DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA:

"ESTRATEGIA Y DISEÑO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE"

AUTORES:

DE LA TORRE MOSCOSO, HUGO MARCELO
PARRA ROSERO, MARIO ANDRÉS

DIRECTOR:

ING. RON EGAS, MARIO BERNABÉ

SANGOLQUÍ

2018

CERTIFICADO

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

CERTIFICACIÓN

Certifico que el trabajo de titulación, "***ESTRATEGIA Y DISEÑO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE***" fue realizado por los señores ***De la Torre Moscoso, Hugo Marcelo y el señor Parra Rosero, Mario Andrés*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustenten públicamente.

Sangolquí, 09 de Agosto del 2018

Firma:

.....

Ing. Mario Bernabé Ron Egas Ms.C

C. C 1704229747

AUTORIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORÍA DE RESPONSABILIDAD

Nosotros, ***De la Torre Moscoso Hugo Marcelo y Parra Rosero Mario Andrés***, declaramos que el contenido, ideas y criterios del trabajo de titulación: "***ESTRATEGIA Y DISEÑO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE***" es de nuestra autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 09 de Agosto del 2018

Firmas:

.....	.....
Hugo Marcelo De la Torre Moscoso	**Mario Andrés Parra Rosero**
C. C 1719893057	C. C 1722068796

AUTORIZACION

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

AUTORIZACIÓN

Nosotros, ***De la Torre Moscoso Hugo Marcelo y Parra Rosero Mario Andrés*** *autorizamos a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación:* ***"ESTRATEGIA Y DISEÑO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA (CSIRT) ACADÉMICO PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE"*** *en el Repositorio Institucional, cuyo contenido, ideas y criterios son de nuestra responsabilidad.*

Sangolquí, 09 de Agosto del 2018

Firmas:

.....	.....
Hugo Marcelo De la Torre Moscoso	**Mario Andrés Parra Rosero**
C. C 1719893057	C. C 1722068796

DEDICATORIA

A mi familia que ha sido siempre el pilar de cada decisión y testigos de camino para poder desarrollarla, por la comprensión de mis padres en cada momento y los consejos para nunca dejarme vencer por las adversidades.

A mis amados hermanos que cado uno ha puesto un granito de arena para lograr llegar a esta meta tan anhelada por mi parte, ellos siempre han estado con diferentes gestos y hasta con una palabra de aliento.

A mis tías y tíos que han contribuido con su apoyo incondicional en diferentes situaciones que he afrontado durante mi carrera estudiantil.

Y a todas las personas que en su momento pasaron por mi vida y me apoyaron en cada una de mis decisiones y en este camino, por brindarme esa amistad verdadera.

Hugo De la Torre

A Dios, por darme vida y salud, por permitirme tener y disfrutar a mi hermosa familia, por guiarme en cada etapa de mi vida permitiéndome crecer y ser una persona de bien en todo aspecto posible.

A mis inigualables padres Amanda y Mario, por su formación, comprensión y apoyo incondicional en cada paso de mi vida, todo lo que soy es gracias a ellos.

A mis queridos hermanos Andrea y David, por estar siempre presentes y regalarme parte de su tiempo en los momentos bellos que hemos pasado.

A mis abuelitas, por sus sabios y largos consejos de vida, y a mis abuelitos, que sé que me acompañan, ya que siento su presencia en todo momento.

A Caro, por su compañía y apoyo fundamental hasta en la mínima cosa posible, y por tener tanta paciencia y amor para brindarme.

A mis demás familiares, que, a pesar de no verles seguido, disfruto de su compañía en cada momento compartido.

Mario Parra

AGRADECIMIENTO

Primeramente, agradezco a Dios por permitirme tener salud y vida para cosechar una meta más en mi vida, llegando a culminar con éxito una etapa más de la vida estudiantil, por darme cada día motivos para seguir luchando por mis metas y objetivos.

A mis padres Hugo y Elena por haber sacrificado muchas veces su tiempo y bienestar por verme seguir cosechando metas y objetivos, por ser esa mano de apoyo, y por haberme formado con valores y principios.

A mis hermanos porque cada uno de ellos me dio su apoyo incondicional en cada momento, me apoyaron y me brindaron su ayuda cuando más lo necesite, por nunca dejarme solo a pesar de las adversidades.

A mi compañero y amigo de Tesis Mario que, a pesar de adversidades, diferencias hicimos un buen equipo de trabajo para lograr desarrollar nuestro trabajo de titulación, por brindarme su amistad durante los años de estudio y durante el desarrollo del trabajo de titulación.

A mi Tuto de Tesis el Ing. Mario Ron por ser la guía, y el apoyo durante el desarrollo, quien nos brindó sus conocimientos para solventar nuestras dudas o desconocimiento de diferentes temas dentro del desarrollo.

A la Universidad de las Fuerzas Armadas ESPE por tener docentes con excelencia que ayudaron a mi formación como profesional, brindándome nuevos conocimientos y así haber logrado culminar y pertenecer a esta prestigiosa Universidad.

Hugo De la Torre

En primer lugar, agradezco a Dios por darme cada vez un día más de vida y permitirme llegar a este momento tan importante dentro de mi crecimiento profesional y pudiendo compartirlo con las personas que amo.

A mis padres Amanda y Mario, quienes con su amor y paciencia me han dado la mejor educación y lecciones de vida para alcanzar este bello momento, los amo.

A mis hermanos Andrea y David, que siempre están dispuestos a brindarme su ayuda y apoyo, los amo.

A mi novia Caro, que siempre está a mi lado en las buenas y malas, sin importar la situación que se presente, llenando mi vida de felicidad.

A Hugo mi compañero de tesis, mi amigo, que me ha brindado su amistad y me ha acompañado durante toda esta difícil etapa, que, a pesar de las adversidades, pudimos salir adelante.

A la Universidad de las Fuerzas Armadas ESPE, por permitirme formarme como profesional y ser parte de tan prestigiosa institución.

A mi director de tesis, Ing. Mario Ron, por brindarnos su conocimiento y la oportunidad para el desarrollo de nuestra investigación, guiándonos en cada paso hasta la culminación de la misma.

A mis docentes durante toda mi etapa universitaria, porque cada uno aportó en mi formación profesional.

Muchas Gracias a todos.

Mario Parra

ÍNDICE DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Con el constante desarrollo de las Tecnologías de la Información y Comunicación, las organizaciones se han vuelto dependientes de una conectividad digital para la provisión de sus servicios; conjuntamente las actividades maliciosas relacionadas a la tecnología han crecido exponencialmente provocando enormes gastos y pérdidas económicas a causa de las actividades de contención y resolución efectuadas. Actualmente, cuando ocurre un incidente de seguridad informática, la rápida y eficaz respuesta es primordial. Por tal razón entra en contexto el Equipo de Respuesta ante Incidentes de Seguridad Informáticas (CSIRT), un equipo de especialistas de seguridad de TI que dan respuesta a incidentes o amenazas de seguridad de la información, que poseen la capacidad para detectar y mitigar incidentes, vulnerabilidades y riesgos que podrían presentarse. La presente tesis plantea una propuesta para la creación de un CSIRT Académico en la Universidad de las Fuerzas Armadas ESPE que al momento no cuenta con un grupo que se encargue de emitir alertas o de dar un tratamiento adecuado de los incidentes de seguridad informática, es decir, no se tiene un área formalmente establecida en donde se pueda reportar estos incidentes y darles un seguimiento apropiado. Además, la propuesta se encuentra basada en una guía práctica de creación de CSIRTs Académicos y estándares relacionados mundialmente aceptados.

PALABRAS CLAVES

- **EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA - CSIRT**
- **CSIRT ACADÉMICO**
- **ESTÁNDAR ITIL V3**
- **PROYECTO DE CREACIÓN**

ABSTRACT

With the constant development of Information and Communication Technologies, organizations have become dependent on digital connectivity for the provision of their services; jointly the malicious activities related to technology have grown exponentially causing huge expenses and economic losses because of the containment and resolution activities carried out. Currently, when a computer security incident occurs, the quick and efficient response is essential. For this reason, the CSIRTs, a team of IT security specialists who respond to information security incidents or threats, who have the ability to detect and mitigate incidents, vulnerabilities and risks that may arise, come into context. These thesis proposes the creation of an Academic CSIRT at the Universidad de las Fuerzas Armadas ESPE that at the moment does not have a group that is in charge of issuing alerts or giving an adequate treatment to incidents of information security, that means, there is no formally established area where these incidents can be reported and given appropriate follow-up. In addition, the proposal is based on a practical guide for the creation of Academic CSIRTs and related standards worldwide accepted.

KEYWORD

- **COMPUTER SECURITY INCIDENT RESPONSE TEAM**
- **ACADEMIC CSIRT**
- **ITIL V3 FRAMEWORK**
- **CREATION PROJECT**

CAPÍTULO I
INTRODUCCIÓN

1.1 Antecedentes

Con la expansión de los servicios digitales, cada vez más organizaciones requieren de acceso permanente, así como también su infraestructura crítica depende de las posibilidades que tienen sus usuarios para acceder a internet (van der Heide, 2017). En consecuencia, los procesos y actividades fundamentales de las empresas para proporcionar sus servicios se han vuelto dependientes de su conectividad digital; una interrupción en ella puede provocar grandes pérdidas económicas. Las actividades maliciosas asociadas a la tecnología se han incrementado y son la principal causa de gastos realizados para su contención, resolución y prevención de daños potenciales, sin considerar el lucro cesante al interrumpir los servicios a los clientes. En la actualidad, cada vez que ocurre un incidente de seguridad en la información, la rápida y eficaz respuesta es clave. Por tal motivo entran en operación los CSIRT's, con su equipo de expertos de seguridad de TI que dan respuesta a incidentes o amenazas de seguridad de la información, que poseen el conocimiento y capacidad para detectar y manejar los incidentes, con el fin de ayudar a mitigar las vulnerabilidades y los riesgos que podrían presentarse.

Los ataques suceden y los atacantes por lo general son oportunistas, sin importar el tamaño de la organización o la importancia del negocio. Una vez realizado el ataque se debe reaccionar rápidamente para controlar el daño actual y evitar posibles daños futuros. Existen varios nombres con los que se dan a conocer los equipos de respuesta ante incidentes informáticos (Rajnovic, 2011), entre ellos están: CERT (Equipo Respuesta a Emergencias Informáticas), CIRT (Equipo de Respuesta a Incidentes Informáticos), IRT (Equipo de Respuesta a Incidentes), ERT (Equipo de Respuesta a Emergencias), CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática), SIRT (Equipo de Respuesta a Incidentes de Seguridad), SERT (Equipo de Respuesta a Emergencias de Seguridad).

