquí sin cada uno de ustedes.

DEDICATORIA

Dedico esta tesis a mi querida hija, Victoria, quien ilumina mi vida y me motiva a ser la mejor versión de mí mismo. Espero que crezcas en un mundo donde siempre persigas tus sueños con valentía y amor.

A mis hermanos, quienes han sido mis pilares a lo largo de este camino. Su apoyo incondicional, risas y sabios consejos han hecho que cada desafío se sienta más ligero y cada logro más significativo.

Gracias por estar siempre a mi lado y por ser la mejor familia que podría desear.

Un agradecimiento especial a Evelin, cuya presencia ha sido un faro de motivación constante. Tu apoyo incondicional y tus palabras de aliento han sido un impulso fundamental en este viaje.

CONFORMIDAD DEL DOCUMENTO

UNIVERSIDAD TÉCNICA DEL NORTE
Acreditada Resolución Nro. 173-SE-33-CACES-2020
FACULTAD DE POSGRADO

Ibarra, 19 de noviembre de 2024

Dra.
Lucía Yépez
DECANA FACULTAD DE POSGRADO

ASUNTO: Conformidad con el documento final

Señora Decana:

Nos permitimos informar a usted que, revisado el Trabajo final de Grado "PROPUESTA DE CREACIÓN DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS (CSIRT) EN LA UNIVERSIDAD CENTRAL DEL ECUADOR", del maestrante RIVERA GUAMAN JORGE LUIS, de la Maestría en Computación mención Seguridad Informática, certificamos que han sido acogidas y satisfechas todas las observaciones realizadas.

Atentamente,

	Apellidos y Nombres	Firma
Director	Ph.D. Yoo Sang Guun	SANG GUUN YOO
Asesor	MSc. Alexander Guevara Vega	VICENTE ALEXANDER GUEVARA VEGA

Ciudadela Universitaria Barrio El Olivo
Av.17 de Julio 5-21 y Gral. José María Córdova
Ibarra-Ecuador
Teléfono: (06) 2997-800 RUC: 1060001070001
www.utn.edu.ec

AUTORIZACIÓN BIBLIOTECA

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

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

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1104751415		
APELLIDOS Y NOMBRES:	RIVERA GUAMAN JORGE LUIS		
DIRECCIÓN:	QUITO, ATACAMES N23-252 Y LA GASCA		
EMAIL:	jlriverag@uce.edu.ec		
TELÉFONO FIJO:	0983194202	**TELÉFONO MÓVIL:**	0983194202

DATOS DE LA OBRA			
TÍTULO:	PROPUESTA PARA LA CREACIÓN DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS (CSIRT) EN LA UNIVERSIDAD CENTRAL DEL ECUADOR		
AUTOR (ES):	RIVERA GUAMAN JORGE LUIS		
FECHA: DD/MM/AAAA	06/02/2025		
SOLO PARA TRABAJOS DE GRADO			
PROGRAMA:	☐ **GRADO**	X	**POSGRADO**
TITULO POR EL QUE OPTA:	**Magíster en Computación con Mención en Seguridad Informática**		
ASESOR /DIRECTOR:	**Ing. Yoo Sang Guun, Ph.D.**		

2. CONSTANCIAS

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

Ibarra, a los 06 días del mes de febrero de 2025

EL AUTOR:

JORGE LUIS RIVERA GUAMAN

JORGE RIVERA

RESUMEN EJECUTIVO

Este documento presenta la propuesta para implementar un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) en la Universidad Central del Ecuador (UCE), fundamentada en un análisis exhaustivo realizado durante 2024.

La evaluación de la infraestructura tecnológica actual revela vulnerabilidades críticas en la gestión de incidentes de seguridad. Durante el período mayo-agosto 2024, se documentaron 285 incidentes, registrando tiempos de respuesta que exceden los estándares aceptables del sector académico.

El modelo propuesto contempla un CSIRT híbrido especializado en capacitación, compuesto por un equipo central de siete especialistas y una red de 21 enlaces facultativos. Esta estructura optimiza recursos y garantiza cobertura institucional integral. La inversión inicial requerida asciende a $420,399.60 anuales, contemplando personal, infraestructura y programas de capacitación.

La implementación proyecta una reducción significativa de incidentes: 30% en el primer año y 60% al tercer año de operación. Los indicadores clave de rendimiento incluyen la optimización de tiempos de respuesta a 8 horas y el fortalecimiento mensurable de la cultura de ciberseguridad institucional.

El plan de implementación, diseñado para ejecutarse en 12 meses, prioriza el desarrollo de capacidades internas y el establecimiento de colaboraciones estratégicas con otros CSIRTs académicos. Este enfoque asegura la sostenibilidad del proyecto y su alineación con estándares internacionales de ciberseguridad.

La materialización de esta propuesta es imperativa para salvaguardar los activos digitales de la UCE y garantizar la continuidad operativa de sus funciones académicas y administrativas en un entorno digital cada vez más complejo.

EXECUTIVE SUMMARY

This document presents a proposal to implement a Computer Security Incident Response Team (CSIRT) at Universidad Central del Ecuador (UCE), based on comprehensive analysis conducted during 2024.

The assessment of current technological infrastructure reveals critical vulnerabilities in security incident management. Between May-August 2024, 285 incidents were documented, with response times exceeding acceptable standards in the academic sector.

The proposed model envisions a hybrid CSIRT specializing in training, comprising a core team of seven specialists and a network of 21 faculty liaisons. This structure optimizes resources and ensures comprehensive institutional coverage. The required initial investment amounts to $420,399.60 annually, covering personnel, infrastructure, and training programs.

Implementation projects significant incident reduction: 30% in the first year and 60% by the third year of operation. Key performance indicators include optimization of response times to 8 hours and measurable strengthening of institutional cybersecurity culture.

The implementation plan, designed for 12-month execution, prioritizes internal capacity development and establishment of strategic collaborations with other academic CSIRTs. This approach ensures project sustainability and alignment with international cybersecurity standards.

The realization of this proposal is imperative to safeguard UCE's digital assets and ensure operational continuity of its academic and administrative functions in an increasingly complex digital environment.

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

CAPITULO I

EL PROBLEMA

1.1 Introducción

1.1.1 La Importancia de la Ciberseguridad en el Ámbito Académico

Dado que las universidades manejan grandes cantidades de datos confidenciales y valiosos, la ciberseguridad es un aspecto importante del mundo académico. Estas instituciones almacenan no sólo la información personal de estudiantes, Docentes y administradores, sino también materiales de investigación académica, resultados de aprendizaje y comunicaciones internas. Proteger estos materiales es fundamental para mantener la integridad académica, la confidencialidad y la seguridad general de la comunidad universitaria.

En un entorno en el que la tecnología de la información es cada vez más popular, las universidades se enfrentan a diversas amenazas cibernéticas. Los ataques de phishing, ransomware y otros tipos de malware son comunes y pueden tener consecuencias catastróficas. Crear un equipo de respuesta a incidentes de ciberseguridad CSIRTse está convirtiendo en una estrategia esencial para mitigar estos riesgos y garantizar un entorno digital seguro.

Según Villegas-Ch., Ortiz-Garcés y Sánchez-Viteri (2021), los CSIRT en los campus universitarios desempeñan un papel vital en la gestión de incidentes de seguridad al proporcionar un marco estructurado y eficaz para la detección, el análisis y los métodos de respuesta a incidentes. Amenazas cibernéticas. Además, promueve una cultura de ciberseguridad entre estudiantes, Docentes y personal mediante la promoción de prácticas seguras y conciencia de riesgos.

1.1.2 Relevancia para la UCE

La UCE es una de las instituciones de educación superior más grandes y prestigiosas del país. Con una comunidad académica grande y diversa y una infraestructura tecnológica compleja, la UCE enfrenta desafíos de ciberseguridad únicos. Proteger la información y asegurar la continuidad de sus operaciones académicas y administrativas son fundamentales para cumplir con su misión docente e investigadora.

La importancia de la seguridad de la red y la UCE se refleja en varios aspectos. En primer lugar, las universidades manejan grandes cantidades de datos personales sobre estudiantes, Docentes y personal y deben protegerlos del acceso no autorizado y de las fugas de datos. En segundo lugar, la integridad de la investigación académica depende de un entorno seguro y confiable. Finalmente, las interrupciones del servicio debido a

incidentes de seguridad pueden tener un impacto grave en el proceso educativo y la reputación de la institución.

1.2 Planteamiento del problema

1.2.1 Riesgos y Desafíos de Ciberseguridad en la UCE

UCE enfrenta desafíos específicos de ciberseguridad, incluida la exposición a una variedad de amenazas en línea, como malware, phishing y ataques de denegación de servicio (DDoS). Estos riesgos se ven agravados por una falta de respuesta adecuada a los incidentes de seguridad, una capacitación inadecuada de los empleados en prácticas de ciberseguridad y una infraestructura tecnológica inadecuada para detectar y responder eficazmente a estas amenazas.

Los entornos académicos requieren inherentemente un equilibrio entre la apertura a la colaboración y la investigación y la necesidad de proteger material sensible. Esta situación crea desafíos adicionales para implementar medidas de seguridad efectivas sin obstaculizar la misión educativa de la universidad. Además, la diversidad de dispositivos y sistemas utilizados por los estudiantes y el personal complica aún más la gestión de la seguridad.

1.2.2 Impacto de los Incidentes de Seguridad de TI

Los incidentes de seguridad informática pueden tener graves consecuencias para la UCE. Estos problemas pueden incluir interrupción de servicios esenciales, pérdida de datos críticos y pérdida de confianza entre los miembros de la comunidad universitaria. Por ejemplo, un ataque de ransomware podría paralizar los sistemas administrativos, haciendo que el registro, la votación y otros procesos importantes sean inmanejables.

En junio de 2024, la plataforma de soporte de la universidad registró 239 casos relacionados con la seguridad de la información interna de UCE, 30 de los cuales estaban relacionados con problemas con correos electrónicos interceptados por spam o virus. Estos incidentes no solo impactan la eficiencia operativa, sino que también representan una amenaza directa a la integridad y confidencialidad de los datos (Instituto Nacional de Seguridad Cibernética, 2023).

1.3 CSIRT requerido dentro de UCE

1.3.1 Fortalecer la seguridad de la red

La creación del CSIRT es fundamental para mejorar la capacidad de la Universidad para detectar y responder a incidentes de ciberseguridad. Un CSIRT dedicado proporciona una respuesta organizada y eficaz a un incidente de seguridad, minimizando su impacto y evitando que se repita. Además, el CSIRT puede implementar actividades proactivas, como evaluaciones de vulnerabilidad y capacitación en ciberseguridad, para prevenir futuros incidentes, es relevante considerar que existen varios equipos de respuesta ante incidentes dentro de los cuales parecerían lo mismo, pero cambian en su forma de ofrecer los servicios o el enfoque de trabajar, a continuación, explicamos en la siguiente imagen.

Imagen 1 Complementariedad de los Equipos de Respuesta

(Segurilatam, 2023)

La necesidad de responder a las incidencias informáticas a través de la historia se ha mejorado el enfoque y los nombres de los equipos adjuntamos una imagen:

Imagen 2 Diferentes Nombres Un Concepto Similar

(Adeva & Vera, 2021, p. 83)

Hemos decidido trabajar sobre el CSIRT considerando que es muy adaptable a las instituciones educativas con pocos recursos en el área de tecnología. El establecimiento del CSIRT también ayudará a adoptar las mejores prácticas en ciberseguridad, alinearse con los estándares internacionales y mejorar la postura de seguridad de la universidad. El equipo no solo será responsable de la respuesta a incidentes, sino que también desarrollará estrategias de prevención y mitigación de riesgos para contribuir a la resiliencia cibernética de la agencia.

1.3.2 Beneficios para la Comunidad Universitaria

CSIRT no sólo mejora la seguridad de la información, sino que también beneficia a todos los miembros de la comunidad universitaria. El establecimiento del CSIRT ayudará a proteger los datos personales y académicos, garantizará la continuidad de las actividades académicas y administrativas y promoverá una cultura de seguridad entre los estudiantes, Docentes y personal administrativo.

Las actividades de capacitación continua y concientización sobre ciberseguridad son componentes importantes del CSIRT. Estas medidas aumentarán la conciencia sobre la importancia de la seguridad digital y la adopción de prácticas de seguridad, ayudando así a reducir los riesgos y mejorar la resiliencia frente a las ciberamenazas.

1.4 Objetivos de la investigación

1.4.1 Objetivo principal

Proponer un modelo de CSIRT Académico para la UCE que permita mejorar la detección y respuesta a los incidentes de seguridad informática, mediante la capacitación sobre ciberseguridad entre la comunidad universitaria.

1.4.2 Objetivos específicos

1. Analizar las mejores prácticas internacionales en la creación y operación de CSIRTs Académicos.

2. Describir la situación actual de la ciberseguridad en la UCE, identificando los principales riesgos y desafíos a los que se enfrenta.

3. Proponer un modelo de CSIRT Académico para la UCE que responda a las necesidades específicas de la institución.

1.5 Justificación

1.5.1 Impacto del CSIRT

El establecimiento del CSIRT tendrá un impacto profundo y positivo en la agencia. En un entorno cada vez más dependiente de la tecnología, donde las ciberamenazas aumentan y se vuelven más sofisticadas, contar con un CSIRT es fundamental para garantizar la protección de los activos digitales de la Universidad.

En primer lugar, un CSIRT eficaz permitirá a la UCE reducir la frecuencia y gravedad de los incidentes de seguridad. A través de una detección temprana y una respuesta rápida a amenazas como malware, phishing y ataques de denegación de servicio (DDoS), CSIRT mitigará los riesgos que estos incidentes plantean para la integridad, confidencialidad y disponibilidad de los datos. La máxima prioridad será proteger la información confidencial, incluidos los datos personales de estudiantes, Docentes y administradores, así como información crítica de investigación académica. Este nivel de protección es fundamental no sólo para evitar pérdidas financieras y daños operativos, sino también para mantener la confianza de la comunidad universitaria y los socios externos.

Un CSIRT mejorará significativamente la capacidad de la Universidad para responder a posibles ciberataques. La capacidad de recuperarse rápidamente de incidentes cibernéticos minimizará las interrupciones en las actividades académicas y administrativas y garantizará la continuidad de los procesos educativos y administrativos. Este enfoque proactivo no solo mantiene la eficiencia operativa de UCE, sino que también mejora su capacidad para adaptarse a nuevas amenazas cibernéticas, creando un entorno más seguro y sólido.

La creación del CSIRT también tendrá un impacto positivo en la reputación de la UCE. Al demostrar un compromiso claro y proactivo con la ciberseguridad, la universidad podrá posicionarse como una institución líder en seguridad digital en educación. Esta reputación no sólo atraerá a más estudiantes y académicos interesados en un entorno seguro de aprendizaje e investigación, sino que también aumentará la colaboración con otras instituciones y entidades que valoran la seguridad de la información.

1.5.2 Contribución Académica

La investigación y la implementación del CSIRT no sólo beneficiarán directamente a las universidades, sino que también harán una contribución significativa a la documentación y práctica de la ciberseguridad en las instituciones educativas. El programa proporcionará un modelo CSIRT detallado y personalizado que tendrá en cuenta las necesidades y características específicas de una universidad como la UCE, proporcionando un valioso estudio de caso para otras instituciones en Ecuador.

A medida que implementemos el CSIRT, este estudio proporcionará una guía práctica basada en evidencia para que otras universidades sigan su ejemplo. Las recomendaciones y mejores prácticas derivadas de este estudio ayudarán a otras instituciones educativas a abordar desafíos de ciberseguridad similares mediante la promoción de enfoques colaborativos y compartidos en toda la región.

Este trabajo también ayudará a desarrollar políticas y prácticas de ciberseguridad más efectivas en entornos universitarios. Al identificar vulnerabilidades específicas y necesidades de capacitación dentro de la UCE, esta investigación ayudará a desarrollar estrategias que no solo aborden las amenazas actuales, sino que también ayuden a preparar a la comunidad universitaria para amenazas futuras. Por ejemplo, la integración de programas de concientización y capacitación en ciberseguridad dentro del CSIRT fomentará una cultura de ciberseguridad que es fundamental para la sostenibilidad a largo plazo de las prácticas de ciberseguridad universitaria.

La creación de un CSIRT en la UCE no solo mejorará significativamente la seguridad y la resiliencia de la universidad ante incidentes cibernéticos, sino que también enriquecerá el conocimiento y las prácticas de ciberseguridad del sector educativo, beneficiando a instituciones similares.

1.6 Alcance y Limitación

El alcance del estudio se centrará en la propuesta y diseño de un modelo de CSIRT para la UCE, este modelo incluirá la estructura organizativa, las funciones y responsabilidades del equipo, y los procesos y procedimientos necesarios para la gestión de incidentes de ciberseguridad.

Es fundamental para la UCE mejorar la capacidad de detección y respuesta ante ciberataques, sin embargo, una de las mejores herramientas para combatir los ataques informáticos es la prevención que se logra a través de capacitación y concientización en seguridad informática, por tal motivo, el CSIRT debe estar enfocado en el servicio de capacitación.

CAPITULO II

MARCO DE REFERENCIA

2.1 Revisión de la literatura

2.1.1 Definición y objetivos del CSIRT

El Equipo CSIRT es un grupo especializado cuya función principal es gestionar y mitigar los incidentes de seguridad informática. El objetivo es mejorar la capacidad de una organización para gestionar los riesgos cibernéticos respondiendo eficazmente a los incidentes y tomando medidas preventivas para minimizar los riesgos futuros. CSIRT proporciona un enfoque estructurado para la detección, análisis, respuesta y recuperación de incidentes para garantizar la integridad, confidencialidad y disponibilidad de la información (Cichonski et al., 2012). Servicios que ofrecen los Csirt se muestra en tabla Nro. 2

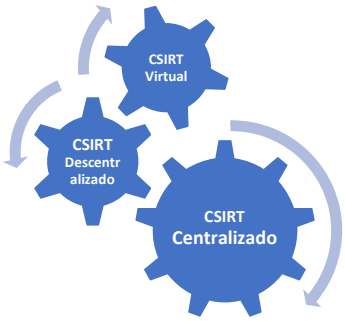
Un CSIRT es primordial para proteger los activos digitales de una organización. Son el primer punto de contacto en caso de un incidente de seguridad, brindando una respuesta rápida y coordinada para minimizar el impacto del incidente. Además, CSIRT desempeña un papel fundamental en la educación y concientización sobre seguridad de la información, promoviendo las mejores prácticas de los usuarios y fortaleciendo la postura de seguridad de la organización (West-Brown et al., 2003).

2.2 La evolución del CSIRT

El CSIRT ha recorrido un largo camino desde su creación en los años 1980. Inicialmente, su enfoque principal era responder a incidentes específicos, pero con el tiempo incorporaron características preventivas y proactivas, como evaluaciones de

vulnerabilidad y capacitación en ciberseguridad. Hoy en día, CSIRT es una parte importante de la estrategia de seguridad de la información de cualquier organización, especialmente en el campo académico donde la protección de la información es crucial (West-Brown et al., 2003).

El desarrollo del CSIRT pasó por varias fases importantes. Al principio, el CSIRT se centró principalmente en la contención y recuperación de incidentes. Sin embargo, a



medida que avanza la tecnología y surgen amenazas cibernéticas, su papel se ha ampliado para incluir la prevención y mitigación de riesgos. Hoy en día, el CSIRT utiliza herramientas avanzadas de análisis y monitoreo para identificar y responder instantáneamente a amenazas, colaborar con otras organizaciones para compartir información y mejorar la defensa colectiva (Cichonski et al., 2012).

2.3 Modelo de implementación

Los modelos de implementación de CSIRT pueden variar según el tamaño y la estructura de la organización. Los modelos más comunes incluyen:

2.3.1 CSIRT centralizado

El modelo CSIRT centralizado es aquel en el que un único equipo es responsable de gestionar todos los incidentes de seguridad de la organización. Este enfoque ofrece numerosos beneficios, incluida una mayor coherencia en la gestión de incidentes y la capacidad de centralizar recursos técnicos y experiencia en una sola ubicación. Los miembros del equipo obtienen una comprensión holística de la seguridad de la organización, lo que les permite identificar patrones y tendencias que pueden haberse pasado por alto en un modelo más descentralizado (Killcrece et al., 2003).

Por ejemplo, en una universidad como la UCE, un CSIRT centralizado puede garantizar

Imagen 3 Modelos de Implementación

que todos los incidentes de seguridad se manejen de manera consistente y eficiente. Esto es particularmente importante en entornos académicos donde la protección de los datos personales y de investigación es primordial. La centralización también facilita la implementación de políticas de seguridad unificadas y garantiza que todos los

departamentos sigan los mismos protocolos, reduciendo así el riesgo de violaciones de seguridad (West-Brown et al., 2003).

2.3.2 CSIRT descentralizado

CSIRT descentralizado es un modelo en el que múltiples equipos operan en diferentes sitios o unidades dentro de la organización, coordinados por un equipo central. Este enfoque es particularmente útil para organizaciones grandes y geográficamente dispersas, como corporaciones multinacionales o grandes instituciones académicas con múltiples campus (Killcrece et al., 2003).

En un modelo descentralizado, cada equipo local gestiona los incidentes de seguridad en su área específica, mientras que un equipo central coordina los esfuerzos y brinda apoyo según sea necesario. Esta estructura permite una respuesta más rápida y realista a los incidentes porque los equipos locales tienen una comprensión más profunda de los sistemas y procesos específicos de su dominio (FIRST , 2021).

Para la UCE, un CSIRT descentralizado podría significar tener equipos de respuesta en cada universidad o departamento importante, con un equipo central dentro de la administración universitaria para coordinar esfuerzos y garantizar la coherencia de las políticas y procedimientos de seguridad. Esto no sólo mejora las capacidades de respuesta a incidentes, sino que también permite una mejor gestión de los recursos y una mejor adaptación a las necesidades específicas de cada unidad (West-Brown et al., 2003).

2.3.3 CSIRT virtual

Virtual CSIRT es un modelo que aprovecha la colaboración y las comunicaciones remotas para gestionar eventos de seguridad. Este tipo de CSIRT utiliza herramientas tecnológicas avanzadas para permitir que los miembros del equipo trabajen juntos en diferentes ubicaciones, lo cual es particularmente útil en situaciones donde se requiere o se prefiere el trabajo remoto (Killcrece et al., 2003).

Un CSIRT virtual ofrece la flexibilidad de reunir a expertos de diferentes áreas geográficas y temáticas sin la necesidad de reubicarlos físicamente. Este modelo funciona bien para organizaciones que adoptan políticas de trabajo remoto u operan en varios países (FIRST , 2021).

Para universidades como la UCE, un CSIRT virtual puede proporcionar una solución flexible y escalable para gestionar incidentes de seguridad. A medida que la tendencia a trabajar y aprender en línea continúa creciendo, la capacidad de gestionar eventos de forma remota se vuelve cada vez más importante. Además, los CSIRT virtuales pueden aprovechar el talento y la experiencia de expertos en ciberseguridad de todo el mundo para mejorar la capacidad de las universidades para responder a amenazas complejas y en evolución (West-Brown et al., 2003).

Cada modelo tiene beneficios y desafíos, y elegir el modelo correcto depende de las necesidades específicas y la estructura organizacional de una institución. El CSIRT centralizado es eficaz para organizaciones pequeñas o aquellas con una estructura de TI unificada, mientras que el CSIRT descentralizado o virtual puede ser más adecuado para

organizaciones más grandes con múltiples sitios o múltiples sistemas (Cichonski et al., 2012).

2.4 Mejores Prácticas Internacionales

2.4.1 Normas y Directrices

La creación y funcionamiento del CSIRT se basa en diversos estándares y directrices internacionales. La Primera Arquitectura de Servicio CSIRT (2021) proporciona una arquitectura detallada para la implementación y operación efectiva del CSIRT. El marco incluye recomendaciones sobre gestión de incidentes, cooperación internacional y formación continua del personal (FIRST , 2021). Plataforma SIM3 (Madurez en la gestión de incidentes de seguridad) Model) proporciona un modelo de madurez para la gestión de incidentes de seguridad, permitiendo al CSIRT evaluar y mejorar sus capacidades (OpenCSIRT , 2021).

La Organización de Estados Americanos (OEA) también ha desarrollado lineamientos específicos para la creación y operación de Equipos de Respuesta a Incidentes de Seguridad Informática (CSIRT) en América Latina y el Caribe. Estas directrices resaltan la importancia de la cooperación regional y el intercambio de información para responder más eficazmente a las amenazas cibernéticas. Las “Directrices para el establecimiento y funcionamiento de CSIRT ” de la OEA brindan orientación práctica para el establecimiento y funcionamiento de CSIRT , enfatizando la necesidad de un enfoque coordinado y multidisciplinario de la ciberseguridad (OEA, 2023).

2.4.2 Casos de Estudio

Ejemplos exitosos de CSIRT en instituciones educativas de todo el mundo. Por ejemplo, el CSIRT de la Universidad de California en Los Ángeles (UCLA) implementa un enfoque proactivo para la gestión de incidentes, utilizando herramientas avanzadas de detección de amenazas y trabajando en estrecha colaboración con otros CSIRT y agencias gubernamentales para mejorar sus capacidades de respuesta (Mowbray, 2013).). En Ecuador, el CSIRT del Instituto Nacional Tecnológico (CSIRT-EPN) y la Red CEDIA (SocCSIRT) son ejemplos destacados de cómo las universidades han desarrollado sólidas capacidades de gestión de incidentes de seguridad (CSIRT-EPN , 2023 ;

UCLA CSIRT ha sido pionera en el uso de tecnología de inteligencia artificial para la detección y respuesta a incidentes. Utilizando algoritmos avanzados de aprendizaje automático, UCLA CSIRT puede identificar patrones inusuales en el tráfico de la red y responder rápidamente a posibles amenazas. Además, su colaboración con otras instituciones y agencias gubernamentales permite compartir información crítica sobre amenazas emergentes, mejorando así la postura de seguridad no solo de UCLA sino de toda la comunidad universitaria (Mowbray, 2013).

En Ecuador, el Instituto Nacional de Tecnología CSIRT ha implementado un enfoque integral para la gestión de incidentes que incluye capacitación y desarrollo continuo del personal y la adopción de las mejores prácticas internacionales de ciberseguridad. CSIRT -EPN ha establecido protocolos claros de detección y respuesta a incidentes y ha desarrollado herramientas personalizadas para el seguimiento y análisis de amenazas. Su cooperación con la red CEDIA promueve el intercambio de información y esfuerzos de coordinación para resolver incidentes cibernéticos a nivel nacional (CSIRT-EPN , 2023; SocCSIRT , 2023).

2.5 Situación local y marco legal en Ecuador

2.5.1 Análisis situacional en la UCE

La UCE es una institución con una compleja infraestructura tecnológica y una gran comunidad académica. La UCE enfrenta desafíos específicos de ciberseguridad debido a la diversidad de dispositivos y sistemas utilizados por estudiantes y Docentes y la necesidad de equilibrar la apertura en la investigación y la colaboración con la protección de datos confidenciales. La infraestructura de red de la UCE está distribuida en todos los departamentos y edificios, cada uno con sus propios requisitos y configuraciones de seguridad (Villegas-Ch. et al., 2021).

La UCE cuenta con una gran comunidad académica y administrativa y maneja grandes cantidades de datos sensibles, incluyendo información personal, académica y financiera. La diversificación de la infraestructura tecnológica desde redes locales hasta servicios en la nube crea múltiples puntos de vulnerabilidad que deben gestionarse adecuadamente. Además, la necesidad de acceso abierto a recursos académicos y de investigación añade mayor complejidad a la gestión de la seguridad de la información dentro de las instituciones (Villegas-Ch. et al., 2021).

2.5.2 Marco legal y regulatorio

En Ecuador, la Ley Orgánica de Protección de Datos Personales (LOPD) establece los principios y requisitos para el adecuado tratamiento de los datos personales. La ley exige que las organizaciones implementen medidas de seguridad para proteger la información personal, incluido el establecimiento de un CSIRT para gestionar eficazmente los incidentes de seguridad (Ley Organizacional de Protección de Datos Personales, 2021).

La LOPDP impone ciertas restricciones al uso de información personal por parte del CSIRT. Por ejemplo, el CSIRT solo puede recopilar y compartir la información personal necesaria para responder a incidentes cibernéticos. Además, el CSIRT debe informar a los interesados sobre la recopilación y el uso de su información personal. En general, la LOPDP proporciona un marco legal que permite al CSIRT trabajar de manera efectiva

para proteger la ciberseguridad y al mismo tiempo proteger los derechos de los propietarios de datos (Ley Organizacional de Protección de Datos Personales, 2021).

Además de la LOPD, la serie de normas internacionales ISO 27000 también proporciona un marco adicional para la gestión de la seguridad de la información. ISO/IEC 27001 define los requisitos para los sistemas de gestión de seguridad de la información (SGSI) , mientras que ISO/IEC 27002 proporciona orientación sobre los controles de seguridad. ISO/IEC 27005 se centra específicamente en la gestión de riesgos de seguridad de la información, proporcionando un enfoque estructurado para identificar, evaluar y mitigar riesgos (ISO/IEC 27005, 2018).