De acuerdo con (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017) en varios países latinoamericanos se han implementado CSIRT Nacionales para dar atención a requerimientos de seguridad en organismos del estado. Sin embargo, no han proporcionado el resultado que se esperaba, en muchos casos por falta de formación técnica o recursos, lo que ha llevado a varias Universidades de la región a tomar conciencia de la no existencia de mecanismos adecuados que permitan proteger la información, especialmente de sus sistemas más críticos. En cada país de la región apenas una o dos Universidades han creado su CSIRT Académico de forma efectiva, propiciando el uso de las buenas prácticas de seguridad y la formación de un personal idóneo que fortalezca las unidades de seguridad de la información.

1.2 Problemática

La Universidad de las Fuerzas Armadas ESPE brinda diferentes servicios a los estudiantes y público en general en su mayor parte la Internet, procesos y operaciones que tienen un grado de importancia para el adecuado funcionamiento de la Universidad. Los avances tecnológicos y principalmente el crecimiento de la Internet han generado que la ESPE tenga cierto nivel de riesgo ante incidentes informáticos debido a un mal manejo de los recursos o por actividades externas maliciosas.

De acuerdo a la problemática actual de la Universidad no existe un grupo que se encargue de emitir alertas o de dar un tratamiento adecuado de los incidentes de seguridad informática, es decir no se tiene un área formalmente establecida en donde se pueda reportar estos incidentes y darles un seguimiento apropiado.

Ante estas situaciones resulta primordial la creación de un grupo de respuesta que cumpla actividades proactivas y reactivas que permitan estar preparados para una adecuada mitigación de los daños de un posible incidente informático que se pueda ocasionar, con el apoyo de reportes emitidos por CSIRTs Nacionales e investigaciones propias que contribuyan una mejora en la seguridad de los sistemas de información de la ESPE.

1.3 Justificación

Las Universidades en los países latinoamericanos, exceptuando Bolivia y Perú tienen CSIRTs Académicos, que brindan un tratamiento adecuado a los incidentes de seguridad informática que se presentan en sus Centros de Estudios de Educación Superior.

Existen varios factores que afectan la creación de CSIRT Académico (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017), los más importantes que se pueden mencionar son:

- La insuficiencia de recursos para realizar la implementación, es decir la falta de equipos, software y capacitación que obligarían a realizar una gran inversión por parte de las instituciones académicas.
- La carencia de políticas de seguridad y la falta de un Sistema de Gestión de la Seguridad de la Información definidas por las instituciones académicas de Educación Superior.
- La carencia de análisis financieros que justifiquen la implementación del CSIRT Académico, que generan dudas al decidir el apoyo inadecuado de las autoridades universitarias.

Dada la insuficiente formación/capacitación en seguridad informática y la brecha digital que actualmente tiene nuestro país, la implementación de un CSIRT Académico sería una ayuda para:

- Identificar vulnerabilidades en la infraestructura tecnológica.
- Mitigar el impacto de amenazas informáticas.
- Aplicar adecuadamente procedimientos reactivos y proactivos ante incidentes informáticos.

1.4 Objetivos

1.4.1 Objetivo General

Proponer un modelo de CSIRT Académico que permita operar un Equipo de Respuesta ante Incidentes Informáticos en la Universidad de las Fuerzas Armadas ESPE, utilizando como metodología base la propuesta de la “Guía Práctica para la creación de un Centro Académico de Respuesta ante Incidentes de Seguridad Informática (CSIRT Académico)” y estándares relacionados mundialmente aceptados.

1.4.2 Objetivos Específicos

- Estudiar la situación actual en materia de detección de vulnerabilidades de la Universidad de las Fuerzas Armadas - ESPE.
- Definir los requerimientos de la ESPE para la creación de un CSIRT académico.
- Especificar las políticas, procedimientos e infraestructura para el funcionamiento del CSIRT-ESPE.
- Elaborar el Proyecto de Creación del CSIRT Académico.

1.5 Alcance

La propuesta del modelo del CSIRT Académico para la Universidad de las Fuerzas Armadas ESPE cubre las 2 primeras fases de la metodología definida por (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017)

Fase I.- Planeamiento Estratégico.

- Conformación del equipo inicial de proyecto
- Definición del Plan inicial de trabajo
- Bitácora
- Estudio de la situación actual en la universidad
- Definición de la entidad patrocinadora

Fase II.- Diseño.

- Plan Estratégico del CSIRT.
- Plan Operativo Anual.
- Análisis y gestión de la demanda.
- Portafolio de Servicios.
- Relación con otros equipos.

- Políticas y Procedimientos.
- Modelo organizacional.
- Clasificación de puestos-especificaciones de clase.
- Infraestructura y equipamiento.
- Planes de seguridad, de recuperación de desastres y continuidad de servicios.
- Presupuesto y Financiamiento.
- Diseño y cronograma de implantación del proyecto.
- Definición de indicadores de evaluación de la implantación del proyecto.
- Elaborar el proyecto definitivo de creación del CSIRT.

CAPÍTULO II
MARCO TEÓRICO

2.1 Introducción

El propósito de este capítulo es presentar el marco teórico sobre el que se apoya proyecto de creación del CSIRT Académico para la Universidad de las Fuerzas Armadas ESPE. Inicialmente se detalla información acerca de los Equipos de Respuesta ante Incidentes de Seguridad Informática, los principales CSIRTs a nivel mundial, el estándar ITIL v3 sobre el que se basan las fases de estrategia y diseño, y por último los pasos de la metodología usada para la creación del CSIRT.

2.2 Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT)

2.2.1 Definición

Un CSIRT es un Equipo de Respuesta a Incidentes de Seguridad Informática. Está conformado por un grupo de expertos responsables de prevenir, identificar y responder a incidentes de seguridad de la información. El equipo de respuesta presta los servicios necesarios para mitigar los riesgos relacionados con ataques a los sistemas de información y brindar una respuesta rápida a los mismos, si estos se producen. En cierto modo, no solo se encargan de la gestión de incidentes (reforzar y proteger la seguridad, brindar respuestas efectivas), también de la elaboración de planes y estrategias para recuperación ante un incidente o vulnerabilidades detectadas (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017).

El acrónimo CSIRT tiene algunas variantes como:

Tabla 1
Acrónimos de CSIRT

Acrónimo	Nombre
CIRT	Cyber or Computer Incident Response Team
CERT	Cyber or Computer Emergency Response Team
CIRC	Cyber or Computer Incident Response Capability
CERC	Cyber o Computer Emergency Response Capability
SIRT	Security Incident Response Team
SERT	Security Emergency Response Team
SIRC	Security Incident Response Capability
SERC	Security Emergency Response Capability
IRT	Incident Response Team
ERT	Emergency Response Team
IRC	Incident Response Capability
ERC	Emergency Response Capability

Fuente: (Campbell, 2003)

Para (Campbell, 2003) los principales objetivos de un CSIRT son:

- Definir las políticas, procedimientos y servicios de respuesta a incidentes proporcionados.
- Manejar adecuadamente la capacidad de informar sobre los incidentes detectados.
- Manejar el incidente (Identificarlo, contenerlo y erradicarlo).
- Recuperarse del incidente (Determinar la causa, reparar el daño y restaurar el sistema).
- Investigar el incidente (Identificar la causa, recolectar evidencia y asignar la culpa).
- Ayudar en la prevención de una repetición del incidente.

2.2.2 Servicios de un CSIRT

Los CSIRTs ofrecen diferentes servicios que varían de acuerdo a la misión y tipo de la organización que lo va planificar e implementar, sin embargo, todos unifican como principal servicio la gestión de incidentes de seguridad informática. De acuerdo a (West-Brown, y otros, 2003) los servicios pueden agruparse en tres categorías:

- Servicios Reactivos.
- Servicios Proactivos
- Servicios de Gestión de Calidad de la Seguridad

La Tabla 2, detalla los servicios correspondientes a cada categoría:

Tabla 2
Servicios de un CSIRT

Servicios Reactivos	Servicios Proactivos	Servicios de Gestión de Calidad de la Seguridad
Alertas y Advertencias Manejo de Incidentes Análisis de incidentes Respuesta al incidente en el lugar. Soporte de Respuesta a incidentes. Coordinación de Respuesta a incidentes. Manejo de Vulnerabilidades Análisis de vulnerabilidades Respuesta a vulnerabilidades Coordinación de Respuestas a Vulnerabilidades. Manejo de Artifacts Análisis de Artifacts Respuesta a Artifacts Coordinación de la respuesta a Artifacts	Anuncios Observación de la tecnología Auditorías y evaluaciones de Seguridad. Configuración y Mantenimiento de las Herramientas, Aplicaciones, Infraestructuras y Servicios de Seguridad. Desarrollo de Herramientas de Seguridad. Servicios de Detección de Intrusión Divulgación de Información	Análisis de riesgo Planificación de continuidad del negocio y recuperación de desastres. Consultoría de Seguridad. Concientización. Educación / Capacitación. Evaluación y/o certificación de productos.

Fuente: (West-Brown, y otros, 2003)

2.2.2.1 Servicios Reactivos

Los servicios reactivos están planteados para dar respuesta, a solicitudes de asistencia, amenaza o ataque informático contra los sistemas de información, estos pueden ser causados por

terceras personas y son notificados mediante la visualización de registros o alertas de monitoreo o IDS (Intrusion Detection System). Los servicios reactivos se encuentran formados por:

Alertas y Advertencias

Consisten en comunicar información detallada de un nuevo ataque informático, vulnerabilidad de seguridad, aviso de intrusión o virus informático, proporcionando un camino de acción recomendado para dar solución al problema resultante en el menor tiempo posible.

La alerta, aviso o advertencia se genera como reacción al problema actual notificando a los involucrados de la actividad y proporcionando una pauta para la protección de sus sistemas de seguridad o para la recuperación de cualquier sistema afectado.

Manejo de Incidentes

Consiste en el análisis, clasificación y respuesta de los reportes recibidos sobre incidentes u eventos, incluyendo actividades de respuesta como:

- Toma de medidas de protección para los sistemas y redes afectados
- Determinación de soluciones y estrategias de mitigación a partir de advertencias o alertas relevantes.
- Búsqueda de actividades intrusivas en otras partes de la red.
- Realiza un filtro de todo el tráfico que ingresa por la red.
- Desarrollar otras soluciones alternativas.

Como complemento del manejo de incidentes se pueden utilizar otros subprocesos que se detallan a continuación:

- **Análisis de Incidentes. -** Consiste en analizar toda la información disponible de un incidente u evento, buscando identificar su alcance, la extensión del daño, su naturaleza y las estrategias o soluciones disponibles para su respuesta.
- **Respuesta a Incidentes in situ. -** Consiste en proporcionar una asistencia directa en el lugar que residen los sistemas afectados, realizando un análisis físico para su pronta reparación y recuperación. Evitando únicamente soportes de respuesta mediante correo electrónico o llamadas telefónicas.

- **Soporte a la Respuesta a Incidentes. -** Consiste en proporcionar una guía remota para que el personal del lugar del sistema afectado pueda realizar la recuperación sin involucrar acciones directas en sitio como se describió anteriormente.
- **Coordinación de la Respuesta a Incidentes. -** Consiste en coordinar los esfuerzos de respuesta de todas las partes involucradas en el incidente u evento, reuniendo información del contacto, estadísticas acerca de la cantidad de sitios involucrados y coordinando con otros CSIRT para intercambiar información de utilidad

Manejo de Vulnerabilidades

Implica obtener información acerca de reportes e informes sobre vulnerabilidades de hardware y software, mediante el análisis de su naturaleza, la mecánica y los efectos, desarrollando estrategias de respuesta para detectar y reparar las vulnerabilidades.

Como complemento del manejo de vulnerabilidades se pueden utilizar otros subprocesos que se detallan a continuación:

- **Análisis de las Vulnerabilidades. -** Consiste en localizar las vulnerabilidades y su posible explotación, realizando evaluación y auditoría técnica en el hardware y software para disminuir las probabilidades de un nuevo ataque informático. Incluye simulaciones en ambientes de prueba obteniendo puntos estratégicos donde se puede mejorar la seguridad.
- **Respuesta a las Vulnerabilidades. -** Consiste en tener a punto una respuesta efectiva para mitigar o reparar una vulnerabilidad determinada, para ello los miembros del equipo deben realizar una investigación o desarrollo de correcciones, parches o soluciones temporales.
- **Coordinación de Respuesta a Vulnerabilidades. -** Comprende la notificación de la vulnerabilidad encontrada en diversas partes de la empresa, compartiendo información sobre cómo solucionar o mitigar la vulnerabilidad mediante una estrategia de respuesta, esto puede implicar comunicación con proveedores, otros CSIRT, expertos o miembros que descubrieron o informaron la vulnerabilidad.

Manejo de Artifact

Un artifact es un archivo u objeto hallado en un sistema que podría estar involucrado en un ataque de sistemas y redes o que se está utilizando para imponerse a medidas de seguridad.

El manejo de artifacts implica obtener información de artifacts utilizados en ataques informáticos pasados y otras actividades no autorizadas, procediendo al análisis de su naturaleza, su mecánica, versión, entre otros puntos, para desarrollar estrategias de respuesta en defensa y detección de estos hechos.

Como complemento del manejo de artifacts se pueden utilizar otros subprocesos que se detallan a continuación:

- **Análisis de Artifact. -** Se realiza un examen técnico de cualquier artifact encontrado en el sistema y se lo compara con artifacts existentes o nuevos con la finalidad de comprobar las funciones que realiza.
- **Respuesta a Artifact. -** Implica fijar las acciones convenientes para una correcta detección y eliminación de artifacts de un sistema, así como las acciones para evitar la instalación de los mencionados.
- **Coordinación de Respuesta a Artifact. -** Comprende compartir los resultados de los análisis y las estrategias de respuesta para un artifact determinado con otros expertos en seguridad, CSIRT e investigadores.

2.2.2.2 Servicios Proactivos

Los servicios proactivos intentan evitar incidentes y reducir su impacto y alcance si llegan a ocurrir, mejorando la infraestructura y los procesos de seguridad de la organización. Los servicios proactivos se encuentran formados por:

- **Anuncios. -** Comprenden alertas de intrusión, advertencias de vulnerabilidad y avisos de seguridad, para informar a otros grupos acerca de nuevas vulnerabilidades, ataques y herramientas de intrusión detectadas, permitiéndoles proteger sus sistemas y redes antes de que puedan ser explotados.

- **Observatorio de Tecnología. -** El equipo está siempre investigando sobre nuevos métodos de ataque y tendencias relacionadas en la identificación de futuras amenazas, mediante información de sitios web, artículos, noticias y también estableciendo comunicación con otras partes que sean autoridades en estos campos, dando como resultado directrices o recomendaciones a largo plazo.
- **Evaluaciones o Auditorías de la Seguridad. -** Proporciona una revisión minuciosa de la infraestructura de seguridad de la organización, conjuntamente con las prácticas de seguridad establecidas actualmente, para realizarla se necesita la aprobación de la alta dirección puesto que la evaluación se realiza a nivel de seguridad lógica y física.
- **Configuración y Mantenimiento de las Herramientas, Aplicaciones, Infraestructuras y Servicios de Seguridad. -** Consiste en la definición de una guía para una correcta configuración de las herramientas y aplicaciones que se usan en el CSIRT, pudiendo tener acceso a las configuraciones de clientes externos o miembros de la organización.
- **Desarrollo de Herramientas de Seguridad. -** Comprende el desarrollo de herramientas de software que el grupo o el CSIRT necesiten o deseen. Estas pueden incluir desde el desarrollo de parches de seguridad para un software personalizado, hasta scripts (lenguaje de programación que ejecuta diversas funciones en el interior de un programa de computador) para mejorar la funcionalidad de herramientas existentes.
- **Servicios de Detección de Intrusiones. -** Consiste en la revisión de los registros de los IDS existentes, para identificar eventos o intentos de ataques informáticos, luego proceden a la aplicación de estrategias para una correcta eliminación y minimización de los mismos, por lo que algunas organizaciones externalizan esta actividad a otros profesionales en el área.
- **Difusión de Información Relacionada con la Seguridad. -** Consiste en la difusión de información útil en la organización para mejorar la seguridad, esta información puede ser desarrollada y publicada por el CSIRT o por otra parte de la organización (TI, Recursos Humanos) y puede incluir:
    - Documentos de alertas, advertencias y otros anuncios.
    - Archivos de mejores prácticas.
    - Orientación en seguridad informática.
    - Estadísticas actuales y tendencias de incidentes.

2.2.2.3 Servicios de Gestión de Calidad de la Seguridad

Los servicios que entran en esta categoría son diseñados y establecidos para mejorar la seguridad general de la organización, mediante retroalimentaciones y evaluaciones de experiencias adquiridas en la prestación de servicios reactivos y proactivos.

Los servicios mencionados pueden beneficiar a las cualidades de seguridad mencionadas a continuación:

- **Análisis de Riesgo. -** Consiste en mejorar la capacidad de la organización en el análisis y evaluaciones de los riesgos, optimizando la habilidad de la organización para asegurarse contra amenazas reales. Los CSIRT mediante este servicio ayudan en el perfeccionamiento de actividades de análisis de riesgo de la seguridad de la información para nuevos sistemas y procesos comerciales.
- **Planificación de la Continuidad del Negocio y Recuperación de Desastres. -**Con base en las ocurrencias pasadas y predicciones futuras de incidentes o tendencias de seguridad se deben realizar esfuerzos de planificación para determinar la mejor manera de responder a tales incidentes garantizando la continuidad de las operaciones comerciales.
- **Consultoría de Seguridad. -** Los miembros del equipo CSIRT pueden proporcionar asesoramiento y orientación a la organización sobre la implementación de mejores prácticas de seguridad, estas recomendaciones entran en el campo de seguridad de la información, desarrollo de políticas de seguridad o instalación de equipos y aplicaciones.
- **Concientización. -** Comprende la búsqueda de oportunidades para generar conciencia de seguridad en todos quienes conforman la organización, no solo orientándolos en el cumplimiento de prácticas de seguridad, sino en la comprensión de los problemas de seguridad que pueden generarse en las operaciones diarias de cada uno. Estas actividades de concientización pueden ser reuniones, seminarios, boletines, carteles, sitios web u otros más.
- **Educación / Capacitación. -** De una forma similar al tema anterior de concientización, busca proveer de información acerca de actividades principales de la seguridad de la información a los miembros de la organización, mediante talleres, cursos o tutoriales que transmitan pautas para responder ante un incidente.

- **Evaluación o Certificación de Productos. -** Mediante una evaluación o un programa de certificación el CSIRT puede realizar evaluaciones de productos y otros servicios destinados a garantizar la seguridad.

2.2.3 Tipos de CSIRT

En la actualidad existen diferentes CSIRT según su público objetivo, pertenecientes a distintos sectores de la sociedad y de organizaciones. Para el (Centro Criptológico Nacional (CCN Cert) y TB-Security, 2011) los diferentes ámbitos en los que se ha implementado equipos CSIRT son:

2.2.3.1 CSIRT para las Pymes

Por el tamaño que mantienen estas empresas, es poco viable que de forma individual estas empresas implementen las funcionen de un CSIRT. Por lo tanto, este tipo de equipos de respuesta buscan agrupar pequeñas organizaciones que mantengan características similares para ofrecerles el servicio.

2.2.3.2 CSIRT Académico

Estos centros optan por tener su responsabilidad en entidades académicas conformadas por estudiantes y personal de universidades o colegios. La dimensión de la comunidad estipulará los servicios a ofrecer, el modo que lo van hacer y el grado de intervención directa en el campo.

2.2.3.3 CSIRT Comercial

Prestan servicios a cambio de una remuneración económica a clientes profesionales del sector comercial, normalmente utilizan acuerdos de servicios específicos con cada cliente de su comunidad.

2.2.3.4 CSIRT Militar

Prestan servicios a instituciones militares con responsabilidades de infraestructuras de TI con fines de defensa. Su comunidad está determinada por organizaciones militares y entidades estrechamente relacionadas.

2.2.3.5 CSIRT Gubernamental

En este tipo de equipos se encuentran aquellos CSIRT cuyo objetivo es proteger la infraestructura de TI de un gobierno u estado y los servicios que son ofrecidos a su población. Generalmente la comunidad a la que se encuentran dirigidos son las administraciones públicas y sus organismos. Estos equipos pueden combinarse con CSIRT Nacionales o funcionar de manera independiente. Estos CSIRT habitualmente están patrocinados por instituciones del estado.