La serie ISO 27000 consta de una serie de especificaciones y estándares relacionados con la seguridad de la información. Estos estándares están diseñados para ayudar a las organizaciones a establecer, implementar, mantener y mejorar sistemas de gestión de seguridad de la información (SGSI). Si bien la serie de normas ISO 27000 no se centra específicamente en los equipos de respuesta a incidentes de seguridad de la información, proporcionan un marco común relacionado con la seguridad de la información y, por lo tanto, impactan las operaciones de seguridad de los CSIRT.

ISO/IEC 27001 - Sistemas de gestión de seguridad de la información (SGSI): Esta norma especifica los requisitos para establecer, implementar, mantener y mejorar un SGSI en una organización. El CSIRT está directamente relacionado con la seguridad de la información en la gestión de incidentes de seguridad de la información y, por lo tanto, puede beneficiarse de un SGSI que cumpla con la norma ISO 27001. La implementación de un SGSI que cumpla con la norma ISO/IEC 27001 garantiza que el CSIRT opere dentro de un alcance claramente definido... Marco de gestión de la seguridad de la información, incluidas políticas, procedimientos y controles para gestionar los riesgos de seguridad de la información (ISO/IEC 27001:2013).

ISO/IEC 27002 - Código de prácticas para la gestión de la seguridad de la información: si bien no se centra en CSIRT , este estándar proporciona orientación detallada sobre las prácticas de seguridad de la información, incluida la gestión de incidentes. Los CSIRT pueden utilizar la norma ISO 27002 como base para establecer sus procesos y controles, garantizando que las mejores prácticas de seguridad de la información se integren en sus operaciones diarias. ISO/IEC 27002 proporciona un conjunto de controles que los CSIRT pueden aplicar para proteger la información, prevenir incidentes de seguridad y responder eficazmente cuando ocurren incidentes (ISO/IEC 27002:2013).

ISO/IEC 27035 - Gestión de incidentes de seguridad de la información: esta norma se centra específicamente en la gestión de incidentes de seguridad de la información y proporciona orientación para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar los procesos de gestión de incidentes. Los CSIRT pueden

beneficiarse al seguir las pautas de este estándar para mejorar su efectividad. ISO/IEC 27035 proporciona un enfoque estructurado para la gestión de incidentes, desde la preparación y planificación hasta la detección, análisis, respuesta y lecciones aprendidas (ISO/IEC 27035:2016).

ISO/IEC 27010 - Comunicaciones seguras entre entidades: esta norma aborda la seguridad de las comunicaciones entre organizaciones, que pueden ser relevantes para la colaboración entre CSIRT de diferentes entidades. Las comunicaciones seguras son fundamentales para los CSIRT , especialmente cuando comparten información sobre incidentes y amenazas de seguridad con otras organizaciones o CSIRT externos. ISO/IEC 27010 proporciona orientación sobre cómo establecer canales de comunicación seguros y confiables para garantizar la transmisión de información confidencial de manera segura (ISO/IEC 27010:2015).

ISO 17799: Esta norma proporciona mejores prácticas para la gestión de la seguridad de la información, cubriendo aspectos como la política de seguridad, la organización de la seguridad de la información y la gestión de activos.

ISO 22301: esta norma especifica los requisitos para los sistemas de gestión de la continuidad del negocio. El CSIRT debe considerar este estándar para garantizar que las operaciones críticas puedan continuar durante y después de un incidente de seguridad.

Norma 31000:2009: Esta norma internacional proporciona principios y directrices de gestión de riesgos esenciales para identificar, analizar y mitigar los riesgos de seguridad en la gestión de incidentes.

Norma de Control Interno de la Contraloría General de la Nación: Esta norma establece requisitos para la gestión de la seguridad de la información en las instituciones públicas ecuatorianas, incluyendo la necesidad de contar con mecanismos adecuados de gestión de incidentes de ciberseguridad.

2.5.3 ANSI y NIST relacionados con CSIRT

Las regulaciones y estándares desarrollados por el Instituto Nacional Estadounidense de Estándares (ANSI) pueden proporcionar orientación y mejores prácticas en las áreas de seguridad de la información y seguridad de la red, contribuyendo así a la creación y operación de CSIRT. Algunas normas ANSI que pueden ser relevantes para CSIRT incluyen:

ANSI/ISO/IEC 27001:2013 - Sistemas de gestión de seguridad de la información (SGSI) - Requisitos: esta norma proporciona un marco para establecer, implementar, mantener y mejorar un SGSI. CSIRT puede utilizar este estándar para ayudar a las organizaciones a mejorar la seguridad de la información y garantizar que las prácticas de gestión de incidentes sean coherentes con el enfoque general de gestión de la seguridad (ANSI/ISO/IEC 27001:2013).

ANSI/ISO/IEC 27002:2013 - Controles del sistema de gestión de seguridad de la información: este estándar proporciona un catálogo de controles de seguridad de la información que las organizaciones pueden utilizar para implementar un SGSI. CSIRT puede utilizar este estándar para ayudar a las organizaciones a identificar los controles de seguridad necesarios para satisfacer sus necesidades específicas y garantizar una respuesta eficaz a los incidentes de seguridad (ANSI/ISO/IEC 27002:2013).

Instituto Nacional de Estándares y Tecnología SP 800-61r2 – Directrices para la gestión de incidentes de seguridad de la información : si bien no es un estándar ANSI, esta directriz del Instituto Nacional de Estándares y Tecnología (NIST) proporciona un conjunto sólido de pautas y mejores prácticas para gestionar incidentes de seguridad. Es particularmente útil para la creación y operación de CSIRT , ya que proporciona un enfoque detallado y estructurado para la respuesta a incidentes desde la preparación hasta la recuperación (Cichonski et al., 2012).

Instituto Nacional Estadounidense de Estándares/ Instituto Nacional Estadounidense de Estándares y Tecnología SP 800-61:2015 - Sistema de gestión de incidentes de seguridad de la información (SGSI): Directrices para el establecimiento, implementación, operación, mantenimiento y mejora: esta norma proporciona orientación para la creación, implementación, operación, mantenimiento y mejora de un SGSI. CSIRT puede utilizar este estándar para ayudar a las organizaciones a desarrollar y gestionar un SGSI eficaz , garantizando que las prácticas de gestión de incidentes sean consistentes y efectivas (NIST , 2015).

Instituto Nacional Estadounidense de Estándares/ Instituto Nacional Estadounidense de Estándares y Tecnología SP 800-63-3:2018 - Cifrado de datos: Implementación de requisitos de cifrado de datos: este estándar proporciona requisitos para la implementación del cifrado de datos. CSIRT puede utilizar este estándar para ayudar a las organizaciones a proteger sus datos confidenciales garantizando que la información crítica esté protegida del acceso no autorizado durante un incidente (NIST , 2018).

Instituto Nacional Estadounidense de Estándares/ Instituto Nacional Estadounidense de Estándares y Tecnología SP 800-115:2018 - Guía de evaluación de la seguridad de la información: esta norma proporciona orientación para la evaluación de la seguridad de la información. CSIRT puede utilizar este estándar para ayudar a las organizaciones a evaluar la seguridad de su información, identificando vulnerabilidades y riesgos que deben gestionarse para mejorar su postura de seguridad (NIST , 2018).

ANSI/ASIS RMSC.1-2015 - Estándar de gestión de riesgos de seguridad de la información : este estándar proporciona orientación para gestionar los riesgos de seguridad de la información, lo cual es fundamental para evaluar y mitigar el riesgo de incidentes de seguridad. CSIRT puede utilizar este estándar para desarrollar estrategias efectivas de gestión de riesgos, garantizando que las organizaciones estén preparadas para abordar y mitigar proactivamente los riesgos de seguridad (ASIS, 2015).

ANSI/TIA-942-A:2016 – Sistemas de cableado estructurado empresarial: este estándar proporciona un marco para el diseño, instalación y mantenimiento de sistemas de cableado estructurado. CSIRT puede utilizar este estándar para ayudar a las organizaciones a mejorar la seguridad de la infraestructura de TI y garantizar que las redes y los sistemas se diseñen y mantengan de forma segura (TIA , 2016).

ANSI/TIA-952-B:2019 - Infraestructura de cableado para la seguridad de la información: este estándar proporciona un marco para el diseño, instalación y mantenimiento de sistemas de cableado estructurado que cumplen con los requisitos de seguridad de la información. CSIRT puede utilizar este estándar para ayudar a las organizaciones a proteger su infraestructura de TI de las amenazas cibernéticas y garantizar que las prácticas de cableado sean seguras y confiables (TIA , 2019).

ANSI/TIA-942-A:2016 - Sección 9.5: Seguridad de la información: Esta sección de ANSI/TIA-942-A proporciona orientación específica para la seguridad de la información en sistemas de cableado estructurado. El CSIRT puede utilizar estas directrices para ayudar a las organizaciones a implementar controles de seguridad dentro de su infraestructura de TI y garantizar que las prácticas de seguridad sean integrales y efectivas (TIA , 2016).

En resumen, la implementación y operación del CSIRT de la Universidad Central del Ecuador debe estar en línea con las mejores prácticas y estándares internacionales para asegurar su efectividad y el cumplimiento de los marcos legales y regulatorios pertinentes. La adopción de los estándares ISO/IEC, así como los estándares ANSI y las directrices NIST, sentará una base sólida para la gestión de la seguridad de la información, la respuesta a incidentes y la protección de datos personales dentro de las organizaciones.

CAPÍTULO III

MARCO METODOLÓGICO

3.1 Enfoque y diseño de la investigación

Para desarrollar un modelo CSIRT efectivo para la UCE, se utilizará un enfoque metodológico mixto, que combina métodos cualitativos y cuantitativos este enfoque permite la triangulación de datos, proporcionando una visión más completa y confiable del contexto y las necesidades de ciberseguridad en la institución.

- **Métodos Cualitativos**: Se utilizarán para explorar las percepciones y experiencias de las partes interesadas y para identificar necesidades y desafíos específicos de seguridad de TI en el ámbito académico. Las entrevistas en profundidad y los grupos focales proporcionarán información contextual y detallada fundamental para comprender los matices de la ciberseguridad en entornos académicos.
- **Métodos Cuantitativos**: Se emplearán para recopilar y analizar datos sobre la incidencia de incidentes de ciberseguridad, las tendencias de ciber amenazas y la eficacia de los controles de seguridad existentes. A través de encuestas estructuradas y análisis de datos de accidentalidad, se obtendrá información generalizable a la población objeto de estudio, permitiendo una valoración precisa y representativa de la situación actual.

3.2 Procedimientos de la investigación

3.2.1 Fase 1: Análisis de mejores prácticas internacionales

Objetivo: Efectuar una revisión detallada y crítica de la información existente sobre la creación y operación de CSIRTs en instituciones académicas y otras entidades organizacionales.

3.2.1.1 **Proceso:**

1. **Selección de Fuentes:** Se procederá a la selección de fuentes de alta relevancia, incluyendo tratados, monografías, artículos académicos, informes técnicos y normativas internacionales.
2. **Análisis de Contenido:** Se realizará un análisis meticuloso del contenido para discernir las mejores prácticas, estructuras organizativas, políticas de gestión de incidentes y tecnologías empleadas.
3. **Síntesis de Información:** La información recopilada será sintetizada con el propósito de extraer conclusiones clave que informen el desarrollo del modelo de CSIRT para la UCE.

3.2.2 Fase 2: Diagnóstico de la situación actual en la UCE

Objetivo: Evaluar el estado actual de la ciberseguridad en la UCE, abarcando la infraestructura tecnológica, políticas de seguridad y prácticas vigentes de gestión de incidentes.

3.2.2.1 Proceso:

1. **Evaluación de Infraestructura:** Se procederá a un análisis profundo de la infraestructura tecnológica existente, incluyendo redes, sistemas informáticos y herramientas de seguridad.
2. **Revisión de Políticas y Procedimientos:** Se evaluarán las políticas y procedimientos vigentes relacionados con la seguridad informática.
3. **Entrevistas y Encuestas:** Se llevarán a cabo entrevistas y encuestas dirigidas a personal clave de TI, administradores y usuarios finales para recabar información sobre la percepción y efectividad de las prácticas actuales de ciberseguridad.

3.2.3 Fase 3: Diseño del modelo CSIRT para la UCE

Objetivo: Desarrollar un modelo de CSIRT adaptado a las necesidades y contexto de la UCE.

3.2.3.1 Proceso:

1. **Estructura Organizativa:** Propuesta de una estructura para el CSIRT, incluyendo roles y responsabilidades.
2. **Procesos y Procedimientos:** Diseño de protocolos para la gestión de incidentes y respuesta a amenazas.
3. **Recursos Necesarios**: Identificación de los recursos humanos, tecnológicos y financieros necesarios.

3.2.4 Fase 4: Validación del modelo propuesto

Objetivo: Validar la efectividad y viabilidad del modelo de CSIRT propuesto.

3.2.4.1 Proceso:

Método: Evaluación de expertos y simulaciones de incidentes para medir la respuesta del CSIRT.

CAPÍTULO IV

DESARROLLO Y VALIDACIÓN DEL MODELO CSIRT PARA LA UCE

4.1 Introducción

El análisis de mejores prácticas internacionales en CSIRTs académicos incluye una serie de recomendaciones para su creación y operación efectiva. Estas prácticas están orientadas a garantizar una respuesta rápida y coordinada a incidentes de seguridad informática, y abarcan aspectos como la definición y alcance de los CSIRTs académicos, Estructura organizativa, servicios ofrecidos, Colaboración y compartición de información, capacitación y desarrollo profesional, herramientas y tecnologías utilizadas, métricas y evaluación de desempeño.

4.2 FASE 1: Análisis de mejores prácticas internacionales en CSIRTs académicos

4.2.1 Definición y alcance de los CSIRTs académicos

Los CSIRTs académicos son equipos especializados dentro de instituciones educativas y de investigación que se encargan de prevenir, detectar y responder a incidentes de seguridad informática (Cichonski et al., 2012). Según West-Brown et al. (2003), el alcance de estos equipos suele abarcar:

- Protección de la infraestructura de red de la institución
- Salvaguarda de datos de investigación y propiedad intelectual
- Aseguramiento de la integridad de los sistemas académicos y administrativos
- Educación y concientización en ciberseguridad para la comunidad académica

Ejemplos específicos incluyen el CSIRT de la Universidad Técnica Particular de Loja (UTPL), que se centra en la gestión de incidentes relacionados con la infraestructura de TI de la universidad, y el CSIRT de la Escuela Politécnica Nacional (EPN), que además de responder a incidentes, realiza análisis de riesgos específicos para su entorno académico.

Tabla 1 Análisis de mejores prácticas en CSIRTs académicos

Aspecto	Ventajas	Desventajas
Marco de Gestión	- Proporciona estructura clara y sistemática para manejar incidentes - Establece roles y responsabilidades definidos- Facilita la medición y mejora continua - Permite una respuesta coordinada a incidentes	- Puede resultar demasiado rígido para entornos académicos dinámicos - Requiere actualización constante de procedimientos - Puede generar burocracia excesiva - Demanda recursos significativos para su mantenimiento

Protección de Activos	- Asegura la protección de propiedad intelectual - Salvaguarda datos de investigación críticos - Protege información personal de la comunidad universitaria - Mantiene la integridad de sistemas académicos	- Puede limitar el acceso a recursos necesarios para investigación - Puede obstaculizar la colaboración académica - Requiere equilibrio entre seguridad y accesibilidad- Costos elevados de implementación de controles
Alcance Educativo	- Permite personalización por perfil de usuario - Facilita la creación de cultura de seguridad - Promueve la participación activa - Desarrolla capacidades internas	- Requiere recursos significativos para desarrollo de contenido - Necesita actualización constante de materiales - Demanda personal especializado en educación - Resultados visibles a largo plazo
Infraestructura Diversa	- Permite cobertura integral de sistemas - Facilita la segmentación de servicios - Admite diferentes niveles de protección - Habilita respuestas específicas por área	- Complejidad en la gestión de múltiples sistemas - Dificultad para mantener consistencia - Mayores costos operativos - Requiere expertise diversificado
Aspectos Culturales	- Fomenta una cultura de seguridad proactiva - Promueve la responsabilidad compartida - Facilita la adopción de buenas prácticas - Mejora la conciencia de seguridad	- Resistencia al cambio cultural - Tiempo significativo para ver resultados - Necesidad de motivación continua - Dificultad para medir impacto
Cumplimiento Normativo	- Asegura conformidad con regulaciones - Establece estándares claros - Facilita auditorías - Reduce riesgos legales	- Complejidad en cumplimiento multinivel - Costos de implementación elevados - Necesidad de actualizaciones frecuentes - Puede limitar flexibilidad operativa
Sostenibilidad	- Permite desarrollo a largo plazo - Facilita la mejora continua - Promueve la autonomía - Construye capacidades internas	- Requiere compromiso financiero sostenido - Necesita apoyo institucional continuo - Demanda recursos dedicados - Dependencia de personal clave

La tabla presenta las ventajas y desventajas de implementar un CSIRT en un entorno académico. Los beneficios incluyen la protección de datos críticos, la gestión estructurada de incidentes y la promoción de una cultura de seguridad a través de educación personalizada. Entre los desafíos se destacan la rigidez del marco, los altos costos, la complejidad de gestionar varios sistemas, la actualización constante de procedimientos y materiales, el equilibrio entre seguridad y accesibilidad, y la resistencia al cambio.

Análisis

El análisis destaca la necesidad de un CSIRT académico enfocado en capacitación y concienciación, estructurado en varias dimensiones críticas:

1. **Dimensión Educativa**: Desarrollar programas de capacitación específicos para estudiantes, docentes y personal administrativo, utilizando métodos pedagógicos innovadores como simulaciones y gamificación.
2. **Dimensión de Concienciación**: Implementar estrategias de comunicación efectivas, adaptadas a diferentes audiencias y establecer programas de "embajadores de seguridad" para fomentar la participación.
3. **Dimensión de Medición y Evaluación**: Aplicar métricas para evaluar la efectividad de los programas, incluyendo tasas de participación y cambios en el comportamiento.
4. **Dimensión Preventiva**: Promover la identificación temprana de amenazas y construir una cultura de seguridad proactiva que fomente el reporte de incidentes.
5. **Dimensión de Sostenibilidad**: Desarrollar capacidades internas a través de la formación continua y la gestión del conocimiento, como la documentación de lecciones aprendidas.
6. **Dimensión de Integración Académica**: Vincular el CSIRT con programas académicos, incorporando módulos de seguridad y promoviendo proyectos de investigación.

En resumen, este enfoque educativo del CSIRT no solo busca mejorar la postura de seguridad de la institución, sino que también promueve el desarrollo sostenible de capacidades internas y la creación de una cultura de seguridad duradera en la comunidad universitaria.

4.2.2 Estructura organizativa

La estructura de los CSIRTs académicos puede variar según el tamaño y las necesidades de la institución. Killcrece et al. (2003) identifican tres modelos comunes:

- Modelo centralizado: Un único equipo CSIRT atiende a toda la institución. Por ejemplo, el CSIRT de la UCE podría beneficiarse de este modelo, centralizando los esfuerzos de ciberseguridad en un solo equipo coordinado.
- Modelo distribuido: Múltiples equipos CSIRT especializados por departamento o facultad. Un ejemplo de este enfoque se puede observar en grandes universidades

con múltiples campus o unidades académicas, donde la ciberseguridad está distribuida entre diferentes departamentos.

- Modelo híbrido: Combina elementos centralizados y distribuidos, permitiendo una flexibilidad adicional para adaptarse a las necesidades cambiantes de la institución. Ahmad et al. (2021) resaltan la importancia de establecer líneas claras de autoridad y comunicación en todos los modelos, asegurando un vínculo efectivo con la alta dirección.

Tabla 2 Estructura organizativa

Característica	Modelo Centralizado	Modelo Distribuido	Modelo Híbrido
Estructura Organizativa	Un único equipo CSIRT para toda la institución	Múltiples equipos CSIRT por departamento	Combina un equipo central con unidades departamentales
Ventajas	- Respuesta más coherente y coordinada - Mayor eficiencia en uso de recursos- Políticas y procedimientos uniformes - Mejor control y supervisión- Comunicación más directa- Menor costo operativo	- Especialización por departamento - Mejor conocimiento del contexto local - Respuesta más rápida a incidentes locales - Mayor cercanía con usuarios finales - Adaptación a necesidades específicas - Mejor comprensión de riesgos departamentales	- Combina beneficios de ambos modelos - Balance entre coherencia y especialización - Flexibilidad operativa - Mejor escalabilidad - Aprovechamiento de recursos compartidos - Adaptabilidad a diferentes necesidades
Desventajas	- Menor conocimiento específico departamental - Posible lentitud en respuestas locales - Sobrecarga potencial del equipo central - Menor adaptabilidad a necesidades específicas- Distanciamiento de usuarios finales	- Inconsistencias en políticas y procedimientos - Mayor costo operativo - Duplicación de esfuerzos y recursos - Dificultad en coordinación - Variación en calidad de servicio - Complejidad en gestión de recursos	- Mayor complejidad administrativa - Necesidad de coordinación más sofisticada - Costos intermedios- Posibles conflictos de autoridad - Requiere definición clara de roles - Mayor esfuerzo en comunicación

	- Dificultad para escalar en organizaciones grandes		
Costos	- Menor costo inicial - Economías de escala - Inversión centralizada	- Mayor costo operativo - Inversión distribuida - Duplicación de recursos	- Costo moderado - Inversión equilibrada - Optimización de recursos
Eficacia	Alta para organizaciones pequeñas o medianas	Alta para organizaciones muy grandes o distribuidas	Óptima para instituciones medianas a grandes
Requerimientos de Personal	- Equipo central altamente capacitado - Menor cantidad total de personal	- Múltiples equipos especializados - Mayor cantidad total de personal	- Combinación de personal central y departamental - Cantidad moderada de personal
Adecuado para	- Organizaciones pequeñas - Estructuras simples - Presupuestos limitados	- Organizaciones grandes - Estructuras complejas - Departamentos muy especializados	- Universidades medianas a grandes - Estructuras mixtas - Necesidades diversas

La tabla compara tres modelos de CSIRT (centralizado, distribuido e híbrido). El modelo **centralizado** tiene un único equipo que gestiona toda la institución, lo que ofrece coherencia, control y menor costo, pero puede carecer de conocimiento específico y ser más lento en responder a incidentes locales. El modelo **distribuido** asigna equipos a cada departamento, lo que permite una respuesta rápida y adaptada a las necesidades locales, aunque genera mayores costos, duplicación de recursos y dificultades en la coordinación. El modelo **híbrido** combina ambos enfoques, equilibrando coherencia y especialización, lo que mejora la escalabilidad y optimización de recursos, pero introduce mayor complejidad administrativa y de coordinación.

Análisis:

Tabla 3 Evaluación del Modelo Híbrido del CSIRT en la UCE

Criterio de Evaluación	Modelo Híbrido en la UCE
Estructura Organizacional	- Equipo central CSIRT coordinador - Unidades especializadas en cada facultad - Enlaces designados en departamentos clave - Comité de gobierno con representantes de todas las áreas
Beneficios Estratégicos	- Políticas y estándares unificados

	- Respuesta rápida a nivel local - Mejor gestión de recursos - Mayor adaptabilidad a necesidades específicas - Escalabilidad controlada
Requerimientos Presupuestarios	- Inversión inicial: $420,399.60 (primer año) - Costos operativos centralizados - Presupuestos departamentales asignados - Recursos compartidos entre unidades
Necesidades de Personal	- Equipo central: 7 especialistas - Enlaces facultativos: 21 personas - Personal de soporte: según necesidad - Programa de capacitación continua
Infraestructura Tecnológica	- Sistemas centralizados de monitoreo - Herramientas departamentales específicas - Plataforma unificada de gestión - Recursos compartidos de análisis
Indicadores de Éxito	- KPIs centralizados y departamentales - Métricas de respuesta a incidentes - Indicadores de efectividad en capacitación - Evaluaciones de madurez por área
Desafíos de Implementación	- Coordinación entre unidades - Gestión de recursos compartidos - Mantenimiento de estándares uniformes - Balance entre autonomía y control

El modelo híbrido propuesto para la Universidad Central del Ecuador (UCE) plantea un equipo CSIRT central coordinador con unidades especializadas en cada facultad y enlaces en departamentos clave. Sus principales beneficios incluyen la unificación de políticas, una respuesta rápida y adaptada a nivel local, y una gestión de recursos eficiente. Se estima una inversión inicial de $420,399.60 para el primer año, con costos operativos y recursos compartidos entre facultades. El equipo central estaría compuesto por 7 especialistas, apoyados por enlaces en las facultades. El éxito del modelo se medirá mediante KPIs centralizados, métricas de respuesta y evaluaciones de madurez por área, aunque la implementación presenta desafíos como la coordinación y el mantenimiento de estándares uniformes.

El análisis fundamentado sostiene que la implementación de un modelo híbrido de CSIRT en la UCE es necesaria debido a varios factores críticos:

1. **Adaptación a la Estructura Universitaria**: El modelo híbrido aborda las diversas necesidades de seguridad de las 21 facultades y 16 áreas administrativas, integrándose con estructuras existentes como la DTIC.
2. **Optimización de Recursos**: Facilita el uso compartido de herramientas y personal especializado, reduciendo la duplicación de esfuerzos y maximizando el retorno de inversión en seguridad.
3. **Eficiencia Operativa**: Establece procedimientos estandarizados y mantiene una capacidad de respuesta local, permitiendo escalabilidad en función de las necesidades.

4. **Viabilidad Financiera**: Requiere una inversión inicial significativa, pero permite distribuir costos y ajustar el presupuesto según las necesidades.
5. **Sostenibilidad a Largo Plazo**: Fomenta el desarrollo gradual de capacidades internas y la especialización del personal, promoviendo la transferencia de conocimiento.
6. **Factores Críticos de Éxito**: Depende del compromiso de la alta dirección, la asignación de presupuesto, un plan de implementación por fases, capacitación y un sistema de evaluación continua.

La viabilidad del modelo se condiciona a la aprobación de un presupuesto inicial de $420,399.60, el compromiso de al menos 28 recursos humanos, inversión en infraestructura y apoyo constante de las autoridades universitarias. En conjunto, el análisis concluye que el modelo híbrido es no solo ideal, sino viable para la UCE, siempre que se aseguren los recursos y compromisos necesarios para su implementación y sostenibilidad a largo plazo

4.2.3 Servicios ofrecidos

Los CSIRTs académicos modernos ofrecen una gama integral de servicios que, según el marco actualizado de FIRST (2023) y las directrices de ENISA (2022), se pueden clasificar en las siguientes categorías:

Tabla 4 Categorías de Servicios de los CSIRTs Académicos

Categoría de Servicios	Descripción	Ejemplos en CSIRTs Académicos	Beneficios
Servicios Reactivos	- Respuesta a incidentes - Análisis de malware - Análisis forense digital - Coordinación de respuesta - Gestión de vulnerabilidades	- CSIRT-CEDIA: Sistema automatizado de detección y respuesta - CSIRT-EPN: Laboratorio de análisis forense - CSIRT-UTPL: Plataforma integrada de gestión de incidentes	- Respuesta rápida a amenazas - Minimización de impacto - Recuperación efectiva - Documentación de incidentes
Servicios Proactivos	- Monitoreo continuo - Evaluaciones de seguridad - Threat hunting - Inteligencia de amenazas - Desarrollo de herramientas	- RedCLARA CSIRT: Sistema de alertas tempranas - CSIRT-ESPE: Plataforma de threat intelligence - CSIRT-UPS: Desarrollo de herramientas automatizadas	- Prevención de incidentes - Detección temprana - Mejora continua - Reducción de riesgos
Servicios de Gestión de Seguridad	- Análisis de riesgos - Gestión de continuidad	- CSIRT-ESPOL: Framework de gestión de riesgos	- Mejora en gobernanza - Cumplimiento regulatorio

	- Cumplimiento normativo - Políticas de seguridad - Métricas y KPIs	- CSIRT-UTE: Sistema de gestión de continuidad - CSIRT-PUCE: Programa de cumplimiento	- Resiliencia organizacional - Optimización de recursos
Servicios de Calidad	- Auditorías de seguridad - Certificaciones - Evaluaciones de madurez - Mejora de procesos	- CSIRT-UCE: Programa de auditorías - CSIRT-USFQ: Sistema de gestión de calidad - CSIRT-UCSG: Framework de mejora continua	- Aseguramiento de calidad - Estandarización - Mejora continua - Medición de efectividad
Servicios Educativos	- Capacitación - Concienciación - Simulacros - Ejercicios prácticos	- CSIRT-UPS: Academia de seguridad - CSIRT-UDLA: Programa de concienciación - CSIRT-UTN: Laboratorios virtuales	- Desarrollo de capacidades - Cultura de seguridad - Reducción de errores humanos - Empoderamiento de usuarios

Los CSIRTs académicos brindan una amplia gama de servicios divididos en varias categorías. Los **servicios reactivos** responden a incidentes de seguridad, como el análisis forense y la gestión de vulnerabilidades, minimizando el impacto de los incidentes (ej., CSIRT-CEDIA y CSIRT-EPN). Los **servicios proactivos** incluyen monitoreo continuo y caza de amenazas, previniendo incidentes y mejorando la seguridad a largo plazo (ej., RedCLARA y CSIRT-ESPE). Los **servicios de gestión de seguridad** garantizan la continuidad y cumplimiento normativo, optimizando los recursos institucionales (ej., CSIRT-ESPOL y CSIRT-UTE). Los **servicios de calidad** aseguran la mejora continua a través de auditorías y evaluaciones de madurez (ej., CSIRT-UCE). Finalmente, los **servicios educativos** promueven la capacitación y concienciación, desarrollando una cultura de seguridad y reduciendo errores humanos (ej., CSIRT-UPS y CSIRT-UTN).