2.2.3.6 CSIRT Nacional

Estos tipos de CSIRT son fundamentales como punto de contacto para todo un país, puesto que tienen coordinación y responsabilidad sobre todos los sectores del mismo. En muchos casos estos equipos atienden a la comunidad CSIRT de su país y asumen la responsabilidad de coordinación de otros CSIRT en el ámbito nacional.

2.2.3.7 CSIRT de Protección de Infraestructuras Críticas

Pueden ser considerados CSIRT del sector interno, puesto que se centran principalmente en el resguardo de las infraestructuras críticas de la información, por ejemplo, Sistemas financieros, Organizaciones de telecomunicaciones, Centrales de energía, Sector sanitario, Instalaciones de investigación, alimentación, agua, transporte, entre otras).

2.2.3.8 CSIRT de Proveedor

Su objetivo central son los productos o servicios que ofrece un proveedor, eliminando o reduciendo el impacto negativo de las vulnerabilidades de los mencionados, ya sea un producto tecnológico o servicio de TI.

2.2.4 Beneficios de un CSIRT

Los beneficios obtenidos con la existencia de un CSIRT pueden categorizarse en 3 áreas según (Campbell, 2003):

Económicos

- Reduce la cantidad de personal y el tiempo requerido para manejar un incidente, es decir disminuyen la cantidad de pérdida de productividad de los trabajadores afectados por el incidente, ya que, con menos tiempo perdido, los costos en controlar el incidente son menores.
- Acorta los costos de operación con la centralización de conocimiento altamente especializado en un solo lugar, mejorando la calidad de gestión técnica de seguridad, como auditorías o forensias.

De Relaciones Públicas

- Minimiza un potencial de exposición negativo de la organización, es decir una noticia de incidentes que dañe la reputación de la misma. Con la existencia del equipo de respuesta se demuestra que la organización tiene una alta responsabilidad en el manejo de incidentes.
- Aumenta el conocimiento de la comunidad en contenidos técnicos necesarios para prevenir situaciones de riesgo, mejorando el grado de sensibilización de los usuarios.

Legales

- En algunos casos puede convertirse en una necesidad para cumplir con regulaciones gubernamentales.
- Ofrece un punto cualificado para gestionar y coordinar los aspectos normativos y jurídicos asociados a los incidentes, en el cual la protección de las evidencias digitales es mejor.

2.2.5 Personal que conforma un CSIRT

2.2.5.1 Capacidad

Actualmente no existe una cifra fija sobre la cantidad de personal técnico necesario para conformar el equipo CSIRT, puesto que cada CSIRT es distinto, funciona en un ambiente diferente y tiene un tamaño diferente.

Sin embargo, con la experiencia colectiva de la comunidad CSIRT, los valores presentados a continuación por (van der Heide, 2017) resultan ser una buena aproximación:

- Para entregar 2 servicios básicos de respuesta de incidentes y anuncios: un mínimo de 4 trabajadores a tiempo completo o semejantes.
- Para un CSIRT completo funcionando en horario de oficina y mantenimiento de sus propios sistemas: entre 6 y 8 trabajadores a tiempo completo o semejantes.
- Para un CSIRT operando con personal completo de 7x24 (24 horas al día, 7 días a la semana): un mínimo de 12 trabajadores a tiempo completo o semejantes.

2.2.5.2 Competencias

Dependiendo de los servicios que se vayan a entregar, se requerirán habilidades más especializadas por parte del personal técnico, las competencias básicas clave que deben poseer los expertos del CSIRT se pueden clasificar en:

Competencias Personales

- Buen espíritu de equipo.
- Altas habilidades analíticas.
- Fluida explicación de cuestiones técnicas difíciles.
- Sentimiento de confidencialidad para la información.
- Buena organización.
- Alta comunicación y escritura.
- Capacidad de aprendizaje y de mente abierta.

Competencias Técnicas

- Conocimiento en diferentes tecnologías y protocolos de internet.
- Conocimiento de sistemas operativos.
- Conocimiento de infraestructura de red.
- Conocimiento de aplicaciones de internet.
- Conocimiento de amenazas de seguridad.
- Conocimiento de análisis y respuesta a riesgos.

Competencias Adicionales

- Alta disponibilidad.

- Buen nivel de educación.
- Experiencia en el campo de TI.

2.2.5.3 Estructura Organizativa

La estructura organizativa para los miembros del CSIRT dependen primordialmente de la estructura de la organización a la cual va ofrecer sus servicios, y de la posibilidad de contratar expertos externos para cubrir funciones específicas. Para (Bronk, Thorbruegge, & Hakkaja, 2006) un equipo CSIRT típico estaría determinado por los siguientes cargos:

General

- Director general

Personal

- Director de oficina
- Asesor Contable
- Asesor de Comunicaciones
- Asesor jurídico

Equipo técnico

- Líder de equipo
- Técnicos expertos
- Investigadores

Personal externo

- Trabajadores externos

Posteriormente es fundamental definir el modelo organizativo para el CSIRT, (Bronk, Thorbruegge, & Hakkaja, 2006) exponen los siguientes modelos:

Modelo de Empresa Independiente

Este modelo se refiere a un CSIRT ampliado que actúa como una organización independiente, haciendo uso de sus propios directivos y empleados.

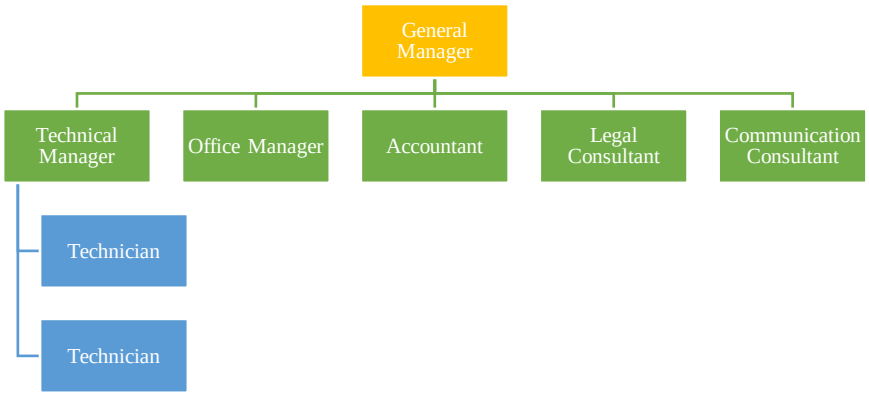

Figura 1. Modelo de Empresa Independiente
Fuente: (Bronk, Thorbruegge, & Hakkaja, 2006)

Modelo Incrustado

Este modelo es utilizado para la creación de un CSIRT dentro de una organización que tiene un departamento de TI existente, además este modelo tiene la posibilidad de adaptarse a situaciones especiales que vayan surgiendo con el tiempo por su número fijo de trabajadores asignados a las diferentes funciones.

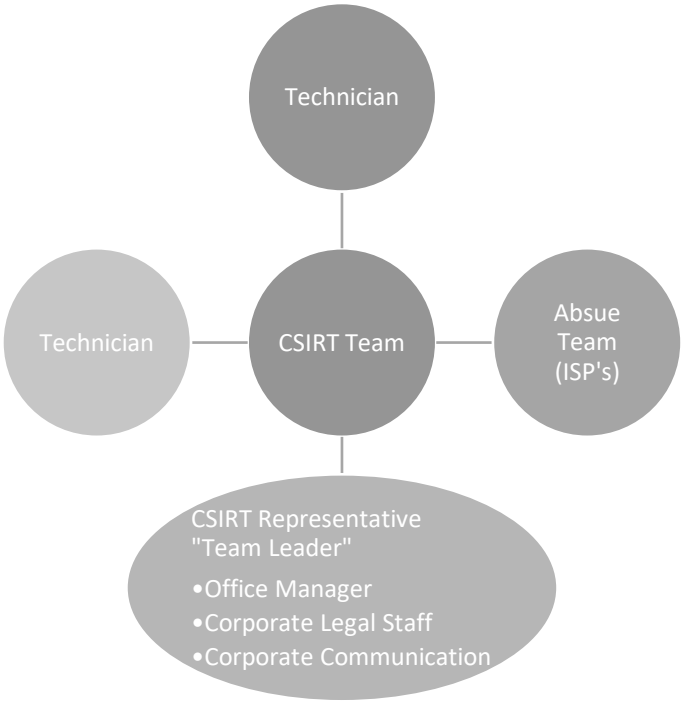

Figura 2. Modelo Incrustado
Fuente: (Bronk, Thorbruegge, & Hakkaja, 2006)

Modelo Universitario

Este modelo es adoptado principalmente por las instituciones académicas para la creación de un CSIRT Académico y de Investigación. Muchas de estas instituciones manejan un CSIRT independiente en sus respectivos campus y un CSIRT central en su matriz, siendo el CSIRT central el punto de contacto con el mundo exterior, es decir pueden compartir servicios con otras universidades y sus respectivos CSIRT para disminuir gastos.

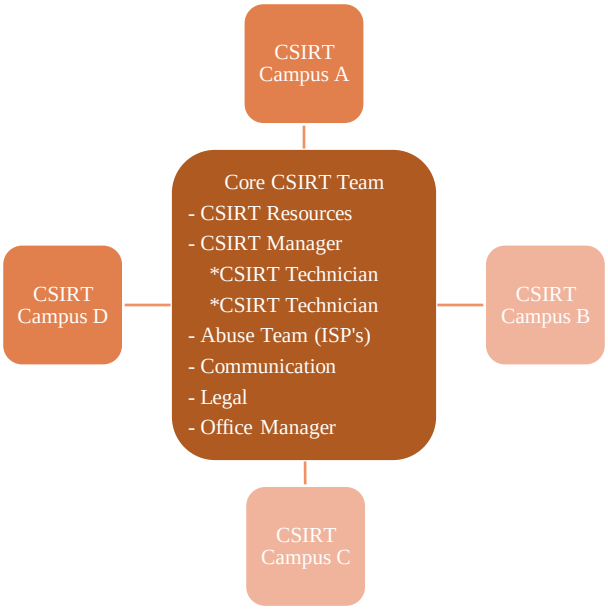

Figura 3. Modelo Universitario
Fuente: (Bronk, Thorbruegge, & Hakkaja, 2006)

Modelo Voluntario

Este modelo está determinado por un grupo de expertos que se reúnen para asesorarse y apoyarse mutuamente de una forma voluntaria, dependiendo únicamente de la motivación de los participantes.

2.2.5.4 Código de conducta, ética y práctica

Es muy importante que los miembros del CSIRT tengan en cuenta un conjunto de reglas o pautas para mantener un comportamiento profesional adecuado dentro y fuera el trabajo. Generalmente un CSIRT tarda alrededor de un año para generar confianza en su entorno, y si no

se hace una buena detección de empleados, se puede perder esta confianza de la noche a la mañana. Por lo cual, un buen ejemplo es el CSIRT Code of Practice from Trusted Introducer.[1]

2.2.5.5 Formación

Un plan de capacitación para el personal del CSIRT puede incluir: una capacitación interna para que los nuevos miembros entiendan el funcionamiento del CSIRT y una capacitación externa para mejorar las habilidades técnicas del equipo y mantenerse actualizados de los avances tecnológicos.

Existen diferentes opciones para una encontrar una capacitación externa de alta calidad para el personal del CSIRT en:

- TRANSIST[2]
- CERT/CC[3]
- SANS[4]
- FIRST[5]

2.2.6 Modelo Organizacional de un CSIRT

Al momento de implementar un Equipo de Repuesta a Incidentes de Seguridad (CSIRT) se debe tomar en cuenta que existen diferentes modelos organizacionales, los cuales no se deben pasar por alto, más bien, deben ser tomados en cuenta para poder decidir cuál de los modelos existentes se va a implementar y a desarrollar para una determinada área de aplicación. (Killcrece, 2003).

2.2.6.1 Equipo de Seguridad

Un equipo de seguridad se puede implementar en entidades pequeñas o que tengan necesidades específicas, como de seguridad, teniendo en cuenta una necesidad centrada en la administración más que nada. Estas organizaciones lo que primero hacen es implantar o tener

[1] Trusted Introducer CSIRT Code of Practice : <https://www.trusted-introducer.org/TI-CCoP.pdf>
[2] TRANSIST: <https://www.terena.org/activities/transits/>
[3] CERT/CC <https://www.sei.cmu.edu/education-outreach/courses/index.cfm>
[4] SANS: <https://www.sans.org/>
[5] FIRST: <https://www.first.org/>

equipos con componentes de infraestructura como puede ser firewalls, redes privadas (VPN), sistemas de detección de intrusos (IDS).

2.2.6.2 Modelo Distribuido.

En este modelo se tiene un equipo compuesto de personas de varias divisiones, grupos o sectores de la misma empresa. Los cuales se rigen a un gerente que es la cabeza principal de cada uno de los grupos, donde los gerentes son los que interactúan centralmente. En este modelo se rige ya a la existencia de políticas, procedimientos y procesos de manejo de incidentes más formalizados, un método establecido de comunicación con toda la organización u empresa sobre las amenazas de seguridad y estrategias de respuesta, y finalmente un gerente de CSIRT designado y miembros del equipo encargados o asignados tareas de manejo más específico de incidentes.

2.2.6.3 Modelo Centralizado

En este modelo se tiene un equipo centralizado donde se encuentran asignadas las tareas y sus responsabilidades para cada uno, y así poder manejar las incidencias en toda la organización. La parte vital o importante de este modelo es la facilidad para agrupar sintetizar y diseminar información en toda la empresa. El CSIRT tiene una respuesta óptima para informar actividades fuera de lo común, realiza o tiene la capacidad de participar en análisis de incidentes y vulnerabilidades.

Tiene la autoridad de analizar toda actividad y tener una respuesta al incidente que se haya reportado. Este tipo de decisiones o acciones deben ser aprobadas por el gerente del CSIRT para poder ser ejecutadas. El equipo tiene carta abierta para tomar decisiones sobre aplicar estrategias de recuperación y mitigación de incidentes, pero siempre y cuando dichos procesos hayan sido autorizados o previamente aprobados por la gerencia.

- **Servicios Básicos**

Tabla 3
Servicios Básicos del Modelo Centralizado

Alertas y Advertencias.	Se las valora según la importancia y la gravedad en la que afectan, después de su valoración se las envía a las unidades dentro de la organización para ser atendidas.
Análisis de Incidentes	Al tener un modelo centralizado se consigue identificar dificultades en el análisis.
Soporte en Respuesta de Incidentes	Es responsable de enviar información técnica y guías sobre como tomar decisiones o efectuar procedimientos para recuperarse ante el incidente de seguridad.
Coordinación de Respuestas a Vulnerabilidades y "Artifacs"	Concentra la recopilación de información y distribuye las guías para detectar y recuperarse ante un incidente.
Anuncios	Se mantiene al día las actualizaciones de las diferentes tecnologías. Además se recibe, clasifica y prioriza los anuncios sobre la seguridad y la distribución de información importante para la organización

Fuente: (Killcrece, 2003)

- **Servicios Adicionales**

Tabla 4
Servicios Adicionales Modelo Centralizado

Respuesta en Sitio	Análisis de vulnerabilidades y "artifacts"
Auditorias o Valoraciones de Seguridad	Configuración y mantenimiento de herramientas de seguridad, aplicaciones e infraestructuras
Desarrollo de Herramientas de Seguridad	Servicios de detección de intrusiones (IDS)

Fuente: (Carozo, Martinez, & Vidal, 2008)

2.2.6.4 Modelo Combinado

La manera de operar de este modelo es central, que tiene una interacción con los miembros de cada área distribuidos por la organización. Realiza un análisis de alto nivel y realiza

recomendaciones estratégicas de recuperación y mitigación. Centraliza la recolección de información y ayuda a organizar y despertar las aptitudes dentro de la organización.

2.2.6.5 Modelo Coordinador

Este modelo se centra en un CSIRT que principalmente se encarga en coordinar y facilitar actividades de la parte de gestión de incidentes y vulnerabilidades en la parte externa de una comunidad amplia y diversa. Hay varios modelos de un CSIRT coordinadores y cada uno contiene niveles diferentes de autoridad en su comunidad objetivo.

- Primer Tipo: Servir a un grupo de la comunidad objetivo, tener la autoridad para implementar soluciones de respuesta a incidentes y mitigación.
- Segundo Tipo: Servir a un distrito compuesto por varias fuerzas armadas de un país. Teniendo esta autoridad sobre los miembros de este distrito.
- Tercer Tipo: Servir a todo un país, provincia o ciudad, su autoridad es mínima al no tener control sobre la zona a la que está siendo aplicada.

2.2.7 CSIRT del Sector Académico

Un CSIRT Académico brinda servicios a la institución educativa que pertenecen, ofreciendo servicios relacionados a seguridad informática a toda la comunidad que está relacionada con la institución. Este CSIRT no solo dá servicios sino también tiene la facilidad de crear ambientes investigativos, elaborativos para prácticas de seguridad para el bienestar de él y de la comunidad.

Ahora bien, se debe tomar en cuenta que existen varios factores que van a afectar la creación de un CSIRT Académico. (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017) detallan los siguientes:

- No exista el apoyo necesario por parte de las autoridades de la institución.
- Déficit de personas capacitadas, o formadas para poder llevar a cabo un proyecto de esta dimensión.
- Presupuesto insuficiente para el desarrollo e implementación del mismo.
- Falta de políticas a nivel nacional e institucional para la ciberseguridad o protección de datos.

- Procesos de creación y autorización de ejecución de proyectos muy largos o laboriosos.

Al proteger los sistemas de información que posee una organización siempre se encuentran dificultades, todo esto tiene trascendencia por la rapidez con la que la tecnología evoluciona en el cibercrimen. El cibercrimen se ha visto afectado por las siguientes situaciones:

- Actualmente el robo de información de cualquier tipo tiene un afán de lucro, las personas que se dedican a realizar este tipo de robo son recompensados económicamente, este robo de información puede ser toda la información de tarjetas de crédito, robo de identidad y otros.
- Se ha logrado ver con el paso del tiempo un crecimiento del hacking político/social, generando desconfianza hacia la comunidad a la cual pertenece el CSIRT.
- APT (Amenazas persistentes avanzadas). Se debe evitar que grupos criminales, o de gobierno tenga la facilidad de conseguir información clasificada que se encuentra en los sistemas informáticos y que estén altamente relacionados con entidades gubernamentales.
- Ataques comunes más complejos, estos se dan por la facilidad de ejecución que tienen, y no se necesita tener una preparación profesional para poder ejecutarlos.
- Los sistemas de información de la organización o institución tienen conexiones con entes privados y públicos, esto recae en que ya no es una protección de datos individual o mejor dicho propia, sino más bien uno debe proteger la información o los sistemas de toda su red, generando que en cada dominio de seguridad existan responsables.

2.3 Equipos CSIRT a nivel mundial

2.3.1 FIRST

Organización principal y líder mundial encargada de obtener respuesta a incidentes. Reúne varios equipos de respuesta a incidentes de seguridad de instituciones de gobierno, comerciales y educativas. Fomenta la cooperación y coordinación entre organizaciones a nivel mundial, logrando obtener intercambio de información sobre cómo prevenir y mitigar incidentes informáticos.

2.3.2 Equipos CSIRT en América

Figura 4. CSIRTs en América
Fuente: (Banco Interamericano de Desarrollo (BID) & Organización de los Estados Americanos, 2016)

En América la organización encargada es la OEA (Organización de Estados Americanos) dicha organización tiene como objetivo lograr que los estados que conforman esta organización estén en paz, tenga un orden, una justicia, fomentar la parte solidaria y tener colaboración entre los mismos.

En el 2003 se crea y se aprueba una resolución AG/Res. 1939 (XXXIII-O/03), la cual tiene la facilidad o potestad de crear y desarrollar estrategias interamericanas para poder minimizar, combatir y mitigar amenazas de ataques cibernéticos. El (FIRST, 2018) detalla los CSIRT a nivel americano:

- EEUU: existen actualmente 86 equipos de respuesta ante incidentes entre los cuales podemos mencionar.
    - Amazon Security Incident Response Team
    - CERT Coordination Center
    - Duke University and Duke Health
    - eBay Global Information Security Monitoring and Response Team
    - XEROX CSIRT
- Canadá: tiene 11 equipos especializados
    - Above Security Computer Emergency Response Team
    - Bell Canada Information Security Response / CIRT
    - BMO InfoSec Incident Response Team
    - Herjavec Computer Incident Response Team
    - Research In Motion, Corporate Security - Information Security Operations Centre
- México: actualmente cuenta con 4 equipos
    - Centro Especializado en Respuesta Tecnológica de México
    - Scitum Cyber Security Incident Response Team
    - UNAM-CERT
- Guatemala:
    - Cyber Seguridad S.A.