4.2.3.1 **Análisis Comparativo de Servicios CSIRT Académicos**

Tabla 5Análisis de Servicios del CSIRT: Ventajas, Desventajas y Consideraciones para su Implementación

Tipo de Servicio	Ventajas	Desventajas	Consideraciones para Implementación
Servicios Reactivos	- Resolución efectiva de incidentes - Minimización de impacto inmediato - Aprendizaje directo de incidentes	- Alto consumo de recursos durante crisis - Necesidad de personal disponible 24/7	- Priorizar según tipos de incidentes más comunes - Establecer niveles de servicio claros - Implementar rotación de personal

	- Mejora continua basada en experiencia	- Requiere herramientas especializadas - Puede ser estresante para el equipo	- Invertir en automatización
Servicios Proactivos	- Prevención de incidentes - Reducción de riesgos a largo plazo - Mejor planificación de recursos - Desarrollo de capacidades internas	- Requiere inversión significativa inicial - Necesita personal altamente capacitado - Resultados no inmediatamente visibles - Requiere actualización constante	- Comenzar con evaluaciones básicas - Implementar monitoreo gradual - Priorizar áreas críticas - Medir ROI a largo plazo
Servicios de Gestión	- Mejora en gobernanza de seguridad - Cumplimiento normativo - Procesos documentados - Base para mejora continua	- Complejidad administrativa - Puede generar burocracia - Resistencia al cambio - Costos de implementación altos	- Alinear con objetivos institucionales - Implementar por fases - Involucrar stakeholders clave - Mantener documentación actualizada
Servicios de Capacitación	- Desarrollo de cultura de seguridad - Reducción de errores humanos - Empoderamiento de usuarios - Sostenibilidad a largo plazo	- Requiere recursos didácticos - Necesita actualización constante - Participación variable - Difícil medir efectividad	- Adaptar contenido por audiencia - Usar métodos interactivos - Establecer métricas claras - Evaluar regularmente

Los servicios reactivos permiten la rápida resolución de incidentes y la minimización del impacto, pero requieren personal disponible 24/7 y pueden ser estresantes para el equipo. Para implementarlos, se deben priorizar los incidentes más comunes y automatizar procesos. Los servicios proactivos previenen incidentes y reducen riesgos a largo plazo, aunque requieren una inversión inicial alta y personal capacitado. Su implementación debe comenzar con evaluaciones básicas y monitoreo gradual. Los servicios de gestión mejoran la gobernanza y el cumplimiento normativo, pero pueden generar burocracia y costos altos; se recomienda implementarlos por fases e involucrar a las partes interesadas. Finalmente, los servicios de capacitación desarrollan una cultura de seguridad y reducen errores humanos, pero demandan recursos educativos y es difícil medir su efectividad; por lo tanto, es clave adaptar el contenido y evaluar el impacto regularmente.

4.2.3.2 Recomendaciones para la Implementación:

1. **Priorización de Servicios:**
   - Iniciar con servicios esenciales según necesidades específicas
   - Expandir gradualmente según capacidades y recursos
   - Evaluar regularmente la efectividad de cada servicio
2. **Gestión de Recursos:**
   - Asignar recursos según criticidad de servicios
   - Balancear entre servicios reactivos y proactivos
   - Optimizar mediante automatización donde sea posible
3. **Desarrollo de Capacidades:**
   - Formar personal en múltiples áreas de servicio
   - Establecer planes de capacitación continua
   - Desarrollar especialización interna gradualmente
4. **Medición de Efectividad:**
   - Establecer KPIs específicos por tipo de servicio
   - Realizar evaluaciones periódicas
   - Ajustar servicios según resultados obtenidos

Análisis:

Es crucial priorizar servicios que ofrezcan el mayor impacto en la seguridad de la UCE, como la respuesta a incidentes y el monitoreo proactivo, capacitación y concienciación ajustados a los recursos disponibles.

4.2.4 Colaboración y compartición de información

La colaboración entre CSIRTs académicos y otras entidades es fundamental para afrontar las amenazas cibernéticas en constante evolución. Housley y Polk (2001) destacan la importancia de participar en redes nacionales e internacionales, como FIRST o la OEA, que facilitan el intercambio de indicadores de compromiso (IoCs) y técnicas de ataque. Skierka et al. (2015) enfatizan la necesidad de establecer protocolos claros para compartir información sensible, respetando la privacidad y las regulaciones aplicables.

4.2.4.1 Análisis Estratégico de la Colaboración y Compartición de Información

1. **Niveles de Colaboración**

Tabla 6Niveles de Colaboración del CSIRT: Alcance, Beneficios, Desafíos y Requisitos

Nivel	Alcance	Beneficios	Desafíos	Requisitos
Institucional	Entre departamentos UCE	- Respuesta coordinada - Recursos compartidos - Mejor visibilidad de amenazas	- Silos departamentales - Resistencia al cambio - Conflictos de prioridades	- Políticas internas claras - Canales de comunicación establecidos - Protocolos de escalamiento

Nacional	Red de CSIRTs académicos Ecuador	- Inteligencia de amenazas local - Recursos compartidos - Respuesta coordinada nacional	- Diferentes niveles de madurez - Competencia institucional - Restricciones legales	- Acuerdos formales - Estándares comunes - Plataformas compartidas
Internacional	Colaboración global	- Acceso a mejores prácticas - Alertas tempranas - Conocimiento especializado	- Barreras idiomáticas - Diferencias regulatorias - Zonas horarias	- Membresías en organizaciones - Protocolos de comunicación - Recursos multilingües

2. Marco de Implementación

Tabla 7 Estrategias, Métricas y Controles para la Gobernanza y Seguridad

Aspecto	Estrategias	Métricas de Éxito	Controles
Gobernanza	- Comité de supervisión - Políticas de compartición - Procedimientos estandarizados	- Efectividad de decisiones - Cumplimiento de políticas - Tiempo de respuesta	- Auditorías regulares - Revisiones de cumplimiento - Evaluaciones de madurez
Tecnología	- Plataformas seguras de compartición - Herramientas de análisis - Sistemas de automatización	- Disponibilidad de sistemas - Velocidad de compartición - Calidad de datos	- Monitoreo de seguridad - Control de acceso - Cifrado de datos
Procesos	- Clasificación de información - Protocolos de compartición - Procedimientos de validación	- Eficiencia de procesos - Precisión de información - Tiempo de procesamiento	- Verificaciones de calidad - Revisiones periódicas - Mejora continua

La colaboración del CSIRT puede darse en tres niveles: institucional, nacional, e internacional. A nivel institucional, la coordinación entre departamentos de la UCE permite compartir recursos y mejorar la visibilidad de amenazas, aunque enfrenta desafíos como silos departamentales y resistencia al cambio, requiriendo políticas claras y canales de comunicación. A nivel nacional, la colaboración con redes de CSIRTs académicos en Ecuador facilita el intercambio de inteligencia de amenazas y recursos, pero puede verse limitada por la variación en niveles de madurez y restricciones legales, por lo que se necesitan acuerdos formales y estándares comunes. A nivel internacional, la colaboración

global brinda acceso a mejores prácticas y alertas tempranas, aunque enfrenta barreras idiomáticas, regulatorias y de zonas horarias, lo que requiere membresías en organizaciones, protocolos de comunicación y recursos multilingües.

3. Gestión de Riesgos

Tabla 8 Gestión de Riesgos en CSIRT: Impacto, Mitigación y Monitoreo

Riesgo	Impacto	Mitigación	Monitoreo
Fuga de Información	Alto	- Clasificación de datos - Acuerdos de confidencialidad - Control de acceso granular	- Auditoría de accesos - Monitoreo de actividad - Revisiones periódicas
Calidad de Datos	Medio	- Validación de fuentes - Procedimientos de verificación - Estándares de calidad	- Métricas de calidad - Retroalimentación - Evaluaciones regulares
Cumplimiento Legal	Alto	- Asesoría legal - Políticas de cumplimiento - Capacitación regular	- Auditorías de cumplimiento - Actualizaciones normativas - Evaluaciones de impacto

Los riesgos clave en un CSIRT incluyen la fuga de información, que tiene un impacto alto y se mitiga mediante la clasificación de datos, acuerdos de confidencialidad y controles de acceso, con monitoreo basado en auditorías de accesos y revisiones periódicas. La calidad de los datos presenta un impacto medio, mitigado por la validación de fuentes y estándares de calidad, monitoreada mediante métricas y evaluaciones regulares. El cumplimiento legal, con alto impacto, se gestiona a través de asesoría legal, políticas de cumplimiento y capacitación regular, mientras que su monitoreo implica auditorías de cumplimiento, actualizaciones normativas y evaluaciones de impacto.

4. Indicadores de Éxito

Tabla 9 KPIs y Objetivos del CSIRT: Categorías y Frecuencia de Medición

Categoría	KPIs	Objetivo	Frecuencia de Medición
Operativo	- Tiempo de respuesta - Calidad de información - Efectividad de colaboración	- Mejora continua - 95% precisión - 80% efectividad	Mensual

Estratégico	- Madurez de colaboración - Valor agregado - Innovación	- Nivel 4 de 5 - ROI positivo - 2 innovaciones/año	Trimestral
Cumplimiento	- Adherencia a políticas - Incidentes de seguridad - Cumplimiento regulatorio	- 100% cumplimiento - Cero incidentes críticos - 100% conformidad	Mensual

Los KPIs del CSIRT se dividen en tres categorías clave: **Operativos**, **Estratégicos**, y de **Cumplimiento**. Los **KPIs operativos** incluyen el tiempo de respuesta, calidad de información, y efectividad de colaboración, con un objetivo de 95% de precisión y 80% de efectividad, medidos mensualmente para garantizar mejoras continuas. Los **KPIs estratégicos** evalúan la madurez de la colaboración, el valor agregado, y la innovación, con metas como alcanzar el nivel 4 de 5 en madurez y generar dos innovaciones anuales, siendo evaluados trimestralmente. Los **KPIs de cumplimiento** miden la adherencia a políticas, incidentes de seguridad y cumplimiento normativo, buscando un 100% de conformidad y cero incidentes críticos, con medición mensual.

Este análisis más profundo proporciona una base sólida para implementar y gestionar efectivamente la colaboración y compartición de información en el CSIRT académico, considerando múltiples dimensiones y estableciendo métricas claras para su evaluación y mejora continua.

4.2.5 Capacitación y desarrollo profesional

La formación continua del personal es clave para mantener la efectividad de los CSIRTs académicos. Bada et al. (2014) recomiendan programas de certificación en ciberseguridad, como CISSP, CEH o GIAC, junto con la participación en conferencias, talleres especializados y ejercicios de simulación de incidentes. El CSIRT de la Universidad Nacional de Colombia, por ejemplo, prioriza la formación continua de su personal en estas áreas.

4.2.5.1 **Análisis Estratégico de Capacitación y Desarrollo Profesional del CSIRT**

Tabla 10 Dimensiones del Desarrollo y Capacitación en CSIRT: Beneficios, Desafíos y Estrategias

Dimensión	Beneficios	Desafíos	Estrategias de Implementación	Métricas de Éxito
Desarrollo Técnico	- Mantenimiento de competencias actualizadas	- Alto costo de certificaciones - Tiempo fuera de operaciones - Rápida obsolescencia	- Programa de certificaciones escalonado - Laboratorios virtuales internos	- Número de certificaciones obtenidas - Evaluaciones de competencia

	- Mejora en capacidad de respuesta - Innovación en soluciones - Adaptabilidad a nuevas amenazas	de conocimientos - Curva de aprendizaje pronunciada	- Rotación de especialidades - Mentorías técnicas	- Tiempo de respuesta a incidentes - Innovaciones implementadas
Desarrollo Profesional	- Carrera profesional clara - Mayor compromiso - Liderazgo mejorado - Retención de talento	- Limitaciones presupuestarias - Expectativas salariales - Oportunidades limitadas de ascenso - Competencia del mercado	- Plan de carrera estructurado - Programas de liderazgo - Incentivos no monetarios - Proyectos especiales	- Tasa de retención - Satisfacción laboral - Promociones internas - Evaluaciones de desempeño
Gestión del Conocimiento	- Preservación de experiencia institucional - Transferencia de conocimiento efectiva - Base de conocimiento robusta - Continuidad operativa	- Documentación inconsistente - Pérdida de conocimiento tácito - Resistencia a compartir - Tiempo de documentación	- Sistema de gestión del conocimiento - Comunidades de práctica - Documentación estructurada - Sesiones de compartir conocimientos	- Calidad de documentación - Uso de base de conocimiento - Tiempo de incorporación de nuevo personal - Efectividad de transferencia
Ejercicios Prácticos	- Experiencia práctica - Trabajo en equipo mejorado - Preparación para incidentes reales - Identificación de brechas	- Tiempo de preparación - Recursos necesarios - Complejidad logística - Balance con operaciones	- Simulacros regulares - Ejercicios de mesa - CTFs internos - Escenarios realistas	- Desempeño en ejercicios - Mejora en tiempos de respuesta - Efectividad del trabajo en equipo -Lecciones aprendidas implementadas

El desarrollo técnico mantiene las competencias actualizadas y mejora la capacidad de respuesta a amenazas, pero enfrenta desafíos como el alto costo de certificaciones y la rápida obsolescencia. Para mitigarlo, se recomiendan programas escalonados de

certificación y laboratorios virtuales, midiendo el éxito con el número de certificaciones y tiempos de respuesta. El desarrollo profesional fomenta el compromiso y el liderazgo, aunque se ve limitado por restricciones presupuestarias y pocas oportunidades de ascenso; esto se aborda con planes de carrera estructurados y programas de liderazgo, medido por la tasa de retención y evaluaciones de desempeño. La gestión del conocimiento preserva la experiencia institucional y facilita la transferencia de conocimiento, aunque puede haber resistencia y falta de documentación. La solución es implementar un sistema de gestión del conocimiento y fomentar comunidades de práctica, evaluando la calidad de la documentación y la efectividad de la transferencia. Los ejercicios prácticos mejoran la preparación para incidentes reales y el trabajo en equipo, pero requieren tiempo y recursos. Se recomienda realizar simulacros regulares y ejercicios prácticos, con éxito medido por el desempeño en ejercicios y la mejora en tiempos de respuesta.

4.2.5.2 **Plan de Implementación Escalonado**

Tabla 11 Progresión de Capacidades y Certificaciones en Seguridad Informática

Nivel	Duración	Certificaciones	Habilidades y Actividades Clave
Básico	0-6 meses	CompTIA Security+, CISSP Associate	Entrenamiento en herramientas básicas, procedimientos operativos estándar, ejercicios básicos de respuesta.
Intermedio	6-18 meses	CEH, GCIH	Especialización por roles, ejercicios avanzados de simulación, desarrollo de liderazgo técnico.
Avanzado	18+ meses	CISSP, CISM	Investigación y desarrollo, mentoría de nuevo personal, liderazgo de proyectos especiales.

La progresión en seguridad informática se estructura en tres niveles. En el nivel básico (0-6 meses), se adquieren certificaciones fundamentales y conocimientos operativos básicos. En el nivel intermedio (6-18 meses), los profesionales se especializan por roles, obtienen certificaciones específicas y desarrollan liderazgo técnico. Finalmente, en el nivel avanzado (18+ meses), se alcanzan certificaciones avanzadas, se lideran proyectos y se fomenta la investigación y mentoría.

4.2.5.3 **Sistema de Retención y Transferencia**

Tabla 12 Estrategias de Desarrollo y Retención de Talento

Estrategia	**Implementación**	**Beneficios**	**Medición**
Acuerdos de Permanencia	- Contratos por certificación - Períodos mínimos post-capacitación - Reembolso escalonado	- Protección de inversión - Compromiso del personal - ROI asegurado	- Cumplimiento de acuerdos - Retorno de inversión - Retención post-capacitación

Programa de Mentores	- Pares de mentor-aprendiz - Plan de desarrollo personalizado - Evaluación continua	- Transferencia de conocimiento - Desarrollo acelerado - Continuidad operativa	- Efectividad de mentorías - Progresión de aprendices - Satisfacción de participantes
Gestión de Sucesión	- Identificación de roles críticos - Desarrollo de sucesores - Planes de transición	- Continuidad de liderazgo - Desarrollo de talento - Minimización de riesgos	- Cobertura de roles críticos - Preparación de sucesores - Efectividad de transiciones

Este esquema presenta tres estrategias clave para el desarrollo y retención de talento: acuerdos de permanencia, programas de mentoría y gestión de sucesión. Cada estrategia está diseñada para proteger la inversión en capacitación, asegurar la transferencia de conocimiento y garantizar la continuidad operativa mediante el desarrollo de líderes. Los beneficios incluyen compromiso del personal, aceleración del crecimiento y mitigación de riesgos, evaluados a través de métricas como la retención post-capacitación, efectividad de mentorías y preparación de sucesores.

4.2.5.4 **Presupuesto y ROI**

Tabla 13 Inversiones en Capacitación y su Retorno Esperado

Inversión	Retorno Esperado	Métricas de Evaluación
Certificaciones	Mejora en capacidades técnicas	- Tasa de éxito en certificaciones - Aplicación práctica de conocimientos
Entrenamiento interno	Eficiencia operativa mejorada	- Reducción en tiempo de respuesta - Mejora en calidad de servicio
Ejercicios prácticos	Preparación para incidentes	- Desempeño en simulacros - Efectividad en incidentes reales
Gestión del conocimiento	Preservación de expertise	- Calidad de documentación - Eficiencia en transferencia de conocimiento

Este resumen analiza cuatro áreas de inversión en capacitación y sus beneficios esperados. Las certificaciones mejoran las capacidades técnicas del personal, evaluadas por el éxito en certificaciones y la aplicación práctica del conocimiento. El entrenamiento interno aumenta la eficiencia operativa, medido por la reducción en tiempos de respuesta y mejora en la calidad del servicio. Los ejercicios prácticos preparan al equipo para incidentes, evaluados mediante el desempeño en simulacros y respuesta a incidentes reales. Finalmente, la gestión del conocimiento asegura la preservación del expertise, con

métricas como la calidad de la documentación y la eficiencia en la transferencia de conocimiento.

4.2.6 Herramientas y tecnologías utilizadas

Los CSIRTs académicos utilizan una variedad de herramientas para cumplir con sus funciones. Mundie y McIntire (2013) clasifican estas herramientas en categorías principales como:

a) Sistemas de gestión de incidentes (e.g., RTIR, TheHive): Estos sistemas permiten un seguimiento eficiente de los incidentes desde su detección hasta su resolución.
b) Plataformas de inteligencia de amenazas (e.g., MISP, OpenCTI): Facilitan el intercambio de información sobre amenazas emergentes, permitiendo a los CSIRTs anticiparse a los ataques.
c) Herramientas de análisis forense digital (e.g., Volatility, Autopsy): Son esenciales para la investigación detallada de incidentes de seguridad, permitiendo la recolección y análisis de evidencia digital.
d) Sistemas de detección y prevención de intrusiones (IDS/IPS): Utilizados ampliamente por CSIRTs como el de CEDIA, estos sistemas ayudan a identificar y mitigar ataques en tiempo real.

Actualizar regularmente el stack tecnológico es crucial para enfrentar nuevas amenazas y garantizar la protección de la infraestructura académica.

4.2.7 Análisis Estratégico de Herramientas y Tecnologías para el CSIRT UCE

Tabla 14 Comparativa de Herramientas Open Source y Comerciales para la UCE

Categoría	Herramientas Open Source	Herramientas Comerciales	Análisis Costo-Beneficio	Recomendación UCE
Gestión de Incidentes	- TheHive - RTIR - FIR - Costo: Gratuito - Personalizable	- ServiceNow SecOps - IBM Resilient - Costo: $50K-100K/año - Soporte enterprise	**Beneficios:** - Ahorro significativo - Control total sobre personalización **Costos:** - Tiempo de implementación - Necesidad de expertise interno	Implementar TheHive: - Integración con otras herramientas - Comunidad activa - Alta personalización - Costo-efectivo
Monitoreo de Seguridad	- Security Onion - Wazuh - Suricata	- Splunk Enterprise - QRadar	**Beneficios:** - Detección temprana	Implementar Wazuh + Suricata:

	- Costo: Gratuito - Alta flexibilidad	- Costo: $75K-150K/año - Interfaz pulida	- Análisis avanzado **Costos:** - Infraestructura - Mantenimiento	- Capacidades SIEM/IDS - Escalable - Integración con TheHive
Análisis de Vulnerabilidades	- OpenVAS - OWASP ZAP - Nikto - Costo: Gratuito - Actualizaciones frecuentes	- Nessus Pro - Qualys - Costo: $25K-50K/año - Reportes detallados	**Beneficios:** - Identificación proactiva - Remediación guiada **Costos:** - Licencias - Actualizaciones	Implementar OpenVAS: - Escaneo comprehensivo - Buena documentación - Actualizaciones regulares
Análisis Forense	- Volatility - SIFT Workstation - Autopsy - Costo: Gratuito - Herramientas especializadas	- EnCase - FTK - Costo: $30K-60K/año - Soporte legal	**Beneficios:** - Investigación detallada - Evidencia forense **Costos:** - Capacitación - Hardware	Implementar SIFT + Volatility: - Capacidades completas - Comunidad activa - Formatos estándar

La comparación entre herramientas open source y comerciales para la UCE destaca que las primeras, como TheHive, Wazuh, OpenVAS y SIFT, son más económicas y altamente personalizables, aunque requieren experiencia interna. Las herramientas comerciales, aunque más costosas, ofrecen soporte y facilidad de uso. Se recomienda implementar las soluciones open source por su costo-efectividad, escalabilidad e integración con las capacidades actuales de la UCE.

4.2.7.1 **Plan de Implementación por Fases**

Tabla 15 Plan de Implementación de Seguridad para la UCE

Fase	Duración	Objetivos	Recursos Necesarios	Resultados Esperados
Fase 1: Fundamentos	3-6 meses	- Implementar TheHive - Configurar Wazuh básico - Capacitación inicial	- 2 servidores - 1 especialista - 40 horas capacitación	- Sistema básico de tickets - Monitoreo básico - Personal capacitado
Fase 2: Expansión	6-12 meses	- Integrar Suricata	- 3 servidores adicionales	- IDS funcionando

		- Implementar OpenVAS - Ampliar monitoreo	- 2 especialistas - 80 horas capacitación	- Escaneos regulares - Detección mejorada
Fase 3: Madurez	12-18 meses	- Implementar SIFT - Automatizar procesos - Desarrollar playbooks	- Hardware forense - 2 especialistas senior - 120 horas capacitación	- Capacidad forense - Procesos automatizados - Respuesta eficiente

Este plan en tres fases cubre la implementación de herramientas de seguridad en la UCE. En la Fase 1 (3-6 meses), se enfocará en implementar TheHive y Wazuh con capacitación inicial, logrando un sistema básico de tickets y monitoreo. La Fase 2 (6-12 meses) integrará Suricata y OpenVAS, ampliando la detección de amenazas. Finalmente, en la Fase 3 (12-18 meses), se automatizarán procesos y se implementará SIFT para análisis forense. Con el tiempo, se espera mayor capacidad de monitoreo, detección y respuesta ante incidentes.

4.2.7.2 **Estrategia de Capacitación**

Tabla 16 Programa de Capacitación en Ciberseguridad

Nivel	Contenido	Duración	Evaluación
Básico	- Uso básico de herramientas - Procedimientos estándar - Documentación	40 horas	- Pruebas prácticas - Ejercicios simulados
Intermedio	- Configuración avanzada - Integración de herramientas - Troubleshooting	80 horas	- Proyectos prácticos - Casos de estudio
Avanzado	- Personalización - Desarrollo de módulos - Análisis avanzado	120 horas	- Implementaciones reales - Certificaciones

Este plan en tres fases cubre la implementación de herramientas de seguridad en la UCE. En la Fase 1 (3-6 meses), se enfocará en implementar TheHive y Wazuh con capacitación inicial, logrando un sistema básico de tickets y monitoreo. La Fase 2 (6-12 meses) integrará Suricata y OpenVAS, ampliando la detección de amenazas. Finalmente, en la Fase 3 (12-18 meses), se automatizarán procesos y se implementará SIFT para análisis forense. Con el tiempo, se espera mayor capacidad de monitoreo, detección y respuesta ante incidentes.

4.2.7.3 **Métricas de Éxito**

Tabla 17 Métricas Clave de Desempeño del CSIRT UCE

Categoría	Métrica	Objetivo	Frecuencia
Operacional	- Tiempo de detección	- Reducción 50%	Mensual

	- Tiempo de respuesta - Falsos positivos	- Menos de 1 hora - Menos de 10%	
Técnico	- Disponibilidad - Precisión - Cobertura	- 99.9% - 95% - 90%	Semanal
Financiero	- Costo por incidente - ROI - Ahorro vs comercial	- Reducción 30% - Positivo en 18 meses - 70% menos	Trimestral

Esta tabla presenta un marco integral de medición para evaluar el rendimiento del CSIRT de la Universidad Central del Ecuador, abarcando tres categorías fundamentales: operacional, técnica y financiera. Cada categoría establece métricas específicas con objetivos cuantificables y frecuencias de medición definidas, permitiendo un seguimiento sistemático de la efectividad del equipo en la gestión de incidentes de seguridad, la calidad del servicio técnico y la eficiencia en el uso de recursos financieros.

4.2.8 Métricas y evaluación de desempeño

La evaluación del desempeño es esencial para la mejora continua de los CSIRTs académicos. Stikvoort (2015) propone medir el tiempo de respuesta a incidentes, el número de incidentes gestionados, la tasa de éxito en resolución y la satisfacción de los usuarios. Adicionalmente, Bada y Nurse (2019) recomiendan auditorías externas periódicas y benchmarking con otros CSIRTs para identificar áreas de mejora. Un ejemplo sería la implementación de estas métricas en el CSIRT de la Universidad de Oxford, que ha mejorado su tiempo de respuesta y satisfacción de usuarios a través de evaluaciones regulares.

4.2.8.1 Análisis Estratégico de Métricas y Evaluación del CSIRT

Tabla 18 Sistema de Evaluación y Métricas para el Desarrollo del CSIRT UCE

Categoría	Métricas Propuestas	Método de Medición	Frecuencia	Objetivo Inicial	Madurez Esperada
Operativas	- Tiempo de respuesta a incidentes - Tasa de resolución - Precisión en clasificación - Tiempo de detección	- Registros del sistema - Reportes automáticos - Auditorías de casos	Mensual	- Respuesta < 4h - Resolución 70% - Precisión 80% - Detección < 6h	- Respuesta < 1h - Resolución 95% - Precisión 95% - Detección < 2h
Capacitación	- Participación en entrenamientos - Retención de conocimiento - Aplicación práctica - Certificaciones obtenidas	- Registros de asistencia - Evaluaciones post-curso - Observación práctica	Trimestral	- Participación 60% - Retención 70% - Aplicación 50% - 1 cert/persona/año	- Participación 90% - Retención 90% - Aplicación 85% - 2 cert/persona/año
Preventivas	- Vulnerabilidades identificadas - Tiempo de parcheo	- Scans automáticos - Registros de sistemas	Semanal	- Identificación 70% - Parcheo < 30d	- Identificación 95% - Parcheo < 7d

	- Efectividad de controles - Incidentes prevenidos	- Análisis de eventos		- Efectividad 60% - Prevención 40%	- Efectividad 90% - Prevención 80%
Cualitativas	- Satisfacción del usuario - Cultura de seguridad - Calidad de documentación - Colaboración interdepartamental	- Encuestas -Entrevistas - Evaluaciones peer	Semestral	- Satisfacción 70% - Cultura básica - Doc. aceptable - Colab. moderada	- Satisfacción 90% - Cultura madura - Doc. excelente - Colab. alta

La tabla establece un marco de evaluación para el CSIRT de la UCE, definiendo métricas en cuatro áreas fundamentales: operativas (respuesta a incidentes), capacitación (desarrollo del personal), preventivas (gestión de vulnerabilidades) y cualitativas (satisfacción y cultura organizacional). Para cada categoría, se establecen indicadores específicos, métodos de medición y objetivos tanto iniciales como de madurez, permitiendo un seguimiento sistemático del progreso y efectividad del equipo.

4.2.8.2 **Marco de Implementación por Niveles**

Tabla 19 Marco de Implementación y Evolución de Métricas del CSIRT UCE

Nivel	Enfoque	Métricas Clave	Herramientas	Evaluación
Básico (0-6 meses)	- Métricas operativas fundamentales - KPIs básicos - Mediciones manuales	- Tiempo de respuesta - Incidentes resueltos - Tiempo de detección	- Hojas de cálculo - Registros básicos - Formularios	- Revisión mensual - Ajustes según necesidad - Feedback básico
Intermedio (6-18 meses)	- Métricas automatizadas - KPIs avanzados - Análisis de tendencias	- Eficiencia operativa - Prevención - ROI	- SIEM - Dashboards - Analytics	- Revisión quincenal - Análisis detallado - Mejora continua
Avanzado (18+ meses)	- Métricas predictivas - KPIs estratégicos - ML/AI analytics	- Predicción de riesgos - Optimización - Valor estratégico	- BI tools - ML models - Predictive analytics	- Revisión semanal - Optimización continua - Innovación

La tabla describe el desarrollo progresivo del sistema de métricas del CSIRT UCE en tres niveles de madurez. Comienza con un nivel básico (0-6 meses) enfocado en mediciones manuales y KPIs fundamentales, avanza a un nivel intermedio (6-18 meses) con automatización y análisis de tendencias, y culmina en un nivel avanzado (18+ meses) que incorpora análisis predictivo y herramientas de inteligencia artificial. Cada nivel establece

objetivos específicos, herramientas apropiadas y métodos de evaluación, permitiendo una evolución estructurada de las capacidades de medición y análisis del CSIRT.

4.2.8.3 **Balance Cuantitativo-Cualitativo**

Tabla 20 Métricas de Evaluación y Desempeño Integrado del CSIRT UCE

Aspecto	Métricas Cuantitativas	Métricas Cualitativas	Integración
Operaciones	- Número de incidentes - Tiempos de respuesta - Tasas de resolución	- Calidad de resolución - Satisfacción usuario - Efectividad de solución	Combinar para evaluación integral de servicio
Personal	- Horas de capacitación - Certificaciones - Productividad	- Desarrollo de habilidades - Trabajo en equipo - Innovación	Evaluar desarrollo holístico del equipo
Procesos	- Tiempo de proceso - Adherencia a SLAs - Eficiencia	- Calidad de documentación - Mejora de procesos - Adaptabilidad	Optimizar eficiencia y efectividad
Impacto	- ROI - Costos evitados - Eficiencia ganada	- Reputación - Confianza usuarios - Cultura de seguridad	Demostrar valor total del CSIRT

La tabla establece un marco de evaluación que combina indicadores cuantitativos y cualitativos para medir el desempeño del CSIRT en cuatro aspectos fundamentales: operaciones (incidentes y respuesta), personal (capacitación y desarrollo), procesos (eficiencia y documentación) e impacto (ROI y cultura organizacional). Esta estructura integrada permite una evaluación completa y balanceada del rendimiento del equipo, facilitando la toma de decisiones basada en datos tanto objetivos como subjetivos.

4.2.8.4 **Sistema de Evaluación Continua**

Tabla 21 Sistema de Evaluación Continua del CSIRT UCE

Componente	Metodología	Frecuencia	Uso de Resultados
Revisión de Métricas	- Análisis de tendencias - Comparación con objetivos - Identificación de gaps	Mensual	- Ajuste de objetivos - Mejora de procesos - Planificación estratégica
Feedback Stakeholders	- Encuestas - Entrevistas - Focus groups	Trimestral	- Mejora de servicios - Ajuste de prioridades

			- Desarrollo de capacidades
Auditoría de Calidad	- Revisión de procesos - Evaluación de resultados - Verificación de compliance	Semestral	- Optimización de operaciones - Actualización de políticas - Desarrollo de mejores prácticas
Evaluación Estratégica	- Revisión de objetivos - Análisis de madurez - Planificación futura	Anual	- Actualización estratégica - Planificación de recursos - Desarrollo largo plazo

La tabla presenta un sistema integral de evaluación continua para el CSIRT, organizado en cuatro componentes principales: revisión de métricas (mensual), feedback de stakeholders (trimestral), auditoría de calidad (semestral) y evaluación estratégica (anual). Cada componente especifica metodologías específicas, frecuencias de evaluación y el uso previsto de los resultados, permitiendo un ciclo de mejora continua y adaptación estratégica del CSIRT.

4.2.9 Selección de guía:

Para seleccionar la metodología más apropiada, es importante considerar varias opciones y evaluarlas según criterios específicos relevantes para los CSIRTs académicos. Analizaremos tres marcos de trabajo prominentes:

1 NIST SP 800-61 "Computer Security Incident Handling Guide"
2 ISO/IEC 27035 "Information Security Incident Management"
3 ENISA "CSIRT Framework"

4.2.9.1 Criterios de Evaluación para Marcos de Trabajo CSIRT

1. **Adaptabilidad al Entorno Académico**

Tabla 22 Criterios de Adaptabilidad del CSIRT al Entorno Académico

Aspecto	Descripción	Indicadores de Evaluación	Importancia
Flexibilidad Organizacional	Capacidad de adaptarse a la estructura universitaria jerárquica y descentralizada	- Compatibilidad con gobierno universitario - Adaptación a facultades y departamentos - Integración con procesos académicos	Alta

Consideraciones Académicas	Alineación con las necesidades específicas del sector educativo	- Protección de datos académicos - Soporte a investigación - Gestión de recursos educativos	Alta
Balance de Apertura	Equilibrio entre seguridad y libertad académica	- Acceso a recursos académicos - Protección de propiedad intelectual - Flexibilidad para investigación	Media

La tabla presenta los aspectos fundamentales para evaluar la adaptabilidad del CSIRT al contexto universitario, considerando tres criterios esenciales: la flexibilidad organizacional (adaptación a la estructura universitaria), las consideraciones académicas (alineación con necesidades educativas) y el balance de apertura (equilibrio entre seguridad y libertad académica). Cada aspecto incluye indicadores específicos de evaluación y su nivel de importancia, proporcionando un marco para asegurar que el CSIRT se integre efectivamente en el entorno académico de la UCE.

2. **Exhaustividad de la Cobertura**

Tabla 23 Criterios de Exhaustividad en la Implementación del CSIRT

Aspecto	Descripción	Elementos Evaluados	Importancia
Alcance Técnico	Cobertura de aspectos técnicos de seguridad	- Gestión de incidentes - Monitoreo de seguridad - Análisis de vulnerabilidades	Alta
Procesos Organizacionales	Inclusión de aspectos administrativos y de gestión	- Políticas y procedimientos - Gestión de recursos - Métricas y reportes	Alta
Aspectos Humanos	Consideración de factores humanos y culturales	- Capacitación y concienciación - Gestión del cambio - Desarrollo de personal	Media

La tabla define los aspectos críticos para asegurar una cobertura completa en la implementación del CSIRT, abarcando tres dimensiones principales: técnica (seguridad operativa), organizacional (gestión y procedimientos) y humana (capacitación y cultura). Cada aspecto especifica elementos clave de evaluación y su nivel de importancia,

proporcionando un marco estructurado para garantizar una implementación integral del CSIRT en la UCE.

3. **Facilidad de Implementación**

Tabla 24 Evaluación de Factibilidad en la Implementación del CSIRT

Aspecto	Descripción	Criterios de Evaluación	Importancia
Complejidad Técnica	Nivel de expertise requerido para implementación	- Requisitos técnicos - Curva de aprendizaje - Necesidades de infraestructura	Alta
Recursos Necesarios	Requerimientos de recursos humanos y financieros	- Presupuesto necesario - Personal requerido - Tiempo de implementación	Alta
Documentación	Calidad y disponibilidad de guías y documentación	- Claridad de guías - Ejemplos prácticos - Recursos de soporte	Media

La tabla establece los criterios fundamentales para evaluar la viabilidad de implementación del CSIRT, considerando tres aspectos clave: la complejidad técnica (expertise requerido), recursos necesarios (humanos y financieros) y documentación (guías y soporte). Para cada aspecto se detallan criterios específicos de evaluación y su nivel de importancia, proporcionando un marco para evaluar la factibilidad práctica de la implementación del CSIRT en la UCE.

4. **Reconocimiento Internacional**

Tabla 25 Evaluación del Reconocimiento Internacional del CSIRT

Aspecto	Descripción	Indicadores	Importancia
Adopción Global	Nivel de adopción en la comunidad internacional	- Número de organizaciones usuarias - Distribución geográfica - Casos de éxito	Alta
Respaldo Institucional	Apoyo de organizaciones reconocidas	- Respaldo de organismos internacionales - Certificaciones asociadas - Referencias en estándares	Alta
Comunidad de Usuarios	Tamaño y actividad de la comunidad de usuarios	- Foros activos	Media

		- Recursos compartidos - Soporte comunitario	

La tabla presenta los criterios para evaluar el posicionamiento internacional del CSIRT, enfocándose en tres aspectos clave: adopción global (alcance internacional), respaldo institucional (apoyo de organizaciones) y comunidad de usuarios (participación y soporte). Cada aspecto incluye indicadores específicos y su nivel de importancia, proporcionando un marco para evaluar la credibilidad y reconocimiento internacional del modelo CSIRT implementado en la UCE.

5. **Frecuencia de Actualizaciones**

Tabla 26 Criterios de Actualización y Evolución del CSIRT

Aspecto	Descripción	Métricas de Evaluación	Importancia
Mantenimiento	Regularidad de actualizaciones y mantenimiento	- Frecuencia de releases - Corrección de bugs - Mejoras implementadas	Alta
Evolución	Adaptación a nuevas amenazas y tecnologías	- Actualizaciones de seguridad - Nuevas funcionalidades - Adaptación a tendencias	Alta
Retroalimentación	Incorporación de feedback de la comunidad	- Proceso de mejora - Respuesta a sugerencias - Adaptación a necesidades	Media

La tabla establece los parámetros para evaluar la capacidad de actualización y evolución del CSIRT, abarcando tres aspectos esenciales: mantenimiento (actualizaciones regulares), evolución (adaptación a nuevas amenazas) y retroalimentación (mejora basada en feedback). Cada aspecto incluye métricas específicas de evaluación y su nivel de importancia, proporcionando un marco para asegurar que el CSIRT mantenga su efectividad y relevancia a lo largo del tiempo en la UCE.

4.2.9.2 **Matriz de Evaluación**

Tabla 27 Matriz de Evaluación de Criterios para el CSIRT}

Criterio	Peso	Método de Evaluación	Escala
Adaptabilidad al Entorno Académico	25%	Evaluación cualitativa y cuantitativa	1-5
Exhaustividad de la Cobertura	20%	Lista de verificación de componentes	1-5

Facilidad de Implementación	20%	Análisis de recursos y requisitos	1-5
Frecuencia de Actualizaciones	15%	Análisis de historial de mantenimiento	1-5

La tabla presenta un sistema de evaluación ponderado para el CSIRT, definiendo cuatro criterios fundamentales: adaptabilidad al entorno académico (25%), exhaustividad de cobertura (20%), facilidad de implementación (20%) y frecuencia de actualizaciones (15%). Cada criterio se evalúa mediante métodos específicos en una escala de 1-5, proporcionando un marco objetivo para valorar la efectividad y viabilidad del CSIRT en la UCE.

Análisis comparativo:

Tabla 28 Análisis comparativo de Metodologías

Criterio	NIST SP 800-61	ISO/IEC 27035	ENISA CSIRT Framework	SIM3
Adaptabilidad	Alta - Flexible para diferentes tipos de organizaciones.	Media - Orientado más hacia entornos empresariales.	Alta - Específico para CSIRTs, incluyendo los académicos.	Alta - Aplicable a diversos tipos de CSIRTs.
Exhaustividad	Alta - Cubre todas las fases de la gestión de incidentes.	Alta - Cubre todos los aspectos de la gestión de incidentes.	Media - Cubre aspectos clave, pero menos detallado.	Media - Se centra en la madurez organizacional.
Facilidad de Implementación	Media - Guías prácticas, pero complejo para equipos pequeños.	Baja - Requiere comprensión profunda de los estándares ISO.	Alta - Herramientas y plantillas listas para usar.	Media - Requiere comprensión de niveles de madurez.
Reconocimiento Internacional	Alto - Ampliamente adoptado globalmente.	Alto - Estándar ISO reconocido globalmente.	Medio - Bien reconocido en Europa, menos en otras regiones.	Medio - Conocido en la comunidad CSIRT, menos que NIST o ISO.
Frecuencia de Actualizaciones	Media - Actualizaciones periódicas, pero no anuales.	Baja - Actualizaciones menos frecuentes.	Alta - Actualizaciones regulares basadas en retroalimentación.	Media - Se actualiza periódicamente, no tan frecuentemente como ENISA.

La tabla presenta un análisis comparativo de cuatro metodologías principales para la implementación de CSIRTs: NIST SP 800-61, ISO/IEC 27035, ENISA CSIRT Framework y SIM3. En términos de adaptabilidad, tanto NIST, ENISA como SIM3 destacan por su alta flexibilidad para diferentes tipos de organizaciones, mientras que ISO/IEC 27035 muestra una orientación más empresarial. Respecto a la exhaustividad,

NIST e ISO/IEC 27035 sobresalen al cubrir comprehensivamente todas las fases de gestión de incidentes, mientras que ENISA y SIM3 ofrecen una cobertura más específica pero menos detallada. En cuanto a la facilidad de implementación, ENISA lidera con herramientas y plantillas listas para usar, mientras que ISO/IEC 27035 presenta la mayor complejidad debido a su requerimiento de comprensión profunda de estándares. El reconocimiento internacional es dominado por NIST e ISO/IEC 27035, con ENISA teniendo mayor presencia en Europa y SIM3 siendo más conocido específicamente en la comunidad CSIRT. Finalmente, en términos de actualizaciones, ENISA muestra la mayor frecuencia con actualizaciones regulares basadas en retroalimentación, mientras que ISO/IEC 27035 presenta la menor frecuencia de actualizaciones. Esta comparación sugiere que una combinación de NIST como marco principal, complementado con herramientas específicas de ENISA, podría ser la aproximación más efectiva para la implementación de un CSIRT en la UCE

4.2.10 Selección final:

Basado en esta comparación, se recomienda adoptar el NIST SP 800-61 como marco principal, complementado con elementos del ENISA CSIRT Framework. Esta combinación aprovecha la exhaustividad y el reconocimiento del NIST, junto con las herramientas prácticas y la especificidad para CSIRTs del marco de ENISA.

Esta tabla proporciona una visión general clara de las fortalezas y debilidades de cada marco, facilitando la comprensión de por qué se recomienda la combinación del NIST SP 800-61 y el ENISA CSIRT Framework para CSIRTs académicos.

Justificación:

1. El NIST SP 800-61 ofrece la combinación más fuerte de adaptabilidad, exhaustividad y reconocimiento internacional.
2. Su enfoque detallado proporciona una base sólida para establecer y mejorar las capacidades de gestión de incidentes.
3. El complemento del ENISA CSIRT Framework aporta herramientas y plantillas específicas para CSIRTs, facilitando la implementación práctica.
4. Esta combinación permite aprovechar lo mejor de ambos marcos: la profundidad del NIST y la practicidad del ENISA.

Pasos para la implementación:

1. Adoptar la estructura general y fases de gestión de incidentes del NIST SP 800-61.
2. Utilizar las herramientas y plantillas del ENISA CSIRT Framework para la implementación práctica.
3. Adaptar los procesos según las necesidades específicas de la institución académica.
4. Establecer un ciclo de revisión anual para incorporar actualizaciones de ambos marcos.

En conclusión, las mejores prácticas internacionales en CSIRTs académicos enfatizan la importancia de una estructura organizativa clara, servicios integrales, colaboración activa, formación continua, uso de tecnologías avanzadas y evaluación sistemática del

desempeño. La implementación efectiva de estas prácticas puede mejorar significativamente la postura de ciberseguridad de las instituciones académicas.

4.2.11 Análisis de Referencias para el Diseño del CSIRT UCE

El presente estudio busca desarrollar un modelo de CSIRT efectivo y adaptado a las necesidades específicas de la Universidad Central del Ecuador. Para ello, se analizarán:

1. **Referencias Locales Directas:**

- CSIRT CEDIA (Ecuador): Como coordinador nacional de CSIRTs académicos y socio estratégico de la UCE
- CSIRT EPN: Por su experiencia en el contexto universitario público ecuatoriano
- CSIRT UTPL: Por su implementación exitosa en el contexto universitario ecuatoriano

2. **Casos de Estudio Complementarios:**

- Análisis de la implementación de CSIRTs en universidades públicas similares a la UCE en:
    - Tamaño de población estudiantil
    - Estructura organizacional
    - Contexto regulatorio similar
    - Recursos disponibles comparables

Este enfoque más acotado permitirá:

- Identificar mejores prácticas aplicables al contexto específico de la UCE
- Aprender de experiencias en entornos similares
- Desarrollar un modelo realista y viable para la UCE
- Establecer colaboraciones efectivas con CSIRTs locales

Los criterios de comparación utilizados en la tabla se basan en los siguientes marcos y estándares:

Tabla 29 Marcos de Referencia y Estándares para la Implementación del CSIRT

Criterio de Comparación	Marco/Estándar de Referencia	Año	Relevancia para el Análisis
Estructura Organizacional	- FIRST CSIRT Framework - ENISA CSIRT Setting up Guide - ISO/IEC 27035-2	2023 2022 2023	Define modelos organizacionales estándar para CSIRTs y su integración en instituciones académicas
Tamaño del Equipo	- NIST SP 800-61r2 - Carnegie Mellon's Handbook for CSIRTs	2023 2021	Establece parámetros para dimensionamiento de equipos CSIRT según el tamaño y complejidad de la institución

Servicios Principales	- FIRST Services Framework v3.1 - OAS Best Practices	2023 2022	Define catálogo estándar de servicios CSIRT y niveles de madurez en su implementación
Enfoque en Investigación	- SIM3 Maturity Model - GÉANT Campus Best Practices	2022 2023	Establece métricas para evaluar capacidades de investigación y desarrollo en seguridad
Colaboración Nacional	- ITU National Cybersecurity Strategy - ENISA Cooperation Framework	2023 2022	Define marcos de colaboración entre CSIRTs y estrategias de coordinación nacional

La tabla utiliza estos criterios estandarizados para permitir una comparación objetiva entre las diferentes instituciones, facilitando la identificación de mejores prácticas y áreas de oportunidad para el desarrollo del CSIRT en la UCE. Los datos específicos de cada institución fueron obtenidos de sus respectivos informes anuales y sitios web oficiales.

4.2.12 Implicaciones para el modelo CSIRT de la UCE

Basándose en este análisis ampliado, se recomienda que el modelo CSIRT para la UCE:

1. Se establezca como una unidad independiente con apoyo directo de la alta dirección conjuntamente con la Dirección de Tecnología de la Información y Comunicación.
2. Ofrezca un conjunto de servicios de seguridad, priorizando la gestión de incidentes y la capacitación.
3. Invierta en tecnologías clave como SIEM y herramientas de análisis de vulnerabilidades.
4. Desarrolle un programa robusto de capacitación y concientización.
5. Establezca colaboraciones activas con otros CSIRTs académicos en Ecuador, especialmente CEDIA y EPN.
6. Implemente un sistema de métricas para evaluar y mejorar continuamente su desempeño.
7. Adapte sus políticas y procedimientos al marco regulatorio ecuatoriano en materia de ciberseguridad.
8. Desarrolle capacidades especializadas que reflejen las fortalezas y necesidades específicas de la UCE.
9. Participe activamente en iniciativas de coordinación interinstitucional a nivel nacional.

4.3 FASE 2: Diagnóstico de la situación actual de ciberseguridad en la UCE

4.3.1 Estado actual de la UCE

Fundada en 1820, la Universidad Central del Ecuador se encuentra actualmente en un momento crítico en el desarrollo de la tecnología y la ciberseguridad. Como una de las instituciones de educación superior más antiguas y prestigiosas del país, la UCE enfrenta

el desafío de modernizar su infraestructura tecnológica y fortalecer las prácticas de ciberseguridad en un entorno digital y de amenazas cada vez más complejo. Este análisis de la situación actual proporciona una visión general completa del panorama tecnológico de la universidad, desde la infraestructura de red y los sistemas de información hasta la seguridad de TI y las políticas de recursos humanos. El objetivo es establecer una línea de base clara que ayude a identificar fortalezas, debilidades y áreas de mejora, sentando así las bases para una implementación efectiva del CSIRT y el fortalecimiento general de la estrategia de ciberseguridad de la empresa.

4.3.2 Organización

La Universidad Central del Ecuador tiene una estructura orgánica jerárquica liderada por el Honorable Consejo Universitario. En este marco, el Rector supervisa tres Vicerrectores principales: Estudios Académicos y de Posgrado, Administración y Finanzas, Investigación, Doctorado e Innovación. Esta organización permite a la UCE gestionar eficazmente sus funciones académicas, administrativas y de investigación a través de varias juntas y departamentos dedicados.

Los órganos colegiados

Los órganos colegiados de la UCE son cuerpos colectivos que toman decisiones conjuntas y se dividen en tres categorías principales: instituciones de educación superior, instituciones académicas universitarias y organismos administrativos colegiados.

Instituciones de educación superior:

Estos órganos son los encargados de definir las políticas generales y estratégicas de la universidad. En este contexto, el **Honorable Consejo Universitario** (HCU) es el máximo órgano de gobierno de la UCE. Está compuesto por miembros de la comunidad universitaria, incluidos representantes del cuerpo docente, estudiantes y trabajadores. Sus decisiones afectan a todas las áreas de la universidad, desde la política educativa hasta la administración financiera.

4.3.2.1 Instituciones académicas universitarias:

Estos órganos se encargan de la gestión académica dentro de las diferentes facultades y carreras de la UCE. Entre ellos se incluyen:

- Junta Directiva del Colegio: Responsable de la gestión de las carreras y facultades, asegurando que las decisiones tomadas en el Consejo Universitario se implementen adecuadamente a nivel académico.
- Asesor de carrera: Un funcionario académico que guía a los estudiantes en sus decisiones educativas y profesionales, asegurando que se cumplan los objetivos curriculares y profesionales de los programas académicos.
- Comité de búsqueda de egresados de la facultad: Este comité se encarga de mantener el vínculo con los egresados, facilitando su integración en el mercado laboral y promoviendo su participación en actividades de la universidad, como redes de exalumnos o proyectos de investigación.

4.3.2.2 **Organismos administrativos colegiados:**

Estos órganos se centran en la administración y el cumplimiento de las normativas dentro de la UCE. Entre ellos se encuentran:

- Comité de Ética: Encargado de velar por el cumplimiento de los principios éticos en la universidad, tanto en el ámbito académico como en el administrativo. Este comité revisa casos de infracción ética y propone sanciones o recomendaciones.
- Comisión especial para asuntos disciplinarios: Este organismo maneja los casos relacionados con conductas inapropiadas dentro de la universidad, tanto de estudiantes como de personal. Se encarga de investigar y sancionar faltas disciplinarias, de acuerdo con los reglamentos internos.
- Comisión Electoral: Este comité organiza y supervisa las elecciones internas de la universidad, asegurando que los procesos electorales sean justos y transparentes. Es fundamental para la selección de representantes estudiantiles y docentes en los diferentes órganos de gobierno.

4.3.2.3 **Composición del Honorable Consejo Universitario**

El HCU es un órgano de gran relevancia dentro de la UCE, encargado de velar por el respeto y la dignidad dentro de la institución, así como de garantizar el cumplimiento de los principios fundamentales de la universidad. Su composición es diversa, lo que permite una representación amplia de los diferentes sectores de la comunidad universitaria. Este consejo está compuesto por:

- **Rector:** Máxima autoridad ejecutiva de la universidad, responsable de la gestión general y la implementación de las políticas aprobadas por el Honorable Consejo Universitario. El rector también representa a la universidad ante organismos externos.
- **Vicerrector de Estudios Académicos y de Posgrado:** Responsable de supervisar los programas académicos y de posgrado de la universidad. Este vicerrector se asegura de que las políticas educativas sean aplicadas de manera efectiva y que los programas cumplan con los estándares de calidad.
- **Vicepresidente de Investigación, Doctorados e Innovación:** Este vicerrector se enfoca en la promoción de la investigación, la gestión de programas de doctorado y la implementación de proyectos de innovación dentro de la universidad. Su rol es clave para el desarrollo académico y científico de la UCE.
- **Vicepresidente de Administración y Finanzas:** Encargado de la gestión administrativa y financiera de la universidad, asegurando una administración eficiente de los recursos y el cumplimiento de las políticas financieras.
- **16 Decanos:** Estos son representantes de las diferentes facultades o áreas dentro de la universidad. Su función es representar los intereses de sus respectivos departamentos en las discusiones del HCU.
- **21 representantes docentes:** Profesores de la universidad elegidos para representar al cuerpo docente en el consejo. Estos representantes participan en la toma de decisiones que afectan tanto a la enseñanza como a las condiciones laborales del personal académico.

- **13 representantes estudiantiles:** Alumnos elegidos para representar a la comunidad estudiantil. Su función es asegurar que las decisiones del consejo reflejen también los intereses y necesidades de los estudiantes.
- **1 representante de los trabajadores:** Un miembro del personal administrativo o de servicios, que representa los intereses de los trabajadores no docentes en las decisiones del consejo. Este representante asegura que se consideren las preocupaciones del personal en las políticas de la universidad.

La estructura y composición del HCU garantizan que las decisiones se tomen de manera equitativa y que todos los sectores de la universidad tengan voz en los procesos de gobierno. Este enfoque colegiado permite a la UCE mantener un equilibrio entre las necesidades académicas, administrativas y estudiantiles, fortaleciendo su capacidad de tomar decisiones efectivas y bien informadas.

4.3.3 Análisis de seguridad de la información.

Como institución de educación superior con una larga trayectoria, la Universidad Central del Ecuador enfrenta grandes desafíos en el campo de la seguridad de la información. Estos desafíos son particularmente complejos debido a la diversidad de la comunidad universitaria y la diversidad de los servicios que brinda.

Se analizó registros de soporte de mesa de ayuda de la Universidad Central del Ecuador que abarca incidentes reportados desde el 24 de mayo de 2024 hasta el 07 de agosto de 2024, con lo que podemos resumir en los siguiente.

4.3.3.1 **Estadísticas específicas sobre tipos de incidentes más comunes:**

1. Problemas con correo electrónico institucional: 47 incidentes (16.5% del total)
    - Inconvenientes en envío y recepción de correos: 22 casos
    - Problemas de ingreso a la cuenta: 11 casos
    - Inconvenientes con aplicaciones de Office 365: 14 casos
2. Inconvenientes académicos para estudiantes: 43 incidentes (15.1% del total)
    - Problemas en el proceso de matriculación: 24 casos
    - Dificultades en la visualización de reportes/calificaciones: 13 casos
    - Problemas de ingreso al sistema: 6 casos
3. Problemas con sistemas institucionales: 29 incidentes (10.2% del total)
    - Sistema de Titulación: 15 casos
    - Sistema de Talento Humano: 9 casos
    - Otros sistemas (Investigación, Resoluciones): 5 casos
4. Soporte a computadores institucionales: 24 incidentes (8.4% del total)
    - Instalación, configuración y solución de errores de aplicaciones: 17 casos
    - Inconvenientes de acceso al computador: 7 casos
5. Problemas académicos para docentes y administrativos: 22 incidentes (7.7% del total)
    - Inconvenientes con paso de notas: 6 casos
    - Problemas de ingreso a sistemas: 6 casos
    - Otros problemas académicos: 10 casos

4.3.3.2 **Tiempo promedio de detección y respuesta a incidentes:**

Durante este período, se observa que:

1. Tiempo de asignación: La mayoría de los incidentes fueron asignados en menos de 1 hora, con algunos casos llegando hasta 2-3 horas.
2. Tiempo de solución: Varía significativamente dependiendo del tipo de incidente:
    - Problemas simples de correo o acceso: 1-4 horas
    - Inconvenientes académicos: 6-24 horas
    - Problemas de sistemas institucionales: 1-3 días
    - Soporte a computadores: 1-2 días

Es importante notar que muchos incidentes quedaron sin resolver por períodos prolongados, algunos superando los 100 días dentro de este período,

4.3.3.3 **Impacto económico y operativo de los incidentes pasados:**

Aunque el documento no proporciona información directa sobre el impacto económico, podemos inferir algunos efectos operativos basados en la naturaleza y duración de los incidentes durante este período:

1. Pérdida de productividad: Los problemas con correo electrónico y aplicaciones de Office 365 probablemente causaron retrasos en la comunicación y el trabajo administrativo a lo largo de este tiempo.
2. Retrasos en procesos académicos: Los inconvenientes en matriculación, visualización de calificaciones y sistemas de titulación pudieron haber afectado negativamente la experiencia estudiantil y posiblemente retrasado graduaciones durante el período académico cubierto.
3. Sobrecarga del equipo de TI: La gran cantidad de incidentes no resueltos a tiempo sugiere que el equipo de soporte técnico estuvo sobrecargado durante este período, lo que podría haber llevado a una acumulación de problemas y una disminución en la calidad del servicio.
4. Posible pérdida de datos o seguridad comprometida: Algunos incidentes relacionados con cuentas comprometidas o problemas de acceso podrían haber expuesto datos sensibles o causada pérdida de información durante estos meses.
5. Interrupción de la investigación: Los problemas con el sistema de investigación podrían haber retrasado proyectos importantes o la presentación de resultados en el período analizado.

Para mejorar la gestión de incidentes, la Universidad Central del Ecuador debería considerar implementar cambios basados en los patrones observados durante periodo, incluyendo el aumento de la capacidad del equipo de soporte técnico, la implementación de sistemas de detección y respuesta más rápidos, la mejora en la capacitación de usuarios y la actualización y optimización de los sistemas críticos.