- Colombia:
    - COMPUTER SECURITY INCIDENT RESPONSE TEAM OF OLIMPIA MANAGEMENT S.A
    - Response Team Computer Security Incident of the Colombian National Police
    - Security Operations Center - Cyber Operations Command Joint
- Ecuador:
    - Centro de respuesta a Incidentes informáticos de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia
    - Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones
- Perú:
    - JACKSECURITY INCIDENT RESPONSE TEAM
    - SecureSoftCorp-Computer Security Incident Response Team
    - TERIS Telefonica Security Incidents Response Team
    - CLARO PERU Security Incident Response Team
- Brasil:
    - Axur CSIRT
    - Brazilian Academic and Research Network CSIRT
    - Computer Emergency Response Team Brazil
    - Computer Security Incident Response Team of ARCON
- Chile:
    - Chilean Computer Emergency Response Team
    - Neosecure S.A.
- Argentina:

- Centro de Ciberseguridad del Gobierno de la Ciudad Autónoma de Buenos Aires
- Banelco Computer Security Incident Response Team
- ICIC-CERT

- Uruguay:

  - Centro Nacional de Respuesta de Incidentes de Seguridad Informática
  - Computer and Telecommunications Security Incident Response Centre

2.3.3 Equipos CSIRT en Europa

En Europa en cambio se encuentra el Task Force – Collaboration of incident Response Teams (TF-CSIRT). Esta organización permite que se intercambie información de experiencias y de conocimiento en un entorno, para la cooperación entre las mismas. Desarrolla y proporciona servicios para CSIRTs, usando estándares y procesos de manejo de incidentes de seguridad.

2.3.4 Equipos CSIRT en Asia

Según el (Asia Pacific Computer Emergency Response Team, 2018) Asia mantiene un comité llamado APCERT, su objetivo es mantener una red con confianza de expertos con conocimientos en seguridad informática en el continente asiático. Aspectos en los que trabaja el comité:

- Tener una cooperación regional e internacional de Asia y Pacífico en la parte de seguridad de la información.
- Tomar medidas y desarrollar procesos para poder tratar y mitigar incidentes de seguridad en redes regionales o de gran tamaño.
- El intercambio de información y tecnología sea intuitivo y fácil entre los organismos. (seguridad, virus, códigos maliciosos.)
- Crear una Red de ayuda entre CERT y CSIRTs a nivel regional para la respuesta de una emergencia informática eficiente y efectiva.

2.4 ITIL V.3

ITIL es definido como un marco de referencia que documenta buenas prácticas para una correcta gestión de los servicios de TI en una organización. La librería de ITIL se encuentra conformada por los siguientes componentes:

- **Núcleo de ITIL**.- Consta de 5 publicaciones que sirven de guía de mejores prácticas aplicables a todos los tipos de organizaciones que brindan servicios.
- **Guía complementaria de ITIL**.- Es un conjunto complementario de publicaciones con orientación específica para sectores industriales, tipos de organización, modelos operativos y distintas arquitecturas tecnológicas.

La propuesta del CSIRT Académico para la Universidad de las Fuerzas Armadas se encuentra apoyada en las 3 primeras fases del ciclo de vida del núcleo de ITIL:

- Estrategia del Servicio.
- Diseño del Servicio.
- Transición del Servicio.

2.4.1 Estrategia del Servicio

"La estrategia de servicio proporciona orientación sobre cómo diseñar, desarrollar e implementar la gestión del servicio no solo como una capacidad de organización sino también como un activo estratégico" (OGC, 2011).

Esta fase tiene como finalidad, definir los servicios que serán entregados a los usuarios de la organización, gestionándolos de manera que puedan convertirse en un activo que entregue valor. Los procesos asociados directamente a la fase de estrategia del servicio son:

2.4.1.1 Gestión Financiera

La Gestión financiera ofrece al negocio y a TI la cuantificación en términos financieros, del valor de los servicios de TI y del valor de los activos, brindando información sobre el coste real de los servicios. Las organizaciones de TI incorporan cada vez más esta gestión buscando:

- Una toma de decisiones mejorada.
- Cambios más rápidos.
- Gestión de la cartera de servicios.
- Control y conformidad financiera.
- Control operacional.
- Creación y capturación de valor.

Además, la Gestión Financiera genera datos de rendimiento crítico utilizados para responder algunas preguntas importantes para una organización, las cuales no resultarían sencillas de responder instintivamente con información defectuosa o limitada. Algunas de las preguntas mencionadas se detallan a continuación:

- ¿Nuestra estrategia de diferenciación se traduce en mayores ganancias o ingresos, menores costos o una mayor adopción de servicios?
- ¿Qué servicios nos cuestan más y por qué?
- ¿Cuáles son nuestros volúmenes y tipos de servicios consumidos?
- ¿Cuán eficientes son nuestros modelos de provisión de servicios en relación con las alternativas?
- ¿Nuestro enfoque estratégico para el diseño del servicio da como resultado servicios que pueden ofrecerse a un "precio de mercado" competitivo, reducir sustancialmente el riesgo u ofrecer un valor superior?
- ¿Dónde están nuestras mayores ineficiencias de servicio?
- ¿Qué áreas funcionales representan las oportunidades de mayor prioridad para que nos concentremos en la generación de una estrategia de mejora continua del servicio?

Las responsabilidades y actividades de la Gestión Financiera de TI no existen únicamente dentro del dominio de contabilidad y finanzas de TI. Por el contrario, muchas partes de la empresa interactúan para generar y consumir información financiera de TI, operaciones, gestión de proyectos, desarrollo de aplicaciones, infraestructura, gestión de cambios, entre otras. Los datos de la Gestión Financiera utilizados por una organización de TI pueden residir en el dominio contable y financiero, y ser propiedad del mismo, pero la responsabilidad de generarlo y utilizarlo se extiende a otras áreas.

2.4.1.2 Gestión del Portfolio de Servicios

El portfolio de servicios representa los servicios de un proveedor en términos de valor comercial. Enuncia las necesidades comerciales y la respuesta del proveedor a esas necesidades. Por definición, los términos de valor comercial corresponden a los términos de comercialización, proporcionando un medio para comparar la competitividad del servicio entre proveedores alternativos.

Esta gestión puede actuar como la base de un marco de decisión, aclarando o ayudando a aclarar las siguientes preguntas estratégicas:

- ¿Por qué debería un cliente comprar estos servicios?
- ¿Por qué deberían comprarnos estos servicios?
- ¿Cuáles son los precios o los modelos de contra cargo?
- ¿Cuáles son nuestras fortalezas y debilidades, prioridades y riesgos?
- ¿Cómo deben asignarse nuestros recursos y capacidades?

2.4.1.3 Gestión de la Demanda

La Gestión de la Demanda es crítica para realizar una correcta gestión del servicio, ya que si se encuentra mal gestionada puede ocasionar un riesgo a los proveedores de los servicios debido a la incertidumbre en la demanda. Además, puede darse la situación de un exceso de capacidad, la cual generará costos que no crean valor y proporcionen una base para recuperar los costos, en la cual los clientes se comportan reacios en pagar por una capacidad inactiva.

Hay instancias en que una capacidad no utilizada puede ofrecer un mejor nivel de servicio y no sería considerada capacidad inactiva, y en otras se tiene una capacidad insuficiente que genera un impacto en la calidad de los servicios prestados y limita el crecimiento del servicio.

Un punto importante a considerar, es que el consumo genera demanda y la producción es consumida por la demanda, ambas se encuentran sincronizadas, puesto que los servicios no deben ser creados por adelantado y mantenerse almacenados en un inventario anticipándose a la demanda.

Generalmente, cuando un servicio funciona mejor, genera una mayor demanda, provocando exigencias de capacidad en los responsables, los cuales resuelven el inconveniente incrementando los activos del servicio, generando un ciclo de consumo – producción como el que se muestra a continuación:

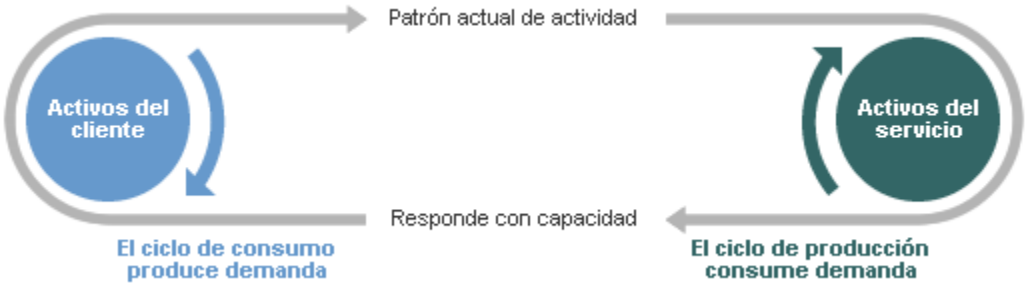

Figura 5. Actividad empresarial y los patrones de demanda de servicios
Fuente: (Quiñonez, 2015)

El objetivo principal de la Gestión de la Demanda es la optimización y racionalización de los recursos de TI, tomando protagonismo cuando existen problemas de capacidad en la infraestructura de TI. Estos problemas se pueden encontrar en:

- Degradación del servicio por aumentos no esperados en la demanda.
- Interrupciones en el servicio.
- Incremento de costes por un exceso de capacidad, tratando de compensar los picos de demanda.

2.4.2 Diseño del Servicio

"El diseño del servicio proporciona orientación para el diseño y desarrollo de los servicios y procesos de gestión de servicios. Cubre los principios de diseño y métodos para convertir objetivos estratégicos en carteras de servicios y servicios activos" (OGC, 2007).

Esta fase tiene como finalidad, diseñar los nuevos servicios que se van incorporar al catálogo de servicios de la organización, permitiendo una correcta definición de los requerimientos y necesidades del cliente. También permite especificar si se cuenta con los recursos y capacidades para entregar los servicios de una manera adecuada. Además, puede revisar los servicios existentes para una futura mejor de acuerdo a las necesidades empresariales.

Los procesos asociados directamente a la fase de diseño del servicio son:

2.4.2.1 Gestión del Catálogo de Servicio

El catálogo de servicios realiza una función similar al portfolio de servicios que se analizó anteriormente, pero realiza su función de cara al exterior. La razón principal de dos documentos similares se debe a que el portfolio de servicios tiene información interna, acerca del funcionamiento de la organización, la cual no es de interés para los clientes, y además, se encuentra en un lenguaje muy técnico que no resulta adecuado.