4.3.3.4 **Resumen de Incidentes.**

Tabla 30 Resumen de Incidentes de Seguridad y Soporte Técnico UCE 2024

Categoría de Incidente	Número de Casos	Porcentaje	Subcategorías Principales
Problemas con correo electrónico institucional	47	16.5%	- Envío y recepción (22 casos - Ingreso a la cuenta (11 casos) - Aplicaciones Office 365 (14 casos)
Inconvenientes académicos para estudiantes	43	15.1%	- Proceso de matriculación (24 casos) - Visualización de reportes/calificaciones (13 casos) - Ingreso al sistema (6 casos)
Problemas con sistemas institucionales	29	10.2%	- Sistema de Titulación (15 casos) - Sistema de Talento Humano (9 casos) - Otros sistemas (5 casos)
Soporte a computadores institucionales	24	8.4%	- Instalación y configuración de aplicaciones (17 casos) - Acceso al computador (7 casos)
Problemas académicos para docentes y administrativos	22	7.7%	- Paso de notas (6 casos) - Ingreso a sistemas (6 casos) - Otros problemas académicos (10 casos)
Otros incidentes	120	42.1%	Varios
Total de Incidentes	**285**	**100%**	

La tabla analiza 285 incidentes de seguridad y soporte técnico en la Universidad Central del Ecuador, clasificándolos en varias categorías:

1. **Problemas con correo electrónico institucional** (16.5%, 47 casos): Incluye dificultades en envío y recepción (22 casos), acceso a cuentas (11 casos) y problemas con Office 365 (14 casos).
2. **Inconvenientes académicos estudiantiles** (15.1%, 43 casos): Se destacan problemas en matriculación (24 casos), acceso a reportes y calificaciones (13 casos) y acceso al sistema (6 casos).
3. **Problemas con sistemas institucionales** (10.2%, 29 casos): Incidentes con el Sistema de Titulación (15 casos), Sistema de Talento Humano (9 casos) y otros sistemas (5 casos).
4. **Soporte a computadores institucionales** (8.4%, 24 casos): Incluye instalación y configuración de aplicaciones (17 casos) y problemas de acceso a computadores (7 casos).
5. **Problemas académicos de docentes y administrativos** (7.7%, 22 casos): Dificultades con el registro de calificaciones (6 casos), acceso a sistemas (6 casos) y otros problemas (10 casos).

Además, la categoría "Otros incidentes" representa un 42.1% (120 casos), sugiriendo la necesidad de una clasificación más detallada. Este análisis es clave para identificar áreas problemáticas, priorizar recursos, desarrollar estrategias preventivas, planificar capacitaciones y mejorar la resolución de incidentes.

4.3.4 Consideraciones para la Implementación de un CSIRT Académico en la UCE

Al considerar la implementación de un sistema robusto de seguridad de la información (como un CSIRT académico), la UCE debe considerar los siguientes factores:

- Falta de homogeneidad de procesos y procedimientos: la diversidad de roles y áreas dificulta la estandarización de métodos y prácticas de seguridad, lo que puede crear brechas de seguridad y dificultar la respuesta ante incidentes (CEFIPRA, 2020).
- Dificultades de comunicación y coordinación: la fragmentación de la academia en diferentes grupos con intereses y necesidades específicas puede obstaculizar la comunicación y coordinación efectiva necesarias para establecer un CSIRT funcional (CEFIPRA, 2020).
- Desafíos en la gestión de la información: La gran cantidad de datos sensibles que maneja la UCE, incluyendo información personal, financiera y académica, requiere un enfoque riguroso para asegurar la confidencialidad, integridad y disponibilidad de la información (CEFIPRA, 2020).
- Confidencialidad e integridad: Garantizar la protección de la información sensible de todos los miembros de la comunidad universitaria representa un desafío importante.

La creación de un CSIRT dentro de la UCE es crucial para fortalecer la ciberseguridad de la institución y proteger su información crítica. Un CSIRT eficaz puede mejorar la capacidad de la UCE para detectar, prevenir y responder a incidentes de seguridad, minimizar el impacto de estos incidentes y mantener la confianza de la comunidad universitaria.

4.3.5 Infraestructura tecnológica

La UCE cuenta con una infraestructura tecnológica compuesta por routers, switches y servidores, principalmente de la marca Cisco. La red de la universidad está segmentada en varias VLANs para estudiantes, docentes y personal administrativo, lo que facilita la gestión de tráfico y seguridad

El análisis de la infraestructura tecnológica incluyó un inventario de los equipos y sistemas utilizados en la UCE. A continuación, se detallan los componentes principales:

Equipos de Red y Servidores: Se realizó la identificación y catalogación de todos los equipos de red en la UCE, incluyendo routers, switches y servidores. Estos equipos están distribuidos a través de las 21 facultades y 16 áreas administrativas, y centralizados en el datacenter de la universidad. Este inventario permitió evaluar el estado actual de los equipos, su ubicación y configuración, así como la necesidad de actualizaciones para aquellos que están cerca de quedar obsoletos.

Dispositivos de Usuario Final: se catalogaron más de 5000 dispositivos, que incluyen computadoras personales, laptops, tablets y smartphones utilizados por estudiantes, Docentes y personal administrativo. esta información es esencial para comprender el alcance de la infraestructura tecnológica de la universidad y para planificar medidas de seguridad adecuadas, como la implementación de políticas de gestión de dispositivos y la protección de datos.

Sistemas de Gestión: Se identificaron sistemas críticos en la UCE que incluyen plataformas de gestión académica, sistemas de recursos humanos, y otros sistemas administrativos. Estos sistemas son soportados por software especializado, como:

- **Sistema Integral de Información Universitaria (SIIU)**: Para la gestión de registros académicos y administrativos.
- **Quipux**: Para la gestión documental y digitalización de procesos administrativos.
- **Plataforma Moodle**: Utilizada para el aprendizaje en línea y la gestión de contenidos educativos.
- **Sistemas ERP**: Para la gestión integrada de recursos y procesos administrativos.
- **Sistema de HelpDesk**: Sistema de soporte general para la universidad

El datacenter centralizado aloja estos sistemas, proporcionando servicios de almacenamiento y procesamiento de datos, asegurando su seguridad y disponibilidad para todas las facultades y áreas administrativas. Estos sistemas son cruciales para las operaciones diarias y la eficiencia institucional.

Sistemas Operativos:

Predomina el uso de sistemas operativos Windows en aproximadamente el 85% de los dispositivos. Sin embargo, se identificaron versiones desactualizadas que no cuentan con soporte, lo que aumenta la exposición a vulnerabilidades. Por ejemplo, se encontró que algunas estaciones de trabajo aún utilizan Windows 7, que ya no recibe actualizaciones de seguridad.

Aplicaciones de Seguridad:

La cobertura de software antivirus y antimalware es inconsistente, con muchas estaciones de trabajo y servidores sin protección actualizada. Esto representa un riesgo significativo, especialmente ante la creciente sofisticación de amenazas como ransomware.

4.3.6 Evaluación de la Red y sus Componentes

La evaluación de la red incluyó:

4.3.6.1 **Arquitectura de Red:**

La arquitectura de red de la Universidad Central del Ecuador incluye una segmentación avanzada a través del uso de VLANs y redes Wi-Fi segmentadas. Esta estructura se organiza de la siguiente manera:

- **VLAN de Estudiantes**: Presente en todos los laboratorios, facilita el acceso a recursos educativos y de investigación específicos para estudiantes.
- **VLAN de Docentes**: Distribuida en áreas estratégicas, proporciona a los docentes acceso controlado a herramientas y datos necesarios para sus actividades académicas y de investigación.
- **VLAN Administrativa**: Gestiona datos sensibles y recursos críticos para las operaciones administrativas de la universidad, con medidas de seguridad reforzadas.
- **Zona Militarizada para el Datacenter**: Un área de seguridad elevada, diseñada para proteger la infraestructura y los datos críticos alojados en el datacenter centralizado.
- **VLAN Wi-Fi**: La red Wi-Fi está segmentada para proporcionar acceso controlado a diferentes grupos de y para proteger datos sensibles mediante políticas de acceso diferenciadas.

4.3.7 Evaluación de la efectividad de los procesos actuales de respuesta a incidentes:

Esta segmentación de red, tanto cableada como inalámbrica, es crucial para mantener la seguridad de la información, minimizar los riesgos de brechas y facilitar una gestión eficiente del tráfico de datos en toda la institución.

Evaluación de la efectividad de los procesos actuales de respuesta a incidentes:

1. Falta de formalización y estandarización:
    - Los procedimientos de respuesta a incidentes no están suficientemente documentados.
    - Hay una carencia de prácticas estandarizadas para la respuesta a incidentes de seguridad.
2. Ausencia de un equipo dedicado:
    - No existe un equipo dedicado exclusivamente a la gestión de incidentes de seguridad.
    - Esto compromete la eficacia y rapidez de la respuesta ante incidentes.
3. Tiempos de respuesta variables:
    - El tiempo de solución varía significativamente según el tipo de incidente:
        - Problemas simples: 1-4 horas
        - Inconvenientes académicos: 6-24 horas
        - Problemas de sistemas institucionales: 1-3 días
        - Soporte a computadores: 1-2 días
    - Muchos incidentes quedaron sin resolver por períodos prolongados, algunos superando los 100 días.
4. Sistema de gestión de incidentes limitado:

- Existe un sistema para la gestión de incidentes, pero no está adaptado específicamente a las áreas de seguridad.
- Es un sistema generalizado que no cubre todas las necesidades de un CSIRT.

5. Falta de capacitación especializada:
   - Hay una necesidad urgente de formación especializada y continua en seguridad de la información para el personal.

Identificación de carencias en herramientas o habilidades:

1. Herramientas de seguridad:
   - Falta de sistemas de detección y prevención de intrusiones (IDS/IPS).
   - Ausencia de soluciones de gestión de eventos e información de seguridad (SIEM).
   - Carencia de herramientas de análisis forense.
2. Habilidades del personal:
   - Falta de personal especializado en ciberseguridad.
   - Necesidad de capacitación en detección y respuesta a incidentes.
   - Carencia de habilidades en análisis forense digital.
3. Procesos y procedimientos:
   - Ausencia de procesos formales para la detección, análisis y mitigación de incidentes.
   - Falta de políticas de seguridad integrales que cubran todas las áreas críticas.
4. Conciencia de seguridad:
   - Baja conciencia sobre la ciberseguridad entre los usuarios finales, incluyendo estudiantes y personal.
   - Falta de programas de capacitación y concienciación efectivos.
5. Gestión de riesgos:
   - Gestión técnica de riesgos incompleta.
   - Falta de evaluaciones periódicas de riesgos y estrategias de mitigación adecuadas.
6. Comunicación y coordinación:
   - Ausencia de protocolos claros para compartir información sensible durante incidentes.
   - Falta de coordinación efectiva entre diferentes departamentos durante la respuesta a incidentes.

En resumen, la UCE enfrenta desafíos significativos en sus capacidades de respuesta a incidentes, incluyendo la falta de un equipo dedicado, procesos estandarizados, herramientas especializadas y habilidades técnicas específicas en ciberseguridad. La implementación de un CSIRT, ayudaría a abordar estas carencias y mejorar significativamente la postura de seguridad de la institución.

4.3.8 Evaluación de habilidades y conocimientos actuales:

Según el análisis de la situación actual de ciberseguridad en la UCE:

- Se identificó una baja conciencia sobre la ciberseguridad entre los usuarios finales, incluyendo estudiantes y personal.
- Muchos usuarios desconocen las políticas de seguridad existentes y cómo aplicarlas.
- Se observó que varios encuestados no cambian sus contraseñas regularmente ni utilizan métodos seguros de gestión de contraseñas.
- Los registros de soporte de mesa de ayuda revelaron incidentes frecuentes relacionados con problemas de correo electrónico, incluyendo casos de phishing y accesos no autorizados.

Identificación de brechas y prioridades:

Basándose en los hallazgos, las principales brechas de conocimiento incluyen:

a) Gestión segura de contraseñas
b) Identificación y prevención de ataques de phishing
c) Conocimiento y aplicación de políticas de seguridad institucionales
d) Manejo seguro de información sensible
e) Uso apropiado de sistemas y aplicaciones institucionales

Prioridades de capacitación:

1. Concientización básica en ciberseguridad para toda la comunidad universitaria
2. Capacitación específica en detección y prevención de phishing
3. Formación en gestión segura de credenciales y autenticación
4. Educación sobre políticas y procedimientos de seguridad de la UCE
5. Entrenamiento en el uso seguro de sistemas académicos y administrativos

4.3.9 Identificar Vulnerabilidades

Comparar los niveles de madurez actuales con los estándares internacionales y las mejores prácticas puede ayudar a identificar brechas en la ciberseguridad de la UCE. Algunas de las brechas identificadas incluyen:

- **Política de seguridad incompleta:** Falta una política de seguridad integral que cubra todas las áreas críticas de la infraestructura tecnológica de la UCE. Es posible que las políticas actuales no cubran aspectos clave como la gestión del acceso, la protección de datos confidenciales y la respuesta a incidentes. Además, es posible que las políticas existentes no reflejen oportunamente las amenazas emergentes y las mejores prácticas internacionales.

- **Implementación inconsistente**: las políticas y procedimientos de seguridad no se aplican de manera consistente en toda la universidad. Esta inconsistencia puede generar vulnerabilidades de seguridad en algunas áreas porque los controles de seguridad en estas áreas no son tan fuertes como en otras. La falta de una

implementación uniforme también puede dificultar la evaluación de la eficacia de las medidas de seguridad.

- **Capacidades de respuesta limitadas**: las capacidades de respuesta a incidentes de seguridad son actualmente limitadas. La UCE no contaba con un equipo dedicado y bien capacitado para gestionar eficazmente los incidentes de seguridad de TI. Esto incluye la falta de procesos formales para la detección, análisis y mitigación de incidentes.

- **Falta de concientización y capacitación**: Estudiantes, docentes y administradores carecen de concientización en ciberseguridad. Además, no existen programas de capacitación continuos para el personal de TI y otros empleados clave. La falta de concientización y capacitación aumenta el riesgo de error humano, lo que lleva a incidentes de seguridad.

- **Herramientas y tecnología insuficientes**: La UCE no cuenta con las herramientas y tecnología adecuadas para detectar y responder a las ciberamenazas. Esto incluye la falta de sistemas de detección de intrusos, herramientas de análisis forense y soluciones de gestión de incidentes. La falta de estas herramientas puede obstaculizar la capacidad de la universidad para identificar y mitigar amenazas de manera efectiva.

- **Gestión de riesgos insuficiente**: la gestión técnica de riesgos es incompleta. No se realizaron evaluaciones periódicas de riesgos y no se implementaron estrategias de mitigación adecuadas. La gestión de riesgos es clave para identificar y priorizar amenazas y vulnerabilidades e implementar medidas de protección adecuadas.

4.3.10 Evaluación de impacto potencial

Evaluar el impacto potencial de las vulnerabilidades de seguridad identificadas es fundamental para comprender la gravedad de los riesgos que enfrenta UCE. Una violación de la seguridad puede tener varios impactos negativos en una universidad, que incluyen:

- Interrupción del servicio: Los incidentes de seguridad pueden interrumpir los servicios educativos y administrativos, comprometiendo la continuidad de las operaciones. Esto podría incluir interrupciones en las plataformas de aprendizaje en línea, los sistemas de gestión académica y los servicios administrativos.

- Pérdida de datos: las violaciones de seguridad pueden provocar la pérdida o corrupción de datos críticos, incluidos registros académicos de estudiantes y empleados, información financiera y datos personales. La pérdida de datos puede tener importantes consecuencias legales y de reputación para la universidad.

- Daño a la reputación: los incidentes de seguridad pueden dañar la reputación de la UCE y socavar la confianza de los estudiantes, el personal y otras partes interesadas. El daño a la reputación puede tener efectos duraderos y afectar la capacidad de una universidad para atraer estudiantes y Docentes.

- Costos financieros: los incidentes de seguridad pueden generar costos financieros significativos, incluidos costos de mitigación, costos de recuperación y posibles sanciones legales. Además, las inversiones necesarias para mejorar la infraestructura de seguridad pueden ser considerables.

4.3.11 Estrategias de mitigación

Para abordar las vulnerabilidades de seguridad identificadas, es necesario desarrollar estrategias de mitigación específicas. Algunas estrategias sugeridas incluyen:

- Desarrollar una política de seguridad integral: Establecer y mantener una política de seguridad integral que cubra todas las áreas clave de la infraestructura tecnológica de la UCE. Estas políticas deben revisarse y actualizarse periódicamente para reflejar las mejores prácticas y las amenazas emergentes.

- Implementación uniforme de políticas y procedimientos: Garantizar la implementación uniforme de políticas y procedimientos de seguridad en toda la Universidad. Esto puede incluir capacitar y supervisar a los empleados para garantizar el cumplimiento.

- Formación y sensibilización: Desarrollar un programa de formación continua en ciberseguridad para estudiantes, Docentes y directivos. Estos planes deben cubrir aspectos clave de la ciberseguridad, incluida la gestión de contraseñas, la identificación de correos electrónicos de phishing y la respuesta a incidentes.

- Adquirir herramientas y tecnologías de seguridad: invertir en herramientas y tecnologías de seguridad adecuadas, incluidos sistemas de detección de intrusos, herramientas de análisis forense y soluciones de gestión de incidentes. Estas

herramientas son fundamentales para detectar y responder eficazmente a las amenazas.

- Fortalecer la gestión de riesgos: Desarrollar un plan de gestión de riesgos tecnológicos, que incluya una evaluación periódica de los riesgos y la implementación de estrategias de mitigación. La gestión de riesgos debe ser un proceso continuo de identificación y priorización de amenazas y vulnerabilidades.

4.3.12 Casos relacionados con la gestión de incidencias de correo electrónico institucional

En UCE, la gestión de incidentes de correo electrónico institucional es un aspecto importante de la ciberseguridad. Cada mes se registran un gran número de casos de incidentes de soporte, con una media de 30 casos de correos electrónicos bloqueados por spam o virus. Estos incidentes ponen de relieve la necesidad de mejorar las capacidades de prevención y respuesta frente a las ciberamenazas.

4.3.13 Evaluación de Capacidades Actuales de Respuesta a Incidentes

La evaluación de las capacidades de respuesta a incidentes incluyó:

4.3.13.1 Procedimientos de Respuesta a Incidentes:

La UCE cuenta con un sistema para la gestión de incidentes, pero la revisión mostró una falta de formalización y capacitación regular, lo cual se identificó como una brecha significativa. Los procedimientos actuales no están suficientemente documentados, y hay una carencia de prácticas estandarizadas para la respuesta a incidentes de seguridad.

Actualmente tenemos la mesa de ayuda la misma que no está adaptada a las áreas de la seguridad más bien es algo muy generalizado.

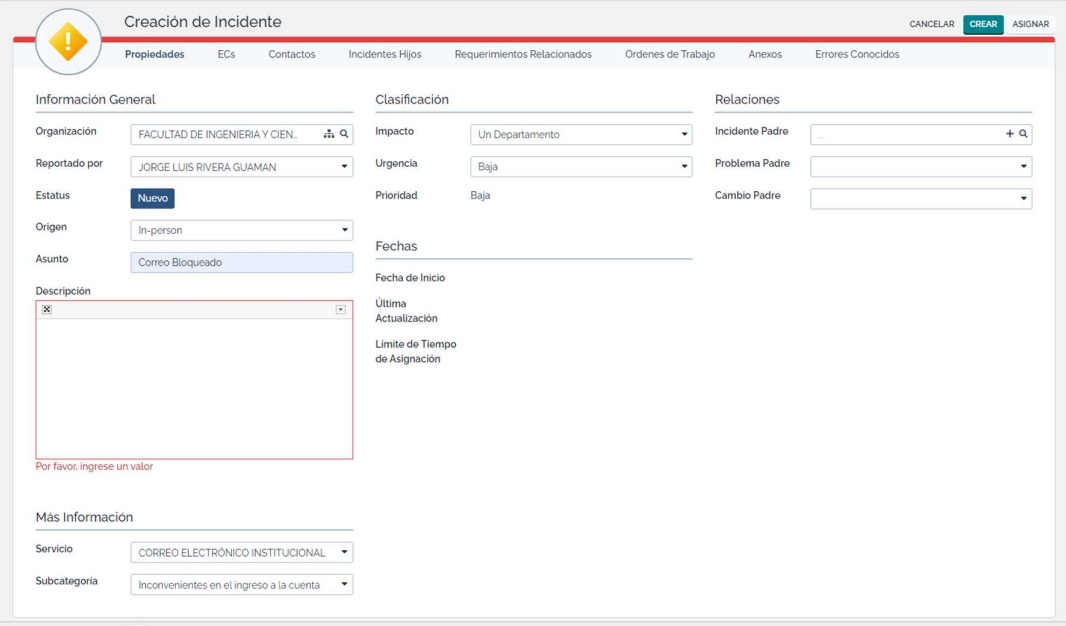


Imagen 4 Mesa de ayuda, DTIC UCE

4.3.14 Equipo de Respuesta a Incidentes:

La evaluación del equipo responsable de la gestión de incidentes reveló una necesidad urgente de formación especializada y continua. Actualmente, no existe un equipo dedicado exclusivamente a la gestión de incidentes, lo que compromete la eficacia y la rapidez de la respuesta. Se recomienda establecer un equipo especializado y proveer capacitación regular para asegurar que estén al día con las mejores prácticas y tecnologías de seguridad, a continuación, detallamos el equipo de DTIC en la cual carece de la seguridad de la información.

Tabla 31 Equipo DTIC UCE 2024

Sección	Nombre
Dirección	ING. MARIO RAÚL MORALES MORALES, PhD.
Desarrollo	ING. DENNIS COLLAGUAZO
	ING. EDGAR ULLOA
	ING. MARCELO QUISHPE
	ING. JAVIER LOACHAMÍN
	ING. DANIEL ALBUJA
	ING. VINICIO ROSALES
	ING. FREDDY GUZMÁN
	ING. PAULINA ORTÍZ
	ING. CARLOS VITERI
Infraestructura e Innovación	ING. GABRIEL CASTRO
	ING. RENE CAMACHO
	ING. ALEX CAIZAPANTA
	ING. PAÚL TUTILLO

Administración de Base de Datos	ING. VINICIO RAMÍREZ
Proyectos y Producción	ING. MARIA ESTHER MOYANO
	ING. FÁTIMA TOBAR
	LCDA. MARÍA JÓSE ANDRADE
Soporte Técnico	ING. MARÍA ELENA CARRILLO
	ING. BELÉN OBANDO
	TLGO. HECTOR TOAPANTA
	TLGA. SONIA GARZÓN
	LCDO. EDUARDO PALACIOS
	LCDO. RAMIRO ALMEIDA
	TLGO. FREDDY CRUZ
Secretaria de Dirección	LCDA. TERESA RAMOS
Personal de Apoyo	ÁNGEL SARANGO

4.3.15 Frecuencia y Naturaleza de los Eventos

Los casos de soporte por correo electrónico empresarial incluyen:

- Correos electrónicos interceptados por spam o virus: Estos incidentes suponen una importante amenaza para la seguridad de la información, ya que pueden servir como vectores para la propagación de malware o intentos de phishing.
- Acceso no autorizado: los intentos de obtener acceso no autorizado a las cuentas de correo electrónico de la empresa pueden resultar en la divulgación de información confidencial.
- Phishing: correos electrónicos diseñados para engañar a los usuarios para que revelen información confidencial como contraseñas o información financiera.

4.3.16 Impacto de Ataques Informáticos en la Comunidad Universitaria

El impacto de estos acontecimientos en la comunidad universitaria puede ser dramático:

- Fallo de comunicación: los incidentes pueden interrumpir la comunicación entre estudiantes, Docentes y administradores, lo que afecta las operaciones diarias.
- Riesgo de exposición de información sensible: El acceso no autorizado y los ataques de phishing pueden llevar a la exposición de información personal y académica.
- Pérdida de confianza: la frecuente ocurrencia de estos incidentes puede minar la confianza de los usuarios en la seguridad de los sistemas de información de la organización.
-

4.3.17 Percepción y conocimientos

Se ha identificado una baja conciencia sobre la ciberseguridad entre los usuarios finales, incluyendo estudiantes y personal. Esto resalta la necesidad de programas de capacitación

y concienciación para mejorar las prácticas de seguridad dentro de la comunidad universitaria

Los usuarios finales, incluyendo docentes y estudiantes, expresaron una baja conciencia sobre prácticas seguras de ciberseguridad. Muchos desconocen las políticas de seguridad existentes y cómo aplicarlas. Por ejemplo, varios encuestados indicaron que no cambian sus contraseñas regularmente ni utilizan métodos seguros de gestión de contraseñas.

4.3.18 Políticas y procedimientos

La creación de un CSIRT en la UCE requiere una comprensión exhaustiva de los requisitos regulatorios y legales que rigen este tipo de iniciativas. Este análisis se centra en identificar y cumplir con las normativas nacionales e internacionales, las políticas internas de la universidad, y las mejores prácticas establecidas en el ámbito de la ciberseguridad.

Estado Actual de Políticas y Procedimientos en la UCE

1. **Marco Normativo Aplicable**

La UCE, como institución de educación superior pública, debe cumplir con:

- Ley de Comercio Electrónico
- Ley Orgánica de Educación Superior
- Normativas de ARCOTEL
- Estándares internacionales relevantes (ISO/IEC 27001, GDPR)

2. **Situación Actual en la UCE**

A. **Políticas de Control de Acceso**

- **Estado Actual:**
  - No existe una política institucional formal sobre instalación de software
  - Se han identificado instalaciones no autorizadas de TeamViewer en múltiples facultades
  - No hay un inventario completo de software de acceso remoto
- **Riesgos Identificados:**
  - Accesos no controlados a la red universitaria
  - Vulnerabilidades de seguridad por software no autorizado
  - Falta de monitoreo de conexiones remotas

B. **Autenticación y Autorización**

- **Estado Actual:**
  - Solo sistemas críticos como el financiero utilizan 2FA
  - La mayoría de sistemas académicos utilizan autenticación simple
  - No existe una política uniforme de contraseñas
- **Sistemas con 2FA implementado:**

- Sistema financiero
- Correo institucional (parcialmente)

- **Sistemas sin 2FA:**
  - Portal académico
  - Sistemas de biblioteca
  - Plataformas de aprendizaje virtual

3. **Brechas Identificadas**

- Falta de políticas formales de seguridad
- Ausencia de estándares de autenticación unificados
- Control limitado sobre software instalado
- Monitoreo insuficiente de accesos remotos

4. **Necesidades Inmediatas**

- Desarrollo de política integral de seguridad
- Implementación uniforme de 2FA en todos los sistemas críticos
- Establecimiento de controles de software
- Creación de procedimientos de monitoreo y auditoría

4.4 FASE 3: Modelo propuesto de CSIRT para la UCE

4.4.1 Fundamentos del Modelo Propuesto

Tabla 32 Implementación del Modelo CSIRT Híbrido Orientado a Capacitación

Componentes del Modelo Híbrido Educativo	Descripción
1. Centro de Capacitación CSIRT (Equipo Central)	**Ubicación**: DTIC UCE **Composición**: Coordinador de Programas Educativos Especialistas en Capacitación (2) Desarrollador de Contenidos Analista de Efectividad Educativa **Responsabilidades**: Desarrollo de programas de capacitación Creación de materiales educativos Evaluación de efectividad de programas Coordinación de campañas de concienciación
2. Unidades de Capacitación Departamental	**Ubicación**: 21 facultades **Roles por unidad**: Facilitador local de capacitación Embajador de ciberseguridad **Responsabilidades**: Implementación de programas locales Adaptación de contenidos al contexto

	Mentorías personalizadas

Tabla 33 Estructura Formativa del Programa de Capacitación CSIRT UCE

Estructura de Programas Educativos	Descripción
1. Niveles de Formación	Básico: Concienciación general Intermedio: Prácticas seguras específicas Avanzado: Formación especializada
2. Modalidades de Entrega	Presencial: Talleres y ejercicios prácticos Virtual: Módulos en línea y webinars Híbrido: Combinación de ambos enfoques

La tabla presenta el diseño educativo del CSIRT estructurado en dos componentes principales: niveles de formación (básico, intermedio y avanzado) y modalidades de entrega (presencial, virtual e híbrido). Este marco proporciona una estructura clara para la implementación de programas de capacitación en ciberseguridad, adaptándose a diferentes niveles de conocimiento y necesidades de aprendizaje en la comunidad universitaria.

Tabla 34 Implementación del Marco NIST SP 800-61 en el Programa Educativo del CSIRT UCE

Aplicación del Marco NIST SP 800-61 con Enfoque Educativo	Descripción
3.3.2.1 Fase de Preparación	**Desarrollo de Programas**: Análisis de necesidades educativas Diseño de currículos específicos Creación de materiales didácticos Establecimiento de métricas de aprendizaje **Infraestructura Educativa**: Plataforma de e-learning Laboratorios de práctica Recursos multimedia Herramientas de evaluación
3.3.2.2 Fase de Detección y Análisis	**Evaluación Continua**: Diagnóstico de conocimientos Identificación de brechas educativas Análisis de efectividad de programas Retroalimentación de participantes **Medición de Impacto**:

	Evaluaciones pre y post capacitación Seguimiento de cambios conductuales Análisis de incidentes relacionados
3.3.2.3 Fase de Implementación y Mejora	**Estrategias de Implementación**: Programas regulares de capacitación Campañas de concienciación Ejercicios prácticos Mentorías y seguimiento **Mejora Continua**: Actualización de contenidos Refinamiento de metodologías Adaptación a nuevas amenazas Incorporación de feedback
3.3.2.4 Evaluación de Resultados	**Métricas Educativas**: Tasas de participación Niveles de retención Cambios conductuales Reducción de incidentes **Indicadores de Efectividad**: Mejora en prácticas de seguridad Incremento en reportes proactivos Adopción de medidas preventivas Satisfacción de participantes

La tabla describe la adaptación del marco NIST SP 800-61 al contexto educativo del CSIRT, estructurada en cuatro fases principales: preparación (desarrollo de programas e infraestructura), detección y análisis (evaluación y medición de impacto), implementación y mejora (estrategias y actualización continua), y evaluación de resultados (métricas e indicadores de efectividad). Este marco proporciona una estructura sistemática para desarrollar, implementar y evaluar los programas de capacitación en ciberseguridad de la UCE.

4.4.1.1 **Componentes del Modelo Híbrido Educativo**

La implementación siguiendo el marco NIST SP 800-61 adaptado proporciona una estructura sistemática para desarrollar y mantener programas educativos efectivos en ciberseguridad.

4.4.2 Introducción:

Esta propuesta para la implementación de un Equipo CSIRT en la UCE surge como resultado de los análisis realizados en la Fase 2 de este proyecto y se fundamenta en la experiencia adquirida en el área de seguridad de la información. A lo largo de esta fase,

se mantuvieron conversaciones con el personal de la Dirección de Tecnologías de la Información y Comunicaciones (DTIC) de la UCE, donde se identificaron diversas vulnerabilidades que afectan a la comunidad universitaria.

Uno de los hallazgos más preocupantes fue el riesgo constante al que están expuestos muchos de los colaboradores de la universidad. Diariamente, llegan mensajes de phishing que intentan engañar a los usuarios para robar sus credenciales de acceso. Estos ataques no solo comprometen sus cuentas de correo institucional, sino que también se extienden a sus redes sociales, afectando su privacidad y seguridad personal.

En este contexto, se hace evidente la necesidad de un CSIRT que no solo responda a los incidentes de seguridad, sino que también eduque y proteja a la comunidad universitaria frente a estas amenazas. La implementación de este modelo permitirá a la UCE mejorar su capacidad de detección y respuesta ante incidentes, y garantizar una mayor protección para su infraestructura tecnológica y los datos sensibles que maneja.

4.4.3 Objetivo del modelo propuesto

El objetivo principal de este modelo es implementar un Equipo de Respuesta a Incidentes de Seguridad Informática en la UCE centrado en la capacitación y concientización de los usuarios, con el fin de prevenir ataques cibernéticos y mejorar significativamente la postura de seguridad de la institución.

Este objetivo nace de:

1. Hallazgos de la Fase 2: El diagnóstico realizado reveló una baja conciencia de ciberseguridad entre los usuarios y una falta de programas de capacitación efectivos. Esto indica la necesidad urgente de un enfoque educativo en seguridad informática.
2. Prevención como estrategia clave: Reconociendo que la mayoría de los incidentes de seguridad tienen su origen en errores humanos o falta de conocimiento, la prevención a través de la educación se convierte en la estrategia más efectiva.
3. Empoderamiento de la comunidad universitaria: Al centrarse en la capacitación, el CSIRT busca empoderar a cada miembro de la comunidad de la UCE para que se convierta en un agente activo en la protección de la información y los recursos digitales de la universidad.
4. Adaptación a recursos limitados: Dado que la UCE, como muchas instituciones académicas, puede tener recursos limitados para tecnologías de seguridad avanzadas, un enfoque en la educación permite maximizar la seguridad con una inversión eficiente.
5. Creación de una cultura de ciberseguridad: El objetivo es ir más allá de la simple transmisión de conocimientos, buscando instaurar una cultura de ciberseguridad que perdure y evolucione dentro de la institución.
6. Alineación con la misión educativa: Este enfoque en capacitación se alinea perfectamente con la misión educativa fundamental de la UCE, extendiendo esta misión al ámbito crucial de la seguridad informática.

7. Preparación para amenazas futuras: Al equipar a la comunidad universitaria con conocimientos y habilidades en ciberseguridad, la UCE estará mejor preparada para enfrentar las amenazas cambiantes del panorama digital.
8. Mejora de la gestión de incidentes: El análisis de la fase 2 reveló tiempos de respuesta variables y muchos incidentes sin resolver por períodos prolongados. El CSIRT busca mejorar significativamente la eficiencia en la detección, respuesta y resolución de incidentes de seguridad.

Este objetivo busca transformar la aproximación de la UCE a la ciberseguridad, pasando de un modelo reactivo a uno proactivo basado en la educación y la prevención. Al centrarse en la capacitación de usuarios, el CSIRT aspira a crear una primera línea de defensa robusta contra los ataques cibernéticos, mejorando la resiliencia general de la institución frente a las amenazas digitales.

4.4.4 Alcance del CSIRT

El CSIRT de la UCE se enfocará principalmente en el desarrollo e implementación de programas de capacitación y concientización para los usuarios de la comunidad universitaria, abarcando las 21 facultades y 16 áreas administrativas. Su alcance incluirá la creación de programas educativos, campañas de concientización, evaluación continua de la efectividad de las capacitaciones, y el establecimiento de una cultura de ciberseguridad en toda la institución.

4.4.5 Justificación

El análisis realizado en la Fase 2 reveló múltiples vulnerabilidades en la infraestructura tecnológica y en las prácticas de seguridad de la UCE,

El análisis realizado en la Fase 2 reveló:

- Baja conciencia de ciberseguridad entre los usuarios, con muchos desconociendo las políticas de seguridad existentes y cómo aplicarlas.
- Falta de programas de capacitación efectivos y ausencia de un equipo dedicado a la gestión de incidentes de seguridad.
- Vulnerabilidades derivadas del desconocimiento de prácticas seguras, como la gestión inadecuada de contraseñas y la susceptibilidad a ataques de phishing.
- Tiempos de respuesta variables para la resolución de incidentes, con algunos casos superando los 100 días sin resolverse.
- Falta de herramientas especializadas en seguridad, como sistemas de detección y prevención de intrusiones (IDS/IPS) y soluciones de gestión de eventos e información de seguridad (SIEM).2.2 Beneficios esperados de un enfoque centrado en la capacitación
- Reducción significativa de incidentes causados por error humano
- Empoderamiento de la comunidad universitaria en temas de ciberseguridad
- Mejora en la detección temprana de amenazas por parte de los usuarios
- Creación de una cultura de seguridad sostenible

4.4.6 Alineación con objetivos institucionales

El CSIRT se alinea con los objetivos de la UCE de proporcionar un entorno educativo seguro y confiable, proteger la integridad de la investigación académica, y mantener la reputación de la universidad como líder en innovación y excelencia académica.

4.4.7 Marco Estratégico del CSIRT

4.4.7.1 Misión y Visión del CSIRT

La misión y visión del CSIRT de la UCE están alineadas con los objetivos institucionales y las necesidades identificadas durante el análisis de la fase 2 y las conversaciones con el personal de TIC.

- **Misión:** Implementar y mantener un programa integral de educación y concientización en ciberseguridad para la comunidad de la Universidad Central del Ecuador, con el objetivo de reducir los incidentes de seguridad relacionados con errores humanos en un plazo de prudencial en años. Este programa se enfocará en desarrollar competencias críticas en seguridad informática, fomentar una cultura de responsabilidad digital, y proporcionar herramientas prácticas para la prevención y detección temprana de amenazas cibernéticas.
- Visión**:** Establecer a la Universidad Central del Ecuador como un centro de excelencia en educación en ciberseguridad dentro del sistema universitario ecuatoriano, caracterizado por:

4.4.7.2 Objetivos Estratégicos de Capacitación y Prevención

4.4.7.2.1 Desarrollar programas de capacitación integrales en ciberseguridad

Descripción: Crear e implementar un conjunto completo de programas de capacitación en ciberseguridad adaptados a diferentes niveles de conocimiento y roles dentro de la comunidad universitaria (estudiantes, docentes, personal administrativo).

Implementación:

1. Realizar una evaluación de necesidades de capacitación en toda la universidad.
2. Diseñar currículos específicos para cada grupo objetivo.
3. Desarrollar materiales de capacitación (manuales, presentaciones, ejercicios prácticos).
4. Implementar una plataforma de e-learning para facilitar el acceso a los cursos.
5. Establecer un calendario de capacitaciones presenciales y en línea.
6. Implementar un sistema de seguimiento y certificación de la capacitación.

Justificación: La capacitación integral es fundamental para crear una base sólida de conocimientos en ciberseguridad. El análisis de la Fase 2 reveló una falta generalizada de conocimientos en seguridad informática entre la comunidad universitaria, lo que aumenta la vulnerabilidad a ataques. Programas de capacitación bien diseñados pueden reducir significativamente los riesgos de seguridad y empoderar a los usuarios para proteger los activos digitales de la universidad.

4.4.7.2.2 Implementar campañas de concientización efectivas

Descripción: Diseñar y ejecutar campañas de concientización en ciberseguridad que lleguen a toda la comunidad universitaria, utilizando diversos canales de comunicación y métodos de engagement.

Implementación:

1. Desarrollar una estrategia de comunicación multicanal (email, redes sociales, carteles, eventos).
2. Crear contenido atractivo y fácil de entender (infografías, videos cortos, podcasts).
3. Organizar eventos de concientización (Día de la Ciberseguridad, seminarios, talleres).
4. Implementar un sistema de recompensas para incentivar la participación.
5. Utilizar técnicas de gamificación para aumentar el engagement.
6. Medir y analizar el impacto de las campañas regularmente.

Justificación: Las campañas de concientización son cruciales para mantener la seguridad en la mente de todos los miembros de la comunidad universitaria. La Fase 2 mostró una baja conciencia de ciberseguridad entre los usuarios, lo que los hace susceptibles a ataques de ingeniería social y phishing. Campañas efectivas pueden cambiar comportamientos y crear una cultura de seguridad proactiva.

4.4.7.2.3 Promocionar la ciberseguridad en el currículo académico de la UCE

Descripción: Incorporar módulos de ciberseguridad como curso opcional en los programas académicos existentes de todas las facultades, asegurando que todos los estudiantes reciban formación básica en seguridad informática.

Implementación:

1. Formar un comité interdisciplinario para diseñar contenidos de ciberseguridad relevantes para cada disciplina.
2. Desarrollar un módulo básico de ciberseguridad adaptable a diferentes carreras.
3. Capacitar a los docentes en la enseñanza de conceptos de ciberseguridad.
4. Implementar proyectos interdisciplinarios que incluyan aspectos de ciberseguridad.
5. Establecer colaboraciones con la industria para proporcionar casos de estudio reales.
6. Evaluar y actualizar regularmente el contenido para mantenerlo relevante.

Justificación: La integración de la ciberseguridad en el currículo asegura que todos los graduados tengan un nivel básico de competencia en seguridad digital. Esto es crucial en un mundo cada vez más digitalizado, donde la ciberseguridad es relevante para todas las disciplinas. Además, prepara mejor a los estudiantes para el mercado laboral, donde las habilidades en ciberseguridad son cada vez más valoradas.

4.4.7.2.4 Establecer un programa de embajadores de ciberseguridad

Descripción: Crear una red de estudiantes, docentes y personal administrativo que actúen como promotores de la ciberseguridad dentro de sus respectivas áreas, difundiendo buenas prácticas y sirviendo como punto de contacto para consultas de seguridad.

Implementación:

1. Desarrollar criterios de selección para los embajadores.
2. Implementar un programa de formación avanzada para los embajadores seleccionados.
3. Crear un sistema de reconocimiento e incentivos para los embajadores.
4. Establecer canales de comunicación regulares entre los embajadores y el CSIRT.
5. Organizar reuniones periódicas y eventos de networking para los embajadores.
6. Evaluar el impacto del programa a través de encuestas y métricas de seguridad.

Justificación: Un programa de embajadores aprovecha el poder de la influencia entre pares para promover la ciberseguridad. Los embajadores pueden llegar a áreas de la universidad que podrían ser difíciles de alcanzar para el CSIRT central. Además, este enfoque descentralizado permite una respuesta más rápida a las preocupaciones de seguridad locales y fomenta un sentido de propiedad de la seguridad en toda la comunidad.

4.4.7.2.5 Reducir los incidentes de seguridad causados por error humano

Descripción: Implementar medidas proactivas y educativas para disminuir significativamente el número de incidentes de seguridad atribuibles a errores humanos o falta de conocimiento.

Implementación:

1. Analizar los incidentes pasados para identificar patrones de error humano.
2. Desarrollar módulos de capacitación específicos dirigidos a los errores más comunes.
3. Implementar simulaciones de phishing y otros ataques para evaluar y mejorar la conciencia de seguridad.
4. Establecer políticas y procedimientos claros para el manejo de información sensible.
5. Implementar controles técnicos (como autenticación de dos factores) para mitigar los riesgos de error humano.
6. Monitorear y reportar regularmente sobre la reducción de incidentes relacionados con errores humanos.

Justificación: Los errores humanos son una de las principales causas de brechas de seguridad. La Fase 2 reveló que muchos incidentes en la UCE se debían a la falta de conocimiento o descuido de los usuarios. Reducir estos incidentes no solo mejora la seguridad general, sino que también ahorra recursos al disminuir el tiempo y esfuerzo

dedicados a la resolución de problemas evitables. Además, este objetivo proporciona una métrica clara para medir el éxito del CSIRT educativo.

4.4.8 Procesos de Implementación de Objetivos Estratégicos

4.4.8.1 Programa de Capacitación Integral

Tabla 35 Plan de Implementación del Programa de Capacitación CSIRT UCE

Fase	Periodo	Actividades	Entregables
Evaluación Inicial	0-3 meses	- Encuestas departamentales - Análisis de incidentes - Identificación de brechas	- Informe de necesidades - Mapa de brechas - Plan de acción
Diseño y Desarrollo	3-6 meses	- Desarrollo curricular - Creación de materiales - Definición de niveles	- Currículos por nivel - Materiales didácticos - Guías de instructor
Implementación	6-12 meses	- Lanzamiento de plataforma - Ejecución de programas - Evaluación continua	- Plataforma operativa - Reportes de progreso - Métricas de impacto

La tabla detalla el cronograma y fases de implementación del programa de capacitación del CSIRT, estructurado en tres etapas principales: evaluación inicial (0-3 meses), diseño y desarrollo (3-6 meses), e implementación (6-12 meses). Cada fase especifica actividades clave y entregables concretos, proporcionando una hoja de ruta clara para el establecimiento progresivo del programa de capacitación en ciberseguridad en la UCE.

4.4.8.2 Campañas de Concientización

Tabla 36 Fases de Implementación de Campañas de Concientización CSIRT UCE

Etapa	Duración	Actividades	Resultados Esperados
Planificación	Trimestre 1	- Estrategia de comunicación - Planificación de canales - Diseño de mensajes	- Plan estratégico - Calendario de campañas - Presupuesto
Implementación	Trimestre 2	- Lanzamiento de campañas - Gestión de canales - Eventos y actividades	- Materiales publicados - Registro de eventos - Participación
Evaluación	Trimestre 3-4	- Medición de impacto - Análisis de resultados - Ajustes estratégicos	- Informes de impacto - Recomendaciones - Plan de mejoras

La tabla presenta el ciclo de implementación de las campañas de concientización del CSIRT, distribuido en tres etapas principales: planificación (primer trimestre), implementación (segundo trimestre) y evaluación (tercer y cuarto trimestre). Cada etapa detalla actividades específicas y resultados esperados, estableciendo un marco estructurado para el desarrollo y ejecución efectiva de las campañas de concientización en seguridad informática en la UCE.

4.4.8.3 **Integración Curricular**

Tabla 37 Fases de Integración Curricular en Ciberseguridad CSIRT UCE

Etapa	Periodo	Acciones	Indicadores de Éxito
Preparación	Semestre 1	- Formación de comité - Diseño de módulos - Desarrollo de contenidos	- Comité establecido - Módulos diseñados - Contenido aprobado
Piloto	Semestre 2	- Implementación piloto - Capacitación docente - Evaluación inicial	- Pilotos completados - Docentes capacitados - Informes de evaluación
Expansión	Año 2	- Despliegue completo - Soporte continuo - Mejora iterativa	- Implementación total - Sistema de soporte - Mejoras documentadas

La tabla establece el cronograma de implementación para la integración de ciberseguridad en el currículo académico de la UCE, distribuido en tres etapas: preparación (primer semestre), piloto (segundo semestre) y expansión (segundo año). Cada fase especifica acciones clave e indicadores de éxito, proporcionando una estructura clara para la incorporación progresiva de contenidos de seguridad informática en los programas académicos de la universidad.

4.4.8.4 **Programa de Embajadores**

Tabla 38 Estrategia de Selección y Formación

Fase	Tiempo	Actividades Clave	Métricas
Selección	Mes 1-2	- Definir criterios - Convocar candidatos - Evaluar postulantes	- Criterios establecidos - Candidatos evaluados - Embajadores seleccionados
Formación	Mes 3-4	- Capacitación inicial - Asignación de roles - Establecer objetivos	- Capacitaciones completadas - Roles asignados - Objetivos definidos
Operación	Mes 5-12	- Implementación activa - Seguimiento regular - Evaluación continua	- Actividades realizadas - Informes de progreso - Evaluaciones completadas

4.4.8.5 **Reducción de Errores Humanos**

Tabla 39 Gestión de Análisis, Control y Mejora

Componente	Periodicidad	Actividades	Indicadores
Análisis	Continuo	- Revisión de incidentes - Identificación de patrones - Evaluación de riesgos	- Patrones identificados - Riesgos evaluados - Recomendaciones
Control	Por fases	- Implementar controles - Establecer políticas - Monitorear efectividad	- Controles activos - Políticas implementadas - Reportes de efectividad
Mejora	Continuo	- Ajustar controles - Actualizar políticas	- Ajustes realizados - Políticas actualizadas

		- Reforzar capacitación	- Capacitación mejorada

Cada tabla ofrece una vista clara y estructurada de las fases de implementación, los periodos de tiempo, las actividades específicas, y los entregables o resultados esperados, junto con las métricas de éxito. Esta organización facilita la planificación detallada, permite un seguimiento eficaz del progreso, optimiza la asignación de responsabilidades y proporciona un marco claro para medir los resultados.

4.4.9 Indicadores clave de rendimiento (KPIs) para programas académicos

Tasa de Integración Curricular (TIC)

Descripción: Porcentaje de programas académicos que han incorporado módulos de ciberseguridad en su currículo.

Fórmula: (Número de programas con módulos de ciberseguridad / Número total de programas académicos) x 100

Objetivo: Alcanzar un 80% de integración en 3 años.

Frecuencia de medición: Anual

Importancia: Mide el éxito en la integración de la ciberseguridad en diversas disciplinas académicas.

Tasa de Participación en Actividades de Ciberseguridad (TPAC)

Descripción: Porcentaje de estudiantes que participan en actividades extracurriculares relacionadas con ciberseguridad.

Fórmula: (Número de estudiantes participantes / Número total de estudiantes) x 100

Objetivo: Alcanzar un 50% de participación en 2 años.

Frecuencia de medición: Semestral

Importancia: Indica el nivel de interés y compromiso de los estudiantes con la ciberseguridad más allá del currículo obligatorio.

Tasa de Participación en Capacitaciones (TPC)

- **Descripción:** Porcentaje de miembros de la comunidad universitaria que han completado al menos una capacitación en ciberseguridad.
- **Fórmula:** (Número de participantes / Población total de la UCE) x 100
- **Objetivo:** 80% en el primer año, incrementando a 95% en el tercer año.
- **Frecuencia de medición:** Semestral

Índice de Aplicación Práctica (IAP)

Descripción: Porcentaje de estudiantes que demuestran la aplicación práctica de conocimientos de ciberseguridad en proyectos o pasantías.

Fórmula: (Número de estudiantes con proyectos prácticos aprobados / Número total de estudiantes en cursos de ciberseguridad) x 100

Objetivo: Alcanzar un 70% de aplicación práctica en 2 años.

Frecuencia de medición: Anual

Importancia: Evalúa la capacidad de los estudiantes para aplicar conocimientos teóricos en situaciones reales.

Tasa de Retención de Conocimientos (TRC)

Descripción: Porcentaje de conocimientos retenidos por los estudiantes 6 meses después de completar un curso de ciberseguridad.
Fórmula: (Puntuación en evaluación de seguimiento / Puntuación en evaluación inicial) x 100
Objetivo: Mantener una tasa de retención del 80% o superior.
Frecuencia de medición: Semestral (6 meses después de cada curso)
Importancia: Mide la efectividad a largo plazo de los programas educativos.

Índice de Contribución a la Investigación (ICI)

Descripción: Número de publicaciones, presentaciones o proyectos de investigación en ciberseguridad realizados por estudiantes y facultad.

Fórmula: Suma total de contribuciones de investigación en un año académico

Objetivo: Incrementar las contribuciones en un 20% anualmente.

Frecuencia de medición: Anual

Importancia: Evalúa el impacto académico y la contribución al campo de la ciberseguridad.

Tasa de Engagement en Campañas (TEC)

- **Descripción:** Nivel de interacción con materiales de concientización (emails, posts, videos).
- **Fórmula:** (Número de interacciones / Número total de materiales distribuidos) x 100
- **Objetivo:** 40% de engagement en el primer año, 70% en el tercer año.
- **Frecuencia de medición:** Mensual

Tasa de Reporte de Incidentes (TRI)

- **Descripción:** Incremento en el número de incidentes de seguridad reportados por usuarios.

- **Fórmula:** ((Número de reportes en período actual - Número de reportes en período anterior) / Número de reportes en período anterior) x 100
- **Objetivo:** Incremento del 50% en el primer año, estabilizándose en el tercer año.
- **Frecuencia de medición:** Mensual

Tiempo Medio de Respuesta a Incidentes (TMRI)

- **Descripción:** Tiempo promedio desde la detección hasta la resolución de un incidente.
- **Fórmula:** Suma de tiempos de resolución / Número total de incidentes
- **Objetivo:** 24 horas en el primer año, reduciendo a 8 horas en el tercer año.
- **Frecuencia de medición:** Mensual

Tasa de Prevención de Incidentes (TPI)

- **Descripción:** Reducción en el número de incidentes de seguridad tras la implementación de medidas preventivas.
- **Fórmula:** ((Número de incidentes en período anterior - Número de incidentes en período actual) / Número de incidentes en período anterior) x 100
- **Objetivo:** Reducción del 30% en el primer año, 60% en el tercer año.
- **Frecuencia de medición:** Semestral

Tasa de Cumplimiento Normativo (TCN)

- **Descripción:** Grado de cumplimiento con regulaciones y estándares de seguridad aplicables.
- **Fórmula:** (Número de requisitos cumplidos / Número total de requisitos aplicables) x 100
- **Objetivo:** 90% de cumplimiento en el primer año, 100% en el tercer año.
- **Frecuencia de medición:** Semestral

4.4.10 Definición de Estructura Organizativa

El diseño de la estructura organizativa del CSIRT es fundamental para asegurar una respuesta efectiva y coordinada a los incidentes de seguridad. Es importante destacar que este departamento debe estar ligado a dirección de tecnologías con el fin de aprovechar los conocimientos de los técnicos como a continuación, se describen los roles clave y sus responsabilidades:

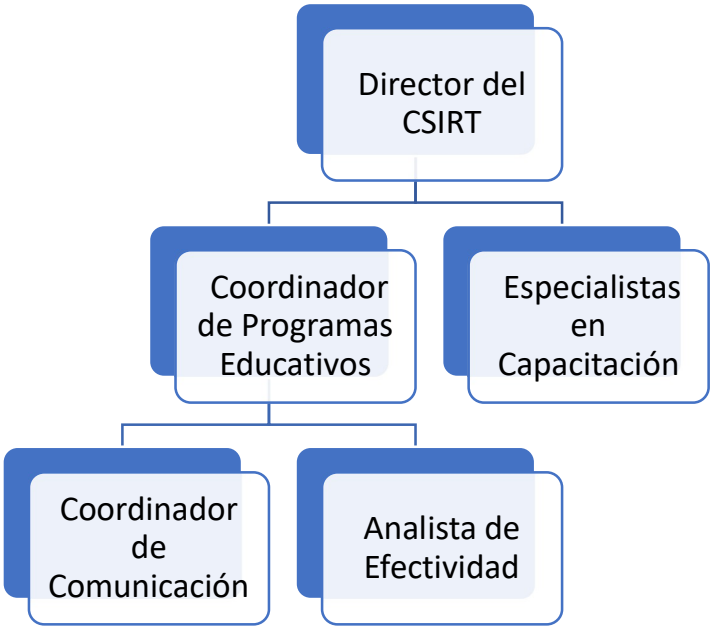


Tabla 40 Estructura Organizativa del CSIRT Educativo UCE

Rol	Descripción	Responsabilidades Principales	Responsabilidades de Capacitación
Director de CSIRT	Líder estratégico y enlace con dirección UCE	- Desarrollo estrategia educativa - Gestión de recursos - Relaciones institucionales	- Supervisión programas educativos - Aprobación contenidos - Medición impacto formativo
Coordinador de Programas Educativos	Gestión de programas de capacitación	- Diseño curricular - Coordinación instructores - Evaluación programas	- Desarrollo plan formativo - Supervisión implementación - Gestión calidad educativa
Especialistas en Capacitación **(2)**	Desarrollo e implementación de formación	- Creación contenidos - Facilitación talleres - Evaluación aprendizaje	- Instrucción directa - Mentoría estudiantes - Actualización materiales
Coordinador de Comunicación	Gestión campañas y comunicaciones	- Estrategia comunicacional - Campañas awareness - Medición efectividad	- Diseño campañas - Gestión embajadores - Eventos especiales

Analista de Efectividad	Evaluación y mejora de programas	- Análisis métricas - Evaluación impacto - Recomendaciones mejora	- Evaluación programas - Análisis resultados - Propuestas optimización

Tabla 41 Estructura de Soporte

Función	Responsabilidades Generales	Enfoque en Capacitación
Soporte Técnico	- Mantenimiento plataformas - Gestión recursos técnicos - Resolución problemas	- Soporte plataforma e-learning - Apoyo laboratorios prácticos - Gestión recursos educativos
Gestión de Contenidos	- Desarrollo materiales - Actualización recursos - Control calidad	- Creación contenido didáctico - Adaptación materiales - Gestión biblioteca recursos

Tabla 42 Coordinación con Facultades

Nivel	Roles	Responsabilidades Educativas
Facultades	Embajadores de Seguridad	- Implementación local programas - Feedback necesidades específicas - Coordinación actividades locales
Departamentos	Coordinadores Departamentales	- Adaptación contenidos - Seguimiento participación - Reporte efectividad

Las tablas presentan la estructura organizativa del CSIRT y su enfoque en capacitación. La primera tabla detalla los roles del equipo, incluyendo al Director de CSIRT, quien lidera la estrategia educativa; el Coordinador de Programas Educativos, encargado de diseñar y evaluar la formación; y los Especialistas en Capacitación, que desarrollan contenido y facilitan talleres. La segunda tabla describe el soporte técnico y la gestión de contenidos, esenciales para el mantenimiento de plataformas y la creación de recursos educativos. Finalmente, la tercera tabla aborda la coordinación con facultades, destacando los Embajadores de Seguridad y Coordinadores Departamentales, que implementan programas y adaptan contenidos según las necesidades locales, asegurando así una capacitación integral y efectiva en toda la organización.

Esta estructura:

1. Prioriza las funciones educativas
2. Mantiene enfoque en capacitación
3. Facilita coordinación efectiva
4. Asegura calidad formativa
5. Permite medición de impacto

4.4.10.1 **Relación con otras unidades académicas y administrativas de la UCE**

Colaboración estrecha con facultades, departamento de recursos humanos, y oficina de comunicaciones para integrar la ciberseguridad en todos los aspectos de la vida universitaria considerando esta jerarquía.

- Dirección de TIC
- Departamento de Recursos Humanos
- Oficina de Comunicaciones
- Facultades y departamentos académicos

4.5 Servicios del CSIRT

El CSIRT de la UCE se enfocará principalmente en servicios orientados a la educación, prevención y apoyo básico en seguridad, alineándose con su misión de fortalecer la cultura de ciberseguridad en la comunidad universitaria. A continuación, se detallan los servicios propuestos:

4.5.1 Servicios de capacitación y concientización

- Cursos y talleres de ciberseguridad para diferentes niveles:
  - Se desarrollarán programas de capacitación adaptados a distintos perfiles dentro de la comunidad universitaria (estudiantes, docentes, personal administrativo).
  - Los cursos cubrirán temas como seguridad básica en línea, protección de datos personales, identificación de amenazas comunes, y prácticas seguras en el uso de tecnologías.
  - Se ofrecerán talleres prácticos para reforzar los conocimientos adquiridos, incluyendo ejercicios de identificación de phishing, configuración segura de dispositivos, y gestión de contraseñas.
- Programas de certificación interna en seguridad informática:
  - Se implementará un sistema de certificaciones internas para reconocer y validar los conocimientos en ciberseguridad de los miembros de la comunidad universitaria.
  - Las certificaciones se estructurarán en niveles (básico, intermedio, avanzado) y se enfocarán en áreas específicas como seguridad en redes, protección de datos, y respuesta a incidentes.
  - Estas certificaciones servirán como incentivo para la formación continua y podrán ser reconocidas en el expediente académico o laboral dentro de la UCE.
- Simulaciones y ejercicios prácticos de seguridad:
  - Se organizarán ejercicios de simulación de ataques cibernéticos para poner a prueba los conocimientos y la capacidad de respuesta de los participantes.
  - Se llevarán a cabo competencias de seguridad (CTF - Capture The Flag) para fomentar el aprendizaje práctico y el trabajo en equipo en la resolución de desafíos de seguridad.
  - Se realizarán simulacros de respuesta a incidentes para preparar a la comunidad universitaria en la gestión de situaciones de crisis de seguridad.