Otra diferencia reside en los servicios incluidos en cada uno de ellos, en el portfolio se encuentran todos los servicios prestados, se prestaron y se prestarán, mientras que el catálogo de servicios excluye aquellos que se encuentran retirados o inactivos, y se enfoca únicamente en los que pueden ser de interés para los clientes. Aunque resulte complejo elaborar este documento, por su alineación con los aspectos técnicos con las políticas de negocio, es imprescindible su elaboración porque:

- Es una guía para la selección de un servicio por parte de los clientes.
- Demarca las funciones y compromisos de TI.
- En algunos casos se lo utiliza como herramienta para ventas.
- Ayuda evitando malos entendidos entre los actores que prestan los servicios.

El objetivo principal de la Gestión del Catálogo de Servicio es compilar la información de todos los servicios que los clientes deben conocer para tener asegurar un entendimiento entre ellos y la organización de TI.

Las funciones que debe cumplir el Catálogo de Servicio son:

- Evitar el lenguaje técnico para una comprensión total de los servicios por personal no especializado.
- Orientar a los clientes.
- Describir los Acuerdos de niveles de servicio.
- Reconocer los clientes de los servicios actuales.

Algunos de los beneficios que ofrece la creación y mantenimiento del Catálogo de Servicio son:

- Ganancia de fluidez y solidez en la relación entre la organización y el cliente.
- Evitar malos entendidos al poner por escrito los acuerdos alcanzados.
- Evitar situaciones de vacío de poder al poner por escrito los responsables de cada servicio.

Pueden existir algunas dificultades en relación al Catálogo de Servicios como:

- La falta de claridad de los servicios que han sido retirados.
- El Catálogo de Servicios revela funcionamiento de la organización que no es de interés para el cliente.
- El Catálogo de Servicios no se encuentra actualizado y en la práctica es infructífero.

2.4.2.2 Gestión de Niveles de Servicio

La Gestión de Niveles de Servicio está encargado de definir, negociar y supervisar la calidad de los servicios de TI ofrecidos. El objetivo de la Gestión de Niveles de Servicio es poner a disposición del servicio del cliente la tecnología. Además, debe asegurarse que la calidad de los servicios de TI se encuentre alineados a la tecnología y los procesos de negocio.

Resulta fundamental cumplir con los siguientes objetivos para una correcta Gestión de Niveles de Servicio:

- Conocer los requerimientos del cliente.
- Describir correctamente los servicios ofrecidos.
- Monitorizar la calidad de los servicios comparándolos con los objetivos fijados en los SLAs.

Las funciones que debe cumplir la Gestión de Niveles de Servicios son:

- Exponer los servicios de una manera entendible al cliente.
- Documentar los servicios de TI.
- Fijar como prioridad el cliente y su negocio.
- Comunicarse con el cliente para proponer servicios de TI adecuados, acorde a las necesidades del cliente.
- Determinar indicadores de rendimiento de TI.
- Monitorizar la calidad de los servicios de TI para una posible mejora.
- Elaborar Planes de mejora para los servicios y la calidad que brindan.

Algunos de los beneficios que ofrece Gestión de Niveles de Servicio son:

- Los servicios de TI cumplen las expectativas y necesidades de los clientes.
- Facilita una buena comunicación con los clientes.
- Determina objetivos entendibles y cuantificables.
- Los clientes están al tanto de la calidad de los servicios ofrecidos, y se crean protocolos de acción en casos de desperfecto en los servicios.
- Facilita buenos acuerdos con proveedores y contratistas.
- El centro de servicios almacena documentación de: SLAs, OLAs para llevar una buena relación con el cliente.
- Los SLAs benefician al cliente para que conozca la razón del coste de sus servicios.

Pueden existir algunas dificultades en la implementación de la Gestión de Niveles de Servicio como:

- Falta de comunicación con los clientes, obteniendo SLAs que no cubren los requerimientos solicitados.
- SLAs basados más en deseos y expectativas del cliente que en servicios ofrecidos por la infraestructura de TI.
- Mala alineación de los servicios de TI con el proceso de negocio del cliente.
- No se utilizan los recursos necesarios para los servicios por decisión de la dirección.
- No se monitoriza adecuadamente el cumplimiento de los SLAs.
- La organización no tiene un compromiso en la calidad de los servicios de TI establecidos.

2.4.2.3 Gestión de la Capacidad

La Gestión de la Capacidad se encarga de asegurar que todos los servicios de TI se encuentren respaldados por la suficiente capacidad de proceso y almacenamiento.

Cuando no se aprovechan de una manera adecuada los recursos, se puede provocar inversiones con gastos adicionales innecesarios, o darse el caso de una insuficiencia de recursos que provocaría una disminución de la calidad del servicio.

Las funciones que debe cumplir la Gestión de la Capacidad son:

- Verificar que se cubren los requerimientos de capacidad TI tanto presentes como futuros.
- Controlar el rendimiento de la infraestructura TI.
- Desplegar planes de capacidad incorporados a los niveles de servicio acordados.
- Gestionar y normalizar la demanda de servicios TI.

El objetivo de la Gestión de la Capacidad es proveer de los recursos informáticos necesarios a los clientes, usuarios y personal del departamento de TI para que cumplan sus tareas.

Es necesario que esta gestión considere los siguientes puntos:

- Verificar el estado actual de la tecnología.
- Verificar planes de negocio y SLAs.
- Evaluar el rendimiento de la infraestructura.

- Desarrollar pruebas de capacidad en varios escenarios.
- Dimensionar los servicios acordes a los procesos de negocio.
- Racionalizar el uso de los servicios.

Algunos de los beneficios que ofrece Gestión de la Capacidad son:

- Optimizar el rendimiento de los recursos informáticos.
- Permite tener la capacidad necesaria en el momento adecuado.
- Ayuda a evitar gastos innecesarios.
- Permite planificar un crecimiento de la infraestructura alineado a las necesidades del negocio.
- Ayuda en la reducción de incompatibilidades y fallos en la infraestructura.

Pueden existir algunas dificultades en la implementación de la Gestión de la Capacidad como:

- Una incompleta información para una planificación adecuada.
- Expectativas injustificadas.
- Creación de infraestructuras muy complejas con un acceso complicado.
- Falta de compromiso por parte de la dirección.
- La constante evolución de la tecnología obliga a revisiones periódicas.
- Una mala planificación provocaría costos innecesarios.

2.4.2.4 Gestión de la Disponibilidad

La Gestión de la Disponibilidad se encarga de la optimización y monitorización de los servicios de TI, para que tengan un funcionamiento fiable e ininterrumpido, de manera que cumplan los SLAs establecidos y tengan un costo razonable.

El objetivo de la Gestión de la Disponibilidad es asegurar la disponibilidad y un correcto funcionamiento de los servicios de TI para el uso de los clientes y usuarios cada vez que los requieran.

Las funciones que debe cumplir la Gestión de la Disponibilidad son:

- Definir los requerimientos de disponibilidad en base a reuniones con los clientes.
- Garantizar un buen nivel de disponibilidad de los servicios.
- Monitorizar que los sistemas de TI se encuentren disponibles.
- Aumentar los niveles de disponibilidad mediante propuestas de mejoras en la infraestructura y servicios.
- Verificar el cumplimiento de los OLAs y UCs que se mantienen con proveedores internos y externos.

Existen ciertos indicadores que permiten validar un correcto proceso de Gestión de la Disponibilidad como: Fiabilidad, Capacidad de Mantenimiento, Capacidad de Servicio, Disponibilidad, mostrados en la figura a continuación.

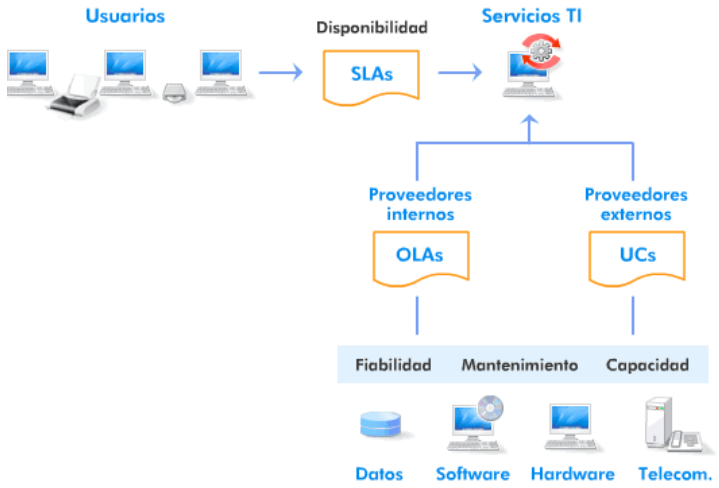

Figura 6. Proceso Gestión de la Disponibilidad
Fuente: (Quiñonez, 2015)

Algunos de los beneficios que ofrece Gestión de la Disponibilidad son:

- Reducción de costes para una alta disponibilidad.
- Cumplimiento de los niveles de disponibilidad.
- Los clientes tienen más percepción de calidad del servicio.

- Aumento de los niveles de disponibilidad.
- Reducción de incidentes.

Pueden existir algunas dificultades en la implementación de la Gestión de la Disponibilidad como:

- Monitorización incorrecta de la disponibilidad del servicio.
- Falta de compromiso en el proceso por parte de la organización de TI.
- Falta de personal y herramientas.
- Objetivos de disponibilidad desalineados con las necesidades del cliente.
- Mala coordinación con otros procesos.

2.4.2.5 Gestión de la Continuidad del Servicio

La Gestión de la Continuidad del Servicio se encarga de impedir que ocurran imprevistas y graves interrupciones de los servicios de TI, causados por fenómenos naturales o causas de fuerza mayor.

La estrategia de la Gestión de la Continuidad del Servicio (ITSCM) debe abarcar procedimientos: proactivos para impedir y minimizar las consecuencias y reactivos para reanudar el servicio lo pronto posible.

Resulta fundamental cumplir con los siguientes objetivos para una correcta Gestión de la Continuidad del Servicio:

- Garantizar una rápida recuperación de los servicios de TI.
- Fijar políticas y procedimientos para una prevención de un desastre.

Algunos de los beneficios que ofrece Gestión de la Continuidad del Servicio son:

- Gestionar los riesgos de una forma adecuada.
- Reducir el tiempo de interrupción por causas de fuerza mayor.
- Mejorar la confianza entre clientes y usuarios.

Pueden existir algunas dificultades en la implementación de la Gestión de la Continuidad del Servicio como:

- Resistencia a inversiones que no generan una rentabilidad a corto plazo.
- Mala planificación de costes asociados.
- Falta de recursos.
- Falta de compromiso en las actividades más urgentes.
- Mal análisis de riesgos.
- Personal no capacitado para realizar acciones reactivas.