4.5.2 Servicios de asesoramiento en prevención

- Consultoría en mejores prácticas de seguridad:
  - El CSIRT ofrecerá servicios de consultoría a departamentos y facultades sobre la implementación de mejores prácticas de seguridad en sus operaciones diarias.
  - Se proporcionará asesoramiento en la selección y configuración de herramientas de seguridad adecuadas para diferentes entornos académicos y administrativos.
  - Se ofrecerá orientación en la creación y mantenimiento de políticas de seguridad específicas para cada área de la universidad.
- Evaluaciones de riesgo desde la perspectiva del usuario:
  - Se realizarán evaluaciones periódicas para identificar los riesgos de seguridad más relevantes para los diferentes grupos de usuarios dentro de la UCE.
  - Se proporcionarán recomendaciones personalizadas basadas en estas evaluaciones para mejorar la postura de seguridad de cada grupo.
  - Se desarrollarán métricas para medir y hacer seguimiento a la evolución de los riesgos de seguridad en el tiempo.
- Guías y recursos de autoformación:
  - Se creará y mantendrá un repositorio en línea de recursos educativos sobre ciberseguridad, incluyendo guías paso a paso, videos tutoriales, y documentación técnica.
  - Se desarrollarán infografías y materiales visuales para facilitar la comprensión de conceptos complejos de seguridad.
  - Se implementará un sistema de aprendizaje en línea que permita a los usuarios acceder a cursos y materiales de formación a su propio ritmo.

4.5.3 Servicios básicos de apoyo en seguridad

- Centro de ayuda para consultas de seguridad:
  - Se establecerá un punto de contacto centralizado para que la comunidad universitaria pueda realizar consultas relacionadas con la seguridad informática.
  - Se implementará un sistema de tickets para gestionar y dar seguimiento a las consultas y solicitudes de asistencia en temas de seguridad.
  - Se ofrecerá soporte a través de múltiples canales, incluyendo correo electrónico, chat en línea y asistencia telefónica.
- Coordinación inicial en caso de incidentes de seguridad:
  - El CSIRT actuará como primer punto de contacto para la notificación de incidentes de seguridad dentro de la UCE.
  - Se establecerán protocolos claros para la recepción, clasificación y escalamiento inicial de incidentes reportados.
  - Se proporcionará orientación inmediata a los usuarios afectados sobre las primeras acciones a tomar en caso de un incidente de seguridad.
- Difusión de alertas y recomendaciones de seguridad:
  - Se implementará un sistema de alerta temprana para informar a la comunidad universitaria sobre amenazas emergentes y vulnerabilidades críticas.

- Se emitirán boletines periódicos con recomendaciones de seguridad y mejores prácticas adaptadas al contexto universitario.
- Se utilizarán diversos canales de comunicación (correo electrónico, redes sociales, portal web) para asegurar una amplia difusión de la información de seguridad.

Estos servicios están diseñados para crear una base sólida de conocimientos en ciberseguridad dentro de la UCE, promoviendo una cultura de seguridad proactiva y empoderando a la comunidad universitaria para protegerse contra las amenazas cibernéticas. El enfoque en la educación y la prevención busca reducir los incidentes de seguridad y mejorar la capacidad de respuesta de la institución ante posibles ataques.

4.6 Aspectos Legales y de Cumplimiento para el CSIRT de la UCE en el Contexto Ecuatoriano

4.6.1 Marco Legal Ecuatoriano Relevante

4.6.1.1 Ley Orgánica de Protección de Datos Personales (2021)

- **Implicaciones para el CSIRT:**
  - Implementar medidas técnicas y organizativas para garantizar la seguridad de los datos personales.
  - Establecer procedimientos para la notificación de violaciones de datos personales.
  - Realizar evaluaciones de impacto en la protección de datos para operaciones de alto riesgo.

4.6.1.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

- **Implicaciones para el CSIRT:**
  - Asegurar la validez legal de las firmas electrónicas en las comunicaciones del CSIRT.
  - Implementar medidas para garantizar la integridad de los mensajes de datos.
  - Establecer políticas para el manejo de evidencia digital en casos de incidentes.

4.6.1.3 Código Orgánico Integral Penal (COIP)

- **Implicaciones para el CSIRT:**
  - Conocer y actuar en conformidad con las disposiciones sobre delitos informáticos.
  - Establecer protocolos para la preservación de evidencias en casos de ciberdelitos.
  - Colaborar con las autoridades en investigaciones de delitos informáticos cuando sea requerido.

4.6.1.4 Ley Orgánica de Telecomunicaciones

- **Implicaciones para el CSIRT:**

- Cumplir con las normativas de seguridad en las redes de telecomunicaciones de la universidad.
- Coordinar con los proveedores de servicios de internet para la gestión de incidentes.

4.6.1.5 Ley Orgánica de Educación Superior (LOES)

- **Implicaciones para el CSIRT:**
  - Alinear las actividades del CSIRT con los principios de autonomía universitaria.
  - Asegurar la protección de la información académica y de investigación.

4.6.2 Regulaciones Sectoriales

4.6.2.1 Normativas de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT)

- **Implicaciones para el CSIRT:**
  - Cumplir con los estándares de seguridad de la información establecidos para instituciones de educación superior.
  - Reportar incidentes de seguridad que puedan afectar la integridad de los sistemas académicos.

4.6.2.2 Directrices del Comité de Seguridad de la Información del Sector Público

- **Implicaciones para el CSIRT:**
  - Alinear las políticas y procedimientos del CSIRT con las directrices nacionales de ciberseguridad.
  - Participar en iniciativas de colaboración en ciberseguridad a nivel nacional.

4.6.3 Estándares Internacionales Aplicables

4.6.3.1 ISO/IEC 27001 - Sistema de Gestión de Seguridad de la Información

- **Implicaciones para el CSIRT:**
  - Implementar un Sistema de Gestión de Seguridad de la Información (SGSI) alineado con este estándar.
  - Realizar auditorías internas y externas periódicas para mantener la conformidad.

4.6.3.2 NIST Cybersecurity Framework

- **Implicaciones para el CSIRT:**
  - Adoptar las mejores prácticas del framework para la identificación, protección, detección, respuesta y recuperación ante incidentes de ciberseguridad.

4.6.4 Consideraciones Específicas para la UCE

4.6.4.1 Política de Privacidad y Protección de Datos de la UCE

- **Implicaciones para el CSIRT:**
  - Alinear las operaciones del CSIRT con la política interna de privacidad de la universidad.
  - Establecer procedimientos para el manejo de datos sensibles de estudiantes y personal.

4.6.4.2 Reglamentos Internos de la UCE

- **Implicaciones para el CSIRT:**
  - Asegurar que las actividades del CSIRT estén en conformidad con los reglamentos internos de la universidad.
  - Proponer actualizaciones a los reglamentos para abordar nuevas necesidades de ciberseguridad.

4.6.5 Estrategias de Cumplimiento

4.6.5.1 Establecimiento de un Programa de Compliance

- Designar un oficial de cumplimiento dentro del CSIRT.
- Desarrollar y mantener un registro de requisitos legales y regulatorios aplicables.
- Realizar evaluaciones periódicas de cumplimiento.

4.7 Desarrollo de Programas de Capacitación

4.7.1 Diseño curricular de programas de ciberseguridad

El CSIRT de la UCE desarrollará currículos adaptados a los diferentes perfiles dentro de la comunidad universitaria:

- Para estudiantes:
  - Fundamentos de ciberseguridad y protección de datos personales
  - Seguridad en redes sociales y navegación web segura
  - Identificación de phishing y otros ataques comunes
  - Proyectos prácticos de seguridad aplicados a sus campos de estudio
- Para docentes:
  - Protección de propiedad intelectual y datos de investigación
  - Seguridad en plataformas de e-learning
  - Detección de plagio y fraude académico
  - Incorporación de conceptos de ciberseguridad en el currículo
- Para personal administrativo:
  - Manejo seguro de información confidencial
  - Seguridad en aplicaciones administrativas y financieras
  - Cumplimiento de normativas de protección de datos
  - Respuesta a incidentes y reporte de anomalías

Los currículos enfatizarán la aplicación práctica de los conceptos a través de ejercicios, simulaciones y estudios de caso relevantes para cada perfil.

4.7.2 Metodologías de enseñanza y aprendizaje

Se implementarán metodologías interactivas y participativas:

- Aprendizaje basado en problemas: Los participantes trabajarán en equipos para resolver desafíos de seguridad realistas.
- Estudios de caso: Análisis de incidentes reales ocurridos en otras instituciones académicas.
- Gamificación: Uso de juegos y competencias para aumentar el engagement, como CTFs (Capture The Flag) adaptados.
- Talleres prácticos: Sesiones hands-on en laboratorios para aplicar técnicas de seguridad.
- Simulaciones: Recreación de escenarios de ataque en ambientes controlados.
- Mentorías: Programas de acompañamiento entre pares para reforzar el aprendizaje.

4.7.3 Herramientas y recursos educativos

El CSIRT implementará:

- Plataforma de e-learning: Para ofrecer cursos en línea asíncronos y material de referencia. Se usará Moodle, ya implementado en la UCE.
- Laboratorios virtuales de seguridad: Entornos simulados para prácticas seguras de técnicas ofensivas y defensivas.
- Herramientas de simulación de ataques: Software como Metasploit para recrear técnicas de hacking ético.
- Recursos multimedia: Videos tutoriales, podcasts y animaciones sobre conceptos clave.
- Foros y wikis: Para fomentar el intercambio de conocimientos entre la comunidad.
- Repositorio de casos de estudio: Compilación de incidentes relevantes para el análisis.

4.7.4 Evaluación y mejora continua de programas

Se establecerá un ciclo de mejora continua que incluye:

- Evaluaciones pre y post capacitación para medir el incremento en conocimientos.
- Encuestas de satisfacción a los participantes.
- Seguimiento a largo plazo para evaluar la retención y aplicación de lo aprendido.
- Análisis de métricas de seguridad institucionales para correlacionar con la efectividad de las capacitaciones.
- Revisión trimestral de contenidos para incorporar información sobre nuevas amenazas.
- Comité asesor con expertos externos para recomendaciones de mejora.
- Benchmarking anual con programas de capacitación de otras instituciones académicas.

Este enfoque integral en capacitación permitirá al CSIRT de la UCE crear una cultura de ciberseguridad sólida y adaptable a las cambiantes amenazas del entorno digital.

4.8 Campañas de sensibilización

Las campañas de sensibilización constituyen un componente fundamental en la estrategia del CSIRT para fomentar una cultura de ciberseguridad en la Universidad Central del Ecuador (UCE). Estas iniciativas se estructuran en tres ejes principales: el diseño de campañas temáticas regulares, la creación de materiales de difusión y comunicación, y la organización de eventos y actividades de promoción de la ciberseguridad.

4.8.1 Diseño de campañas temáticas regulares

El CSIRT de la UCE implementará un programa integral de campañas temáticas regulares con el objetivo de incrementar la conciencia sobre ciberseguridad en toda la comunidad universitaria. La piedra angular de este programa será el "Mes de la Ciberseguridad", una campaña anual intensiva que se extenderá durante un mes completo. Durante este período, se abordarán diversos aspectos de la seguridad informática, dedicando cada semana a un tema específico, como la seguridad de contraseñas, la identificación y prevención de phishing, la seguridad en redes sociales, y la protección de datos personales.

4.8.2 Materiales de difusión y comunicación

Con el propósito de reforzar los mensajes clave de seguridad, el CSIRT desarrollará una gama diversa de materiales educativos. Estos incluirán infografías visualmente atractivas que explicarán conceptos de ciberseguridad de manera accesible, como la anatomía de un correo electrónico de phishing o los pasos para crear contraseñas seguras. Además, se producirán series de videos educativos cortos que abordarán temas específicos de ciberseguridad, incluyendo tutoriales sobre el uso de herramientas de seguridad y dramatizaciones de escenarios comunes de ciberataques.

La difusión de información se complementará con boletines informativos mensuales que contendrán actualizaciones sobre amenazas recientes, consejos de seguridad, noticias relevantes sobre ciberseguridad para la comunidad universitaria, y perfiles de los miembros del equipo CSIRT. Asimismo, se lanzará un podcast de ciberseguridad con episodios regulares que discutirán temas de actualidad, entrevistarán a expertos y responderán preguntas de la comunidad universitaria. Para proporcionar orientación práctica, se desarrollarán guías descargables con instrucciones detalladas sobre cómo implementar medidas de seguridad específicas, como la configuración de VPN para acceso remoto seguro o el cifrado de dispositivos móviles.

4.8.3 Eventos y actividades de promoción de la ciberseguridad

Para fomentar la participación activa en temas de ciberseguridad, el CSIRT organizará una serie de eventos y actividades a lo largo del año académico. Un evento destacado será el Hackathon de Ciberseguridad anual, una competencia donde equipos de estudiantes trabajarán en desafíos de seguridad informática, abordando temas como el hacking ético, el desarrollo de herramientas de seguridad y el análisis forense digital.

La Conferencia de Ciberseguridad UCE se establecerá como un evento anual de alto perfil, reuniendo a expertos en ciberseguridad, académicos y profesionales para compartir conocimientos y mejores prácticas. Este evento incluirá presentaciones de investigación en ciberseguridad, paneles de discusión sobre temas emergentes y talleres prácticos de seguridad informática.

Semestralmente, se organizará una Feria de Seguridad Digital donde se presentarán las últimas tecnologías y soluciones de seguridad. Este evento ofrecerá demostraciones de productos, estaciones interactivas para el aprendizaje práctico y concursos educativos sobre seguridad informática.

Adicionalmente, se implementará una Semana de Concientización en Phishing, dedicada a educar sobre los peligros de esta amenaza creciente. Durante esta semana, se llevarán a cabo simulaciones controladas de phishing, talleres sobre identificación y reporte de correos sospechosos, y competencias entre departamentos para fomentar la participación activa.

Por último, se instituirá el Día del Embajador de Ciberseguridad como un evento anual para reconocer y capacitar a los embajadores de ciberseguridad de la UCE. Este evento incluirá sesiones de formación avanzada, intercambio de mejores prácticas y la entrega de reconocimientos a los embajadores más efectivos.

La implementación coordinada de estas campañas, materiales y eventos tiene como objetivo crear una cultura de ciberseguridad robusta en la UCE, elevando la conciencia y las habilidades de toda la comunidad universitaria en materia de seguridad informática. Este enfoque integral busca no solo educar, sino también inspirar un compromiso activo con las prácticas de ciberseguridad en todos los niveles de la institución.

4.9 Procedimientos para el Manejo de Incidentes de Seguridad

Este diagrama representa el flujo de trabajo completo para el manejo de incidentes de seguridad en el CSIRT de la UCE. El proceso comienza con la detección o reporte de un incidente, que pasa por un triaje inicial donde se clasifica según su prioridad (alta, media o baja). Los incidentes de alta prioridad activan una notificación inmediata y respuesta del equipo CSIRT, mientras que los de media y baja prioridad siguen un proceso más estándar de análisis. Todos los incidentes, independientemente de su prioridad, pasan por fases de investigación, implementación de solución, documentación y generación de lecciones aprendidas, culminando en la actualización de políticas y procedimientos según sea necesario. El proceso es ejecutado por un equipo multidisciplinario que incluye al Coordinador CSIRT, Analistas de Seguridad, Especialistas Técnicos y el Equipo de Comunicaciones.

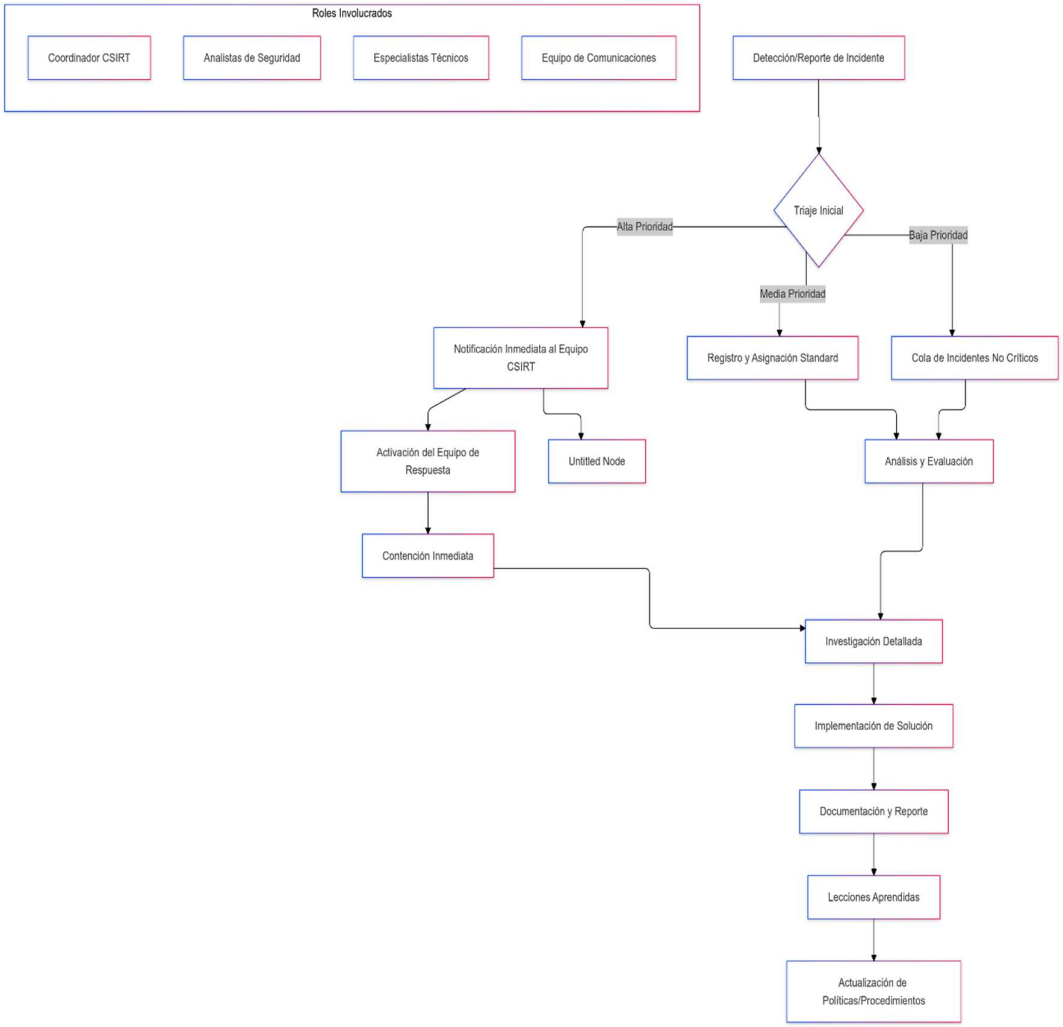


Ilustración 1 Flujo de trabajo completo para manejo de incidentes de seguridad

Los procedimientos de manejo de incidentes se dividen en las siguientes fases:

4.9.1 Detección y Reporte**:**

- El incidente puede ser detectado por herramientas automatizadas o reportado por usuarios.
- Los canales de reporte incluyen:
  - Mesa de ayuda del CSIRT
  - Correo electrónico dedicado
  - Portal web de reporte de incidentes
  - Línea telefónica de emergencia

4.9.2 Triaje Inicial:

- El Analista de Seguridad de turno evalúa la severidad del incidente según:
  - Impacto potencial
  - Cantidad de sistemas/usuarios afectados
  - Sensibilidad de los datos involucrados
  - Riesgo de propagación

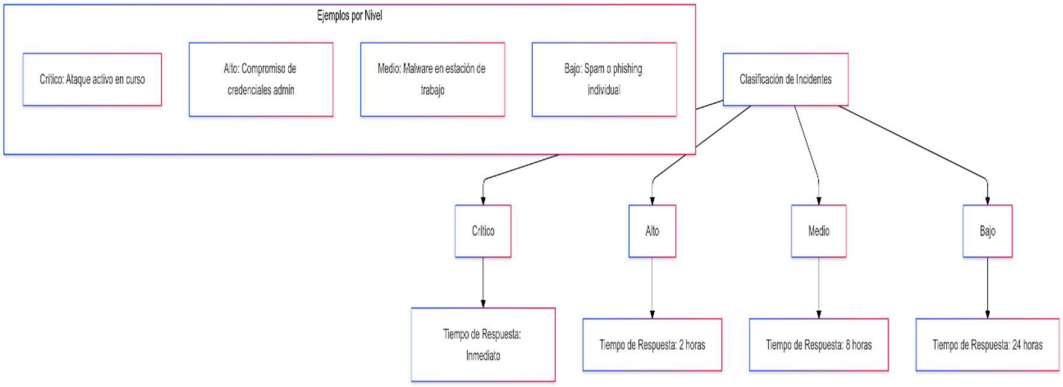


Ilustración 2 Severidad del incidente

Este diagrama ilustra el sistema de clasificación de incidentes de seguridad del CSIRT UCE y sus correspondientes tiempos de respuesta. Los incidentes se categorizan en cuatro niveles de severidad: crítico (respuesta inmediata) para casos como ataques activos en curso, alto (respuesta en 2 horas) para situaciones como compromiso de credenciales administrativas, medio (respuesta en 8 horas) para casos como infecciones de malware en estaciones de trabajo individuales, y bajo (respuesta en 24 horas) para incidentes menores como spam o intentos de phishing individuales. Esta clasificación permite priorizar eficientemente los recursos del CSIRT y asegurar que los incidentes más graves reciban atención inmediata mientras se mantiene un manejo ordenado de todos los casos.

4.9.3 Respuesta Inicial y Contención:

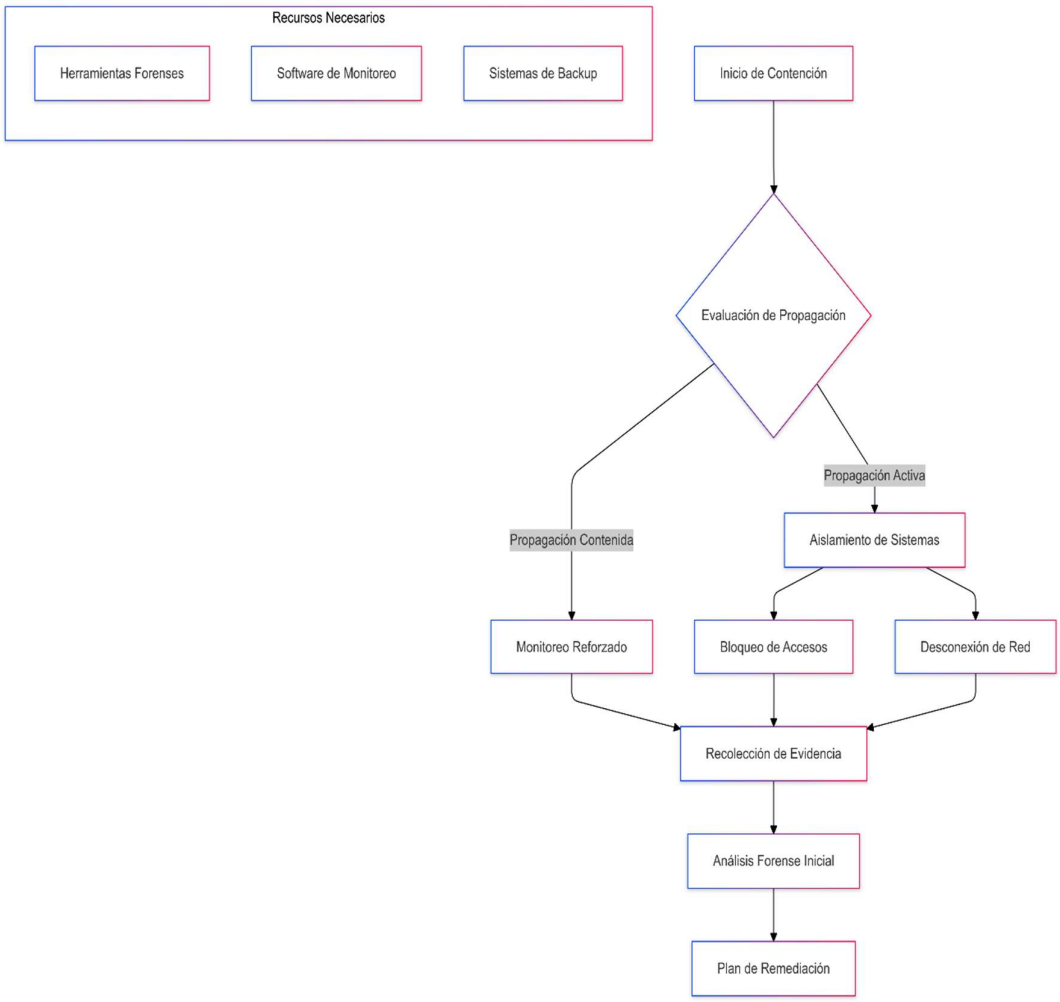


Ilustración 3 Proceso de contención de incidentes de seguridad

Este diagrama representa el proceso de contención de incidentes de seguridad del CSIRT UCE. El flujo comienza con una evaluación de propagación del incidente, que lleva a dos caminos posibles: si hay una propagación activa, se procede con medidas inmediatas como aislamiento de sistemas, bloqueo de accesos y desconexión de red; si la propagación está contenida, se pasa a un monitoreo reforzado. Ambos caminos convergen en la recolección de evidencia, seguida de un análisis forense inicial y el desarrollo de un plan de remediación. El proceso está respaldado por recursos esenciales como herramientas forenses, software de monitoreo y sistemas de backup, asegurando una respuesta efectiva y documentada ante el incidente.

4.9.4 Investigación y Erradicación:

- Equipo involucrado:
    - Analistas de Seguridad (2)

- Especialista Forense (1)
- Coordinador CSIRT

- Recursos tecnológicos utilizados:
  - Herramientas de análisis forense
  - Sistemas de monitoreo de red
  - Plataformas de análisis de malware

4.9.5 Recuperación y Restauración:

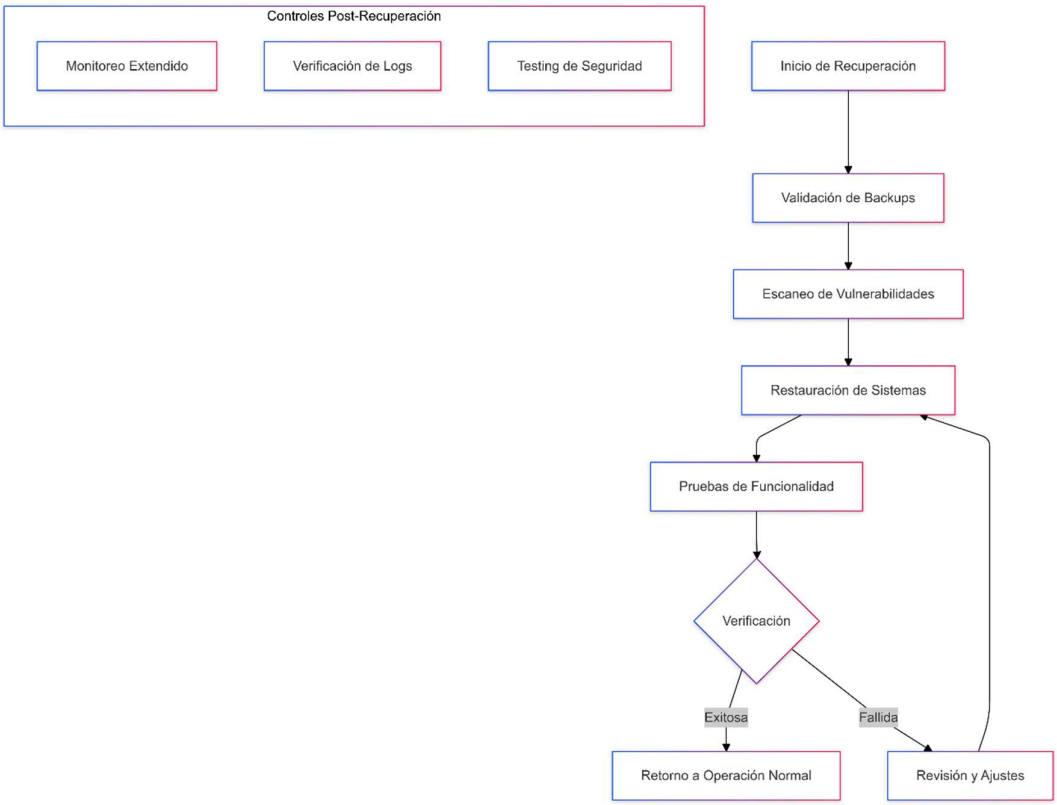


Ilustración 4 Proceso de recuperación de sistemas

Este diagrama ilustra el proceso de recuperación de sistemas después de un incidente de seguridad en el CSIRT UCE. El proceso comienza con la validación de copias de respaldo (backups), seguido de un escaneo de vulnerabilidades para asegurar que los sistemas estén limpios antes de su restauración. Después de restaurar los sistemas, se realizan pruebas de funcionalidad y una verificación final; si esta es exitosa, los sistemas retornan a operación normal, pero si falla, se inicia un ciclo de revisión y ajustes hasta lograr una restauración exitosa. Todo el proceso está respaldado por controles post-recuperación que incluyen monitoreo extendido, verificación continua de logs y pruebas de seguridad, asegurando así una recuperación completa y segura de los sistemas afectados.

4.9.6 Documentación y Cierre**:**

- Responsable: Coordinador CSIRT
- Elementos a documentar:

- Cronología del incidente
- Acciones tomadas
- Evidencia recolectada
- Impacto final
- Lecciones aprendidas

- Actualización de:
  - Base de conocimientos
  - Procedimientos de respuesta
  - Políticas de seguridad

4.9.7 Comunicación y Reportes**:**

- Equipo de comunicaciones gestiona:
  - Notificaciones internas
  - Comunicados a stakeholders
  - Reportes a autoridades (si aplica)
  - Actualizaciones de estado

4.9.8 Mejora Continua**:**

- Revisión trimestral de:
  - Efectividad de respuestas
  - Tiempos de resolución
  - Adecuación de recursos
  - Necesidades de capacitación

Estos procedimientos están diseñados para aprovechar los recursos del CSIRT propuesto y se alinean con las capacidades y estructura organizativa. La implementación efectiva requerirá capacitación continua del personal y actualizaciones periódicas basadas en la experiencia operativa.

4.10 Recursos Necesarios

4.10.1 Recursos Humanos:

Especialistas en Seguridad Informática: Contratar o capacitar a personal especializado en ciberseguridad, con conocimientos en detección y respuesta a incidentes.

Equipo de Respuesta a Incidentes: Formar un equipo dedicado de analistas de seguridad, investigadores de incidentes, ingenieros de seguridad y comunicadores de seguridad.

4.10.2 Detalle de Gastos para Presupuesto Operativo del CSIRT

4.10.2.1 Salarios

El costo total de salarios se basa en la propuesta de remuneración para el equipo de CSIRT, calculado anualmente.

Tabla 43 Estructura de Remuneración y Costos Anuales del Personal de Seguridad

Puesto	Nivel de Servidor Público	Remuneración Mensual ($)	Remuneración Anual ($)	Total Ingresos Anuales (incl. adicionales) ($)	Número de Empleados	Costo Total Anual ($)
Coordinador del CSIRT	Nivel 1	3,418.20	41,018.40	44,886.60	1	44,886.60
Analista de Seguridad	Nivel 3	1,212.00	14,544.00	16,206.00	1	16,206.00
Investigador de Seguridad	Nivel 3	1,412.00	16,944.00	18,806.00	1	18,806.00
Ingeniero de Seguridad	Nivel 3	1,676.00	20,112.00	22,238.00	1	22,238.00
Comunicador de Seguridad	Nivel 4	901.00	10,812.00	12,163.00	1	12,163.00
Docentes e Investigadores de Seguridad de la Información	Nivel 1	1,200.00	14,400.00	16,050.00	2	32,100.00

Total, Salarios Anuales: $146,399.60

4.10.2.2 **Capacitación**

La capacitación es esencial para mantener al equipo actualizado con las últimas tecnologías y prácticas de seguridad.

Tabla 44 Inversión en Capacitación y Desarrollo del Personal de Seguridad

Tipo de Capacitación	Costo por Empleado ($)	Número de Empleados	Costo Total ($)
Talleres y Seminarios	1,500	7	10,500
Certificaciones Profesionales (CISSP, CEH, etc.)	3,000	5	15,000

Total, Capacitación Anual: $25,500

4.10.2.3 **Licencias de Software**

Las licencias de software incluyen herramientas de seguridad, análisis de vulnerabilidades y otros programas necesarios para el funcionamiento CSIRT.

Tabla 45 Análisis de Costos Anuales de Software de Seguridad

Software	Costo Anual ($)
Herramientas de Análisis de Vulnerabilidades	10,000
Software de Gestión de Incidentes	8,000
Herramientas de Monitoreo de Seguridad	7,500
Licencias de Sistemas Operativos y Software de Soporte	5,000

Herramientas de Análisis Forense	6,000
Plataforma de Inteligencia de Amenazas	8,500

Total Licencias de Software Anual: $45,000

4.10.2.4 **Hardware**

Tabla 46 Costos Totales de Equipos de Seguridad y Monitoreo

Equipo	Cantidad	Costo Unitario	Costo Total
Servidores de Alta Capacidad	2	$8,000	$16,000
Estaciones de Trabajo Avanzadas	7	$2,500	$17,500
Dispositivos de Almacenamiento	2	$3,000	$6,000
Equipos de Respuesta a Incidentes	2	$4,000	$8,000

Total Hardware: $47,500

4.10.2.5 **Infraestructura de Red**

Tabla 47 Costos Totales de Equipos de Red y Protección de Intrusiones

Elemento	Cantidad	Costo Unitario	Costo Total
Firewall de Nueva Generación	2	$15,000	$30,000
Switches de Red	4	$2,000	$8,000
Sistema de Detección/Prevención de Intrusiones	1	$20,000	$20,000

Total Infraestructura de Red: $58,000

4.10.2.6 **Infraestructura Física**

Tabla 48 Resumen de Costos de Mobiliario y Espacio de Trabajo

Concepto	Costo Anual
Alquiler de Espacio de Oficina	$24,000
Remodelación y Adecuación	$15,000
Mobiliario y Equipamiento	$10,000

Total Infraestructura Física: $49,000

4.10.2.7 **Otros Gastos Operativos**

Otros gastos operativos incluyen costos administrativos, infraestructura y mantenimiento.

Tabla 49 Análisis de Costos Operativos y Servicios de Apoyo Anual

Descripción	Costo Anual ($)
Material de Oficina	2,000
Mantenimiento de Infraestructura	5,000
Servicios de Red y Comunicaciones	4,000

Costos Administrativos	3,000
Fondo de Respuesta a Incidentes	20,000
Membresías y Colaboraciones	5,000
Asesoría Legal y Cumplimiento	10,000

Total, Otros Gastos Operativos Anual: $49,000

4.10.2.8 Resumen del Presupuesto Operativo Anual

Tabla 50 Resumen de Costos Anuales por Categoría Operativa

Categoría	Costo Anual ($)
Salarios	146,399.60
Capacitación	25,500
Licencias de Software	30,500
Hardware	47,500
Infraestructura de Red	58,000
Infraestructura Física	49,000
Otros Gastos Operativos	49,000

Total, Presupuesto Operativo Anual: $420,399.60

Este detalle de gastos proporciona una visión integral del presupuesto necesario para cubrir los costos operativos del equipo de CSIRT, asegurando que se disponga de fondos suficientes para salarios, capacitación (excluyendo cursos en seguridad informática), licencias de software y otros gastos operativos esenciales.

4.10.3 Calendario detallado de eventos

Tabla 51 Calendario de Eventos para un CSIRT

Mes	Semana	Actividad
1	Semana 1-2	Evaluación inicial de la postura de seguridad de la UCE
	Semana 3	Desarrollo de políticas y procedimientos de seguridad
	Semana 4	Capacitación inicial del equipo CSIRT
2	Semana 1	Implementación de sistema de gestión de incidentes
	Semana 2-3	Campaña de concienciación sobre phishing y seguridad de contraseñas
	Semana 4	Evaluación de vulnerabilidades de la infraestructura de TI
3	Semana 1-2	Implementación de sistema de detección de intrusiones (IDS)
	Semana 3	Taller de seguridad para personal administrativo
	Semana 4	Simulacro de respuesta a incidentes
4	Semana 1	Revisión y actualización de políticas de control de acceso
	Semana 2-3	Implementación de autenticación de dos factores (2FA)
	Semana 4	Capacitación en análisis forense digital
5	Semana 1-2	Desarrollo de programa de embajadores de ciberseguridad
	Semana 3	Implementación de solución SIEM

	Semana 4	Evaluación de la efectividad de las campañas de concienciación
6	Semana 1-2	Hackathon de Ciberseguridad UCE
	Semana 3	Actualización de sistemas operativos y aplicaciones críticas
	Semana 4	Informe de progreso semestral y revisión de KPIs
7	Semana 1-2	Implementación de sistema de gestión de vulnerabilidades
	Semana 3	Taller de seguridad para docentes e investigadores
	Semana 4	Simulacro de respuesta a ransomware
8	Semana 1	Revisión y mejora de procesos de respuesta a incidentes
	Semana 2-3	Campaña de concienciación sobre seguridad en dispositivos móviles
	Semana 4	Auditoría de cumplimiento de políticas de seguridad
9	Semana 1-2	Implementación de sistema de prevención de pérdida de datos (DLP)
	Semana 3	Conferencia de Ciberseguridad UCE
	Semana 4	Evaluación de la madurez del CSIRT
10	Semana 1-2	Implementación de red segmentada para sistemas críticos
	Semana 3	Día del Embajador de Ciberseguridad
	Semana 4	Simulacro de incidente de fuga de datos
11	Semana 1-2	Implementación de sistema de gestión de accesos privilegiados
	Semana 3	Taller de desarrollo seguro para equipo de TI
	Semana 4	Revisión y actualización de plan de continuidad de negocio
12	Semana 1-2	Evaluación final de la postura de seguridad de la UCE
	Semana 3	Presentación de resultados anuales al Consejo Universitario
	Semana 4	Planificación estratégica para el siguiente año

Este calendario está diseñado para abordar las necesidades específicas identificadas en la Fase 2, incluyendo la implementación de nuevas tecnologías, mejora de procesos, capacitación continua y creación de una cultura de ciberseguridad en la UCE.

4.11 Evaluación de Riesgos Detallada para el CSIRT de la UCE

La implementación y operación de un CSIRT en la UCE puede implicar ciertos desafíos que es importante identificar, evaluar y gestionar de manera adecuada. Esta sección ofrece un análisis de posibles riesgos, incluyendo una matriz y estrategias recomendadas para su mitigación.

4.11.1 Metodología de Evaluación de Riesgos

La evaluación de riesgos se realiza utilizando la siguiente metodología:

1. Identificación de riesgos potenciales
2. Evaluación de la probabilidad de ocurrencia (1-5)
3. Evaluación del impacto potencial (1-5)
4. Cálculo del nivel de riesgo (Probabilidad x Impacto)
5. Desarrollo de estrategias de mitigación

4.11.2 Matriz de Riesgos

Tabla 52 Análisis de Riesgos y Estrategias de Mitigación para el CSIRT

ID	Riesgo	Probabilidad (1-5)	Impacto (1-5)	Nivel de Riesgo	Estrategias de Mitigación
R1	Falta de financiación adecuada	4	5	20 (Alto)	- Desarrollar un plan de financiación diversificado - Demostrar el ROI del CSIRT regularmente - Buscar patrocinios y subvenciones externas
R2	Escasez de personal calificado	3	4	12 (Medio)	- Implementar programas de capacitación interna - Colaborar con departamentos académicos para desarrollar talento - Ofrecer incentivos competitivos
R3	Resistencia al cambio organizacional	4	3	12 (Medio)	- Desarrollar un plan de gestión del cambio - Realizar campañas de concientización - Involucrar a stakeholders clave en la planificación
R4	Brechas de seguridad no detectadas	3	5	15 (Alto)	- Implementar sistemas de detección avanzados - Realizar auditorías de seguridad regulares - Establecer un programa de bug bounty
R5	Sobrecarga de incidentes	3	4	12 (Medio)	- Implementar sistemas de triaje eficientes - Establecer acuerdos de nivel de servicio (SLAs) claros - Desarrollar capacidades de

					respuesta automatizada
R6	Obsolescencia tecnológica	2	4	8 (Medio)	- Establecer un presupuesto para actualizaciones regulares - Adoptar tecnologías escalables y flexibles - Mantenerse informado sobre las tendencias tecnológicas
R7	Fuga de información confidencial	2	5	10 (Medio)	- Implementar políticas estrictas de manejo de datos - Utilizar tecnologías de encriptación avanzadas - Realizar capacitaciones regulares sobre seguridad de la información
R8	Conflictos con políticas universitarias existentes	3	3	9 (Medio)	- Realizar una revisión exhaustiva de las políticas existentes - Colaborar con la administración para alinear políticas - Desarrollar un marco de gobernanza claro
R9	Dependencia excesiva de proveedores externos	2	3	6 (Bajo)	- Diversificar proveedores - Desarrollar capacidades internas - Establecer acuerdos de nivel de servicio (SLAs) robustos
R10	Falta de adopción por parte de la comunidad universitaria	3	4	12 (Medio)	- Implementar programas de concientización efectivos

					- Demostrar el valor del CSIRT a través de casos de éxito - Integrar servicios del CSIRT en procesos universitarios clave

4.11.3 Estrategias de Mitigación Detalladas

4.11.3.1 R1: Falta de financiación adecuada

1. Desarrollar un plan de financiación diversificado:
    - Identificar múltiples fuentes de financiación (presupuesto universitario, subvenciones, servicios comerciales)
    - Establecer un comité de supervisión financiera para el CSIRT
    - Desarrollar propuestas de financiación detalladas y convincentes
2. Demostrar el ROI del CSIRT regularmente:
    - Implementar métricas claras de rendimiento y valor
    - Realizar análisis de costo-beneficio periódicos
    - Presentar informes regulares a la administración universitaria
3. Buscar patrocinios y subvenciones externas:
    - Identificar oportunidades de subvenciones gubernamentales y privadas
    - Establecer relaciones con empresas de tecnología para posibles patrocinios
    - Explorar colaboraciones de investigación que puedan atraer financiación

4.11.3.2 R2: Escasez de personal calificado

1. Implementar programas de capacitación interna:
    - Desarrollar un plan de estudios de ciberseguridad para el personal de TI existente
    - Ofrecer oportunidades de certificación y desarrollo profesional
    - Establecer un programa de mentores dentro del CSIRT
2. Colaborar con departamentos académicos:
    - Establecer programas de pasantías con los departamentos de informática y seguridad
    - Ofrecer proyectos de investigación en ciberseguridad para estudiantes de posgrado
    - Crear un programa de "residencia" en ciberseguridad para recién graduados
3. Ofrecer incentivos competitivos:
    - Desarrollar un paquete de compensación atractivo
    - Ofrecer flexibilidad laboral y oportunidades de teletrabajo
    - Proporcionar oportunidades de asistencia a conferencias y eventos de la industria

4.11.3.3 R3: Resistencia al cambio organizacional

1. Desarrollar un plan de gestión del cambio:

    - Identificar y abordar las preocupaciones específicas de diferentes grupos de stakeholders
    - Desarrollar un plan de comunicación claro y transparente
    - Implementar cambios de manera gradual y con retroalimentación continua
2. Realizar campañas de concientización:
    - Organizar sesiones informativas sobre la importancia de la ciberseguridad
    - Crear materiales educativos que expliquen el rol y beneficios del CSIRT
    - Utilizar múltiples canales de comunicación para llegar a toda la comunidad universitaria
3. Involucrar a stakeholders clave en la planificación:
    - Formar un comité asesor con representantes de diferentes departamentos
    - Realizar talleres de co-creación para el diseño de servicios del CSIRT
    - Establecer un sistema de retroalimentación continua

4.11.4 Conclusión

La identificación y mitigación proactiva de riesgos es crucial para el éxito a largo plazo del CSIRT de la UCE. Esta evaluación detallada proporciona una base sólida para la gestión de riesgos, pero debe ser revisada y actualizada regularmente para reflejar el entorno cambiante de ciberseguridad y las necesidades evolutivas de la universidad.

Se recomienda establecer un proceso de revisión trimestral de la matriz de riesgos, ajustando las estrategias de mitigación según sea necesario y monitoreando de cerca los riesgos de alto nivel. Además, es importante integrar la gestión de riesgos en todas las operaciones del CSIRT, fomentando una cultura de conciencia y responsabilidad en todo el equipo.

4.12 Fuentes de Financiación

Esta sección ofrece un análisis detallado y estratégico sobre las fuentes de financiación y la sostenibilidad a largo plazo del CSIRT, destacando las diversas opciones disponibles, como el presupuesto institucional, colaboraciones con la industria y subvenciones gubernamentales. Asimismo, se presentan estrategias clave para garantizar la viabilidad financiera continua del CSIRT, subrayando la importancia de demostrar constantemente su valor.

4.12.1 Presupuesto Institucional de la UCE

- **Descripción:** Asignación anual del presupuesto general de la universidad.
- **Estrategia:** Justificar la inversión en ciberseguridad como parte crítica de la infraestructura universitaria.
- **Desafíos:** Competencia con otras prioridades institucionales.
- **Potencial:** Fuente estable a largo plazo si se demuestra el valor continuamente.

4.12.2 1.2 Subvenciones Gubernamentales

- **Descripción:** Fondos del gobierno ecuatoriano destinados a mejorar la ciberseguridad en instituciones educativas.
- **Estrategia:** Desarrollar propuestas alineadas con las prioridades nacionales de ciberseguridad.
- **Desafíos:** Procesos de solicitud competitivos y requisitos de informes rigurosos.
- **Potencial:** Oportunidad para financiación inicial significativa y proyectos específicos.

4.12.3 1.3 Colaboraciones con la Industria

- **Descripción:** Asociaciones con empresas tecnológicas y de ciberseguridad.
- **Estrategia:** Ofrecer oportunidades de investigación, acceso a talento y pruebas de concepto.
- **Desafíos:** Equilibrar los intereses comerciales con los académicos.
- **Potencial:** Acceso a tecnología de punta y posibles donaciones de equipo.

4.12.4 1.4 Servicios de Consultoría

- **Descripción:** Ofrecer servicios de asesoría en ciberseguridad a otras instituciones o empresas.
- **Estrategia:** Aprovechar la experiencia desarrollada para generar ingresos adicionales.
- **Desafíos:** Asegurar que las actividades comerciales no interfieran con la misión principal.
- **Potencial:** Fuente de ingresos para reinvertir en el CSIRT y oportunidades de desarrollo profesional.

4.12.5 1.5 Programas de Formación Externa

- **Descripción:** Cursos de ciberseguridad ofrecidos al público general o a profesionales.
- **Estrategia:** Desarrollar programas de certificación y formación especializada.
- **Desafíos:** Competencia con otros proveedores de formación en ciberseguridad.
- **Potencial:** Fuente de ingresos recurrente y aumento de la reputación del CSIRT.

4.13 FASE 4: Validación del modelo propuesto

Evaluación de expertos

El modelo de CSIRT será sometido a una evaluación por expertos en ciberseguridad para asegurar que cumple con los estándares y mejores prácticas internacionales. Esto incluirá una revisión detallada de la estructura organizativa, los procesos y las tecnologías propuestas.

CAPÍTULO V

RECOMENDACIONES Y CONCLUSIONES

5.1 Resumen de los Resultados de la Investigación

La creación de un CSIRT en la UCE es un paso importante para fortalecer la ciberseguridad de la institución. Durante el proceso de investigación, se identificaron varias áreas clave que requerían atención para mejorar la capacidad de la UCE para detectar, prevenir y responder a incidentes de ciberseguridad. Los hallazgos más relevantes incluyen:

Se requiere CSIRT : la UCE se enfrenta a una serie de amenazas cibernéticas que podrían comprometer la integridad, la confidencialidad y la disponibilidad de sus datos. La creación del CSIRT hará que la respuesta a estos incidentes sea más estructurada y eficaz.

- Formación y sensibilización: la falta de sensibilización y formación en ciberseguridad entre los miembros de la comunidad universitaria fue una de las principales lagunas identificadas. Los programas de formación y las campañas de sensibilización son clave para mitigar este riesgo.
- Infraestructura tecnológica: Es necesario mejorar la infraestructura tecnológica actual de la UCE con herramientas y tecnologías adecuadas para gestionar los incidentes de seguridad.
- Políticas y procedimientos: debe desarrollar políticas y procedimientos de seguridad integrales y garantizar que se implementen de manera consistente en toda la Universidad.

5.2 Recomendaciones Para la Implementación

5.2.1 Estrategia de Mejora Continua

Para la efectividad y sostenibilidad del CSIRT , se recomiendan las siguientes estrategias:

- Desarrollo de Políticas de Seguridad: Crear y mantener una política de seguridad integral que cubra todas las áreas críticas de la infraestructura tecnológica de la UCE. Estas políticas deben revisarse y actualizarse periódicamente para reflejar las mejores prácticas y las amenazas emergentes.
- Implementar programas de capacitación: Desarrollar programas de capacitación continua en ciberseguridad para estudiantes, docentes y administradores. Estos planes deben incluir ejercicios de respuesta a incidentes y sesiones de capacitación práctica.

- Inversiones en tecnologías de seguridad: Adquirir y mantener herramientas y tecnologías de seguridad avanzadas, como sistemas de detección de intrusos, software de análisis forense y plataformas de gestión de incidentes.
- Monitoreo y evaluación continua: Establecer un sistema de monitoreo continuo para evaluar la efectividad de las políticas y procedimientos de seguridad. Realizar revisiones periódicas y adaptar las estrategias según sea necesario.

5.2.2 Sostenibilidad del CSIRT

La sostenibilidad del CSIRT dentro de la UCE es crucial:

- Apoyo institucional: asegurar el apoyo continuo de la alta dirección y autoridades universitarias. Esto incluye la asignación de los recursos financieros y humanos necesarios para el funcionamiento del CSIRT.
- Colaborar con otros CSIRT: establezca relaciones de colaboración con otros CSIRT y organizaciones de seguridad para compartir información y mejores prácticas.
- Investigación y Desarrollo: Promover la investigación y el desarrollo en el campo de la ciberseguridad involucrando a estudiantes y Docentes en proyectos de investigación y colaboraciones académicas.

5.3 Conclusión

El establecimiento del CSIRT es una medida importante para fortalecer la postura de seguridad de la red de la universidad. Un CSIRT bien estructurado y respaldado no sólo mejorará la capacidad de la UCE para gestionar incidentes de seguridad, sino que también promoverá una cultura de ciberseguridad entre todos los miembros de la comunidad universitaria.

5.3.1 Impacto de la Creación de un CSIRT

Establecer un CSIRT dentro de la UCE traerá varios beneficios importantes:

- Mejora de la respuesta a incidentes: el CSIRT podrá responder a incidentes de seguridad de forma más rápida y eficaz, minimizando su impacto y asegurando la continuidad de las operaciones de la Universidad.
- Aumentar la concienciación sobre la ciberseguridad: los programas de formación y sensibilización ayudarán a aumentar la concienciación sobre la ciberseguridad

entre estudiantes, Docentes y administradores, reduciendo así el riesgo de error humano.

- Fortalecimiento de la infraestructura de seguridad: Las inversiones en tecnologías y herramientas de seguridad fortalecerán la infraestructura tecnológica de la UCE y mejorarán su capacidad para detectar y mitigar amenazas.

5.4 Recomendaciones para futuras investigaciones

5.4.1 Extensiones al CSIRT

Los servicios de CSIRT incluyen seguridad móvil, privacidad y gestión de identidad.

- Desarrollo de nuevas tecnologías: Explorar nuevas tecnologías y métodos para mejorar la detección y respuesta a incidentes, como la inteligencia artificial y el aprendizaje automático.

5.4.2 Investigación Académica sobre Ciberseguridad

- Estudios de caso: Realizar estudios de caso de otras instituciones educativas que implementen CSIRT para identificar mejores prácticas y lecciones aprendidas.
- Evaluación de programas de capacitación: Utilizar métricas y metodologías rigurosas para evaluar la efectividad de los programas de capacitación y concientización en ciberseguridad.
- Análisis de amenazas emergentes: investigar amenazas emergentes en el mundo académico y desarrollar estrategias para mitigar esos riesgos de forma proactiva.

5.5 Referencias

- Antonucci, Y. L. (2017). _The basics of IT audit: Purposes, processes, and practical information_. John Wiley & Sons.

- CEFIPRA. (2020). _The CEFIPRA report on security in academic institutions_. [Online] Available at: https://www.cefipra.org/

- Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). _Computer Security Incident Handling Guide_ (NIST SP 800-61 Rev. 2). National Institute of Standards and Technology.

- Killcrece, G., Kossakowski, K. P., Ruefle, R., & Zajicek, M. (2003). _State of the Practice of Computer Security Incident Response Teams (CSIRTs)_. Carnegie

- ISO/IEC 27005:2018. (2018). _Information technology – Security techniques – Information security risk management_. International Organization for Standardization.

ANSI/ASIS RMSC.1-2015. (2015). Risk Management Standard for Information Security.

ANSI/ISO/IEC 27001:2013. (2013). Sistema de Gestión de la Seguridad de la Información (SGSI) - Requisitos.

ANSI/ISO/IEC 27002:2013. (2013). Controles para Sistemas de Gestión de la Seguridad de la Información.

FIRST. (2021). CSIRT Services Framework. Retrieved from https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

ISO/IEC 27001:2013. (2013). Information technology — Security techniques — Information security management systems — Requirements.

ISO/IEC 27002:2013. (2013). Information technology — Security techniques — Code of practice for information

- Villegas-Ch., W., Ortiz-Garces, I., & Sánchez-Viteri, S. (2021). Proposal for an Implementation Guide for a Computer Security Incident Response Team on a University Campus. *Computers*, 10(102). https://doi.org/10.3390/computers10080102

- Instituto Nacional de Ciberseguridad. (2023). Reporte de incidentes de seguridad informática.

- Organización de los Estados Americanos (OEA). (2023). Guía práctica para la creación de CSIRTs.

Asamblea Nacional del Ecuador. (2021). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459 de 26-may.-2021.

CSIRT CEDIA. (2021). Centro de Respuesta a Incidentes de Seguridad Informática. Recuperado de https://socsirt.cedia.edu.ec/

CSIRT EPN. (2021). Centro de Respuesta a Incidentes de Seguridad Informática. Recuperado de https://www.csirt-epn.edu.ec/

UTPL. (2023). *CSIRT UTPL and online education security*. Universidad Técnica Particular de Loja. https://www.utpl.edu.ec/csirt

Cambridge University. (2023). *Cambridge CSIRT overview*. Cambridge University. https://www.cambridge.edu/csirt

MIT. (2023). *MIT CSIRT services and structure*. Massachusetts Institute of Technology. https://www.mit.edu/csirt

University of Toronto. (2023). *University of Toronto CSIRT profile*. University of Toronto. https://www.utoronto.ca/csirt

University of São Paulo. (2023). *São Paulo CSIRT details*. University of São Paulo. https://www.usp.br/csirt

UNAM. (2023). *UNAM CSIRT and security services*. Universidad Nacional Autónoma de México. https://www.unam.mx/csirt

ENISA. (2016). CSIRT Setting Up Guide. Recuperado de https://www.enisa.europa.eu/publications/csirt-setting-up-guide

ISO/IEC 27005:2018. (2018). Information technology — Security techniques — Information security risk management.

Mowbray, T. (2013). Cybersecurity: Managing Systems, Conducting Testing, and Investigating Intrusions. Wiley.

Norma ISO/IEC 27001:2013 - Sistema de Gestión de la Seguridad de la Información (SGSI) - Requisitos.

Norma ISO/IEC 27002:2013 - Controles para Sistemas de Gestión de la Seguridad de la Información.

Segurilatam. (2023, abril 11). CERT y CSIRT: Algo más que un equipo para apagar el fuego. Segurilatam. https://www.segurilatam.com/tecnologias-y-servicios/ciberseguridad/cert-y-csirt-algo-mas-que-un-equipo-para-apagar-el-fuego_20230411.html

Anexo: Aprobación DTIC-UCE para el uso de la información.

UNIVERSIDAD CENTRAL DEL ECUADOR

La información es un activo de la Institución. Como activo, debe ser protegido, contra uso desautorizado o incorrecto.

La Universidad Central del Ecuador como norma de seguridad de la información, emite el siguiente Acuerdo de Confidencialidad para la utilización de la información emitida bajo solicitud del abajo firmante.

ACUERDO DE CONFIDENCIALIDAD

Yo, JORGE LUIS RIVERA GUAMAN, con identificación número 1104751415 acuerdo las siguientes condiciones a las que me someteré al obtener la información solicitada

Acuerdo:

1. Dar el buen uso de la información de la Universidad Central del Ecuador que recibo bajo mi pedido, y utilizarlo sólo para propósitos de cumplir con lo solicitado en la actividad: investigación con el fin de realizar la tesis de maestría con título: PROPUESTA DE CREACIÓN DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES INFORMÁTICOS (CSIRT) EN LA UNIVERSIDAD CENTRAL DEL ECUADOR.

2. Que la información es exclusivamente de la Universidad Central del Ecuador. Estoy consciente que cualquier divulgación no autorizada, es de mi total responsabilidad.

3. Que la Universidad Central del Ecuador podrá contrastar la información reutilizada, únicamente cuando falte a la verdad y se aleje de puntos objetivos.

4. Que este documento es importante para la protección de la información y que el contenido recibido es de manejo personal e intransferible.

5. Que no debo divulgar en ninguna circunstancia este acuerdo y manejarlo bajo criterios éticos y profesionales.

6. Que la omisión de los puntos anteriores puede conllevar a que la Universidad Central del Ecuador inicie un proceso legal en contra del responsable de la divulgación no autorizada de la información entregada.

Aceptación:

Para constancia de todos los puntos aquí expuestos firmo a continuación.

Atentamente

JORGE LUIS RIVERA GUAMAN

Nombre: Jorge Rivera

Cédula: 1104751415

Cargo: Asistente de Laboratorio Universitario

E-mail: jlriverag@uce.edu.ec

Lugar: Quito Fecha: 12/08/2024

www.uce.edu.ec