2.4.2.6 Gestión de la Seguridad de la Información

La Gestión de la Seguridad de la Información segura que cada proceso como confidencialidad, integridad y disponibilidad satisfagan las necesidades acordadas del servicio. Alinea la seguridad de TI con la propia del negocio, asegurando la confidencialidad, integridad y disponibilidad de los activos de la organización.

La Gestión de la Seguridad de la Información debe cumplir los objetivos de seguridad, observando y entregando información solo a las personas autorizadas para el manejo de la misma. La información debe ser confiable, segura, y debe estar disponible en cualquier momento cuando el usuario la necesite. Todo lo referente a transacciones de negocios e intercambios de información se las debe realizar o deben ser confiables.

Esta gestión engloba los aspectos de seguridad de TI, afirmando que la política de seguridad mantenga en ejecución los servicios y sistemas que se encuentran a cargo.

Se debe tomar en cuenta que la información es lo más importante de una empresa por lo cual debe siempre contener los siguientes aspectos:

- **Confidencialidad:** El acceso a la información solo la tiene el personal autorizado.
- **Integridad:** La información debe ser la adecuada y debe estar completa.
- **Disponibilidad:** El acceso a la información debe ser de manera fácil y en cualquier momento.

Los objetivos se pueden resumir en los siguientes:

- Mitigar, minimizar y prevenir de los riesgos que pongan en amenaza que un servicio se mantenga en línea.
- Cumplir estándares de seguridad acordados en los SLAs.
- Crear políticas de seguridad que estén al 100% alineadas con el giro del negocio.

2.4.2.7 Gestión de Proveedores

La Gestión de Proveedores coordina y gestiona los servicios que reciben para poder pasar a brindar servicios de buena calidad, asegurando que todos estos tengan contratos y acuerdos apoyándose en proveedores que ayuden a abarcar con las necesidades del negocio

Los objetivos que se manejan dentro de esta gestión se los puede delimitar de la siguiente manera:

- Alcanzar el valor por el dinero que se ha entregado a los proveedores.
- Tomar en cuenta que cada contrato debe estar dentro de las necesidades del negocio.
- Obtener y llegar a un acuerdo en contratos y gestión con los proveedores.
- Manejar adecuadamente la relación y el desempeño que se tiene con los proveedores.

Mirar que cada contrato de soporte entregue valor y se alinea con los compromisos que llevan a dar valor al negocio. Teniendo proveedores con objetivos de negocio claros, y logrando que los mismos vayan comprendiendo de mejor manera el objetivo y que aporten valor al mismo.

La gestión de proveedores tiene ciertos riesgos a los cuales debe enfrentarse:

- No existe los lineamientos adecuados para contratar a los proveedores.
- Contratos no concretos donde no se puede mirar objetivos que llegan a ser cuantificables.
- No contempla indicadores de rendimiento o los obtiene tarde lo que da como resultado un suministro con baja calidad.

2.4.3 Transición del Servicio

"La transición de servicio proporciona una guía para el desarrollo y mejora de las capacidades para la transición de servicios nuevos y modificados en operaciones" (OGC, 2007).

Esta fase tiene como finalidad, facilitar la transformación de los servicios definidos en la fase previa en productos que puedan entregan valor a los clientes. Se encuentra supervisada para que los servicios entregados se encuentren alineados al núcleo del negocio, buscando reducir el impacto que genera en muchas ocasiones el cambio.

Los procesos asociados directamente a la fase de transición del servicio son:

2.4.3.1 Gestión de Cambios

La Gestión de Cambios se encarga de la evaluación y planificación del proceso que genera cambios, asegurando que el mismo se concluya de manera eficiente, teniendo un procedimiento adecuado y obteniendo calidad y continuidad del servicio de TI.

Como objetivo tiene realizar e implementar de manera óptima y adecuada los cambios que se necesiten en la infraestructura y servicios TI.

Algunos beneficios que la Gestión de Cambios que ofrece son:

- Reducción de índices y problemas asociados al cambio.
- Restauración a configuraciones estables y que tenían un impacto negativo pequeño.
- Cada cambio tiene una mejor aceptación.
- Evaluación real de costo relacionados con cada cambio.
- Creación de procedimientos para cambios estándar.

Pueden existir algunas dificultades en la implementación de la Gestión de Cambios como:

- Las demás áreas deben aceptar el nivel de autoridad que mantiene la gestión de cambios.
- No seguir los procesos y procedimientos establecidos.

- Al no conocer los procesos, actividades de la organización no pueden desarrollar correctamente la actividad.
- La Gestión de Cambios no maneja herramientas adecuadas para la documentación de procesos.

2.4.3.2 Gestión de Activos y configuración del Servicio

La Gestión de Activos y configuración del Servicio se encarga de llevar un registro donde se evidencie todas las configuraciones que se mantiene en la infraestructura y tiene como objetivos primordiales:

- Disponer de información precisa y fiable de la configuración de la infraestructura para toda la organización.
- Ser apoyo para los demás procesos como: gestión de incidencias, problemas y cambios.

2.4.3.3 Gestión de Versiones y Despliegues

La Gestión de Versiones y Despliegues se encarga de implementar y llevar un control de la calidad de todo el software y hardware que se haya colocado en el ambiente de producción.

Los objetivos más importantes que engloba esta gestión son los siguientes:

- Tener en claro una política de implementación de software y hardware en sus nuevas versiones.
- Pasar los cambios e implementaciones del ambiente real al de producción después de tener todas las validaciones en buen estado.
- Tener un respaldo idéntico del software ocupado en el ambiente de producción.

Algunos beneficios que ofrece Gestión de Versiones y Despliegues son:

- Cuando se realice un cambio este proceso se dará sin un deteriro del servicio.
- Objetivos cumplidos en versiones nuevas.
- Reducción de copias ilegales de software.

- Mantener el control del software y hardware usado.

Pueden existir algunas dificultades la Gestión de Versiones y Despliegues como:

- No se mantiene claro quien esta con la responsabilidad sobre el proceso de implementación de cambios.
- No existe el ambiente de desarrollo donde realizar pruebas optimas de funcionamiento.
- Existe una mala actitud de los demás departamentos al centralizar los cambios.

En el manejo de versiones se pueden llegar a tener 3 clasificaciones:

- **Mayores**: Las que contemplan modificaciones de gran magnitud e importantes dentro de los aspectos funcionales, características técnicas.
- **Menores**: Correcciones en errores conocidos de impacto bajo y que normalmente son modificaciones de implementaciones anteriores.
- **Emergencia**: Cambios o modificaciones que dan una respuesta o resolución rápida a errores presentados.

La siguiente figura ilustra gráficamente la evolución temporal de una versión:

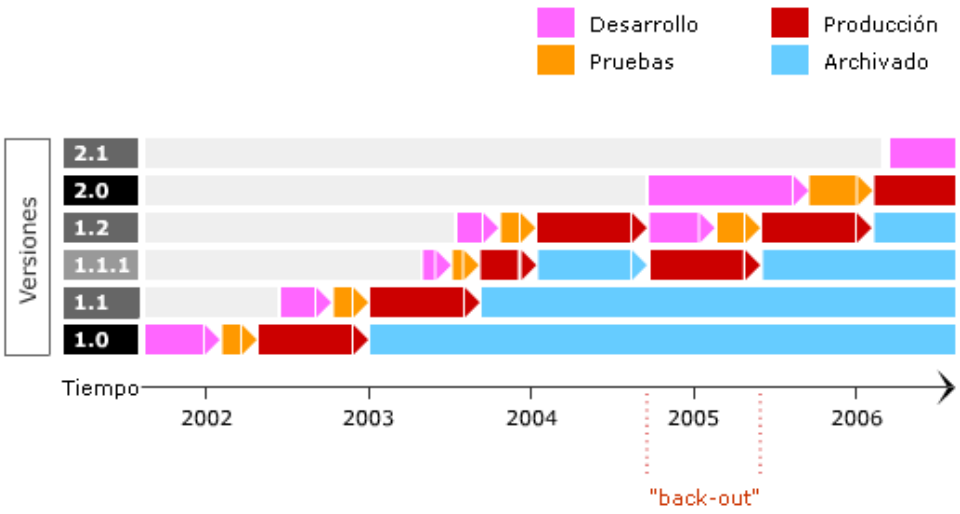

Figura 7. Evolución Temporal de Versiones
Fuente: (Quiñonez, 2015)

2.4.3.4 Validación y Prueba del Servicio

La Validación y Prueba del Servicio se encarga de realizar las evaluaciones necesarias en un ambiente de test o de pruebas antes de realizar su lanzamiento e implementación.

Para llegar a su objetivo esta realiza lo siguiente:

- Tener diseñado un ambiente de pruebas que sea una réplica exacta del ambiente real.
- Conocer en su totalidad la función del servicio para poder realizar las pruebas necesarias en todos los escenarios posibles.
- Tener en conocimiento lo que estipuló el cliente en el requisito para ver que efectivamente se está cumpliendo con lo especificado.
- Tener una planificación basada en un calendario de pruebas.

Algunos de los beneficios que ofrece Validación y Prueba del Servicio:

- Reducción de las incidencias por incompatibilidad de programas o hardware instalado anteriormente.
- Detección de errores conocidos en tiempo real.
- Costos por incidentes resueltos menos por contar con un ambiente de pruebas.

2.4.3.5 Evaluación

En el proceso de Evaluación se realiza la recolección y análisis de la información que está disponible para tener el nuevo cambio y realizando los reportes necesarios para toma de decisiones.

La Evaluación debe proporcionar la información completa para determinar con seguridad que el aspecto del servicio es válido para el negocio.

Pueden existir algunas dificultades de la Evaluación:

- Existe una mala agilidad en el proceso y se generan cuellos de botella y retrasan la implementación.

- Los resultados que detalla la evaluación llegan a ser incompletos ya que la muestra es reducida.

2.5 Pasos para la creación de un CSIRT

La Guía práctica para la creación de un Centro Académico de Respuesta ante Incidentes de Seguridad Informática (CSIRT Académico) propuesta por (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017) conforma 5 fases: Estrategia, Diseño, Transición, Operación y Mejora Continua. La propuesta del CSIRT-ESPE cubre las 2 primeras fases detalladas a continuación.

2.5.1 Fase I.- Planeamiento Estratégico

- **Conformación del equipo inicial de proyecto. -** Se define los promotores del proyecto que conformarán el equipo inicial, siendo el número máximo 5 personas las que pueden conformar el equipo.
- **Definición del Plan inicial de trabajo. -** Se planifican todas las actividades necesarias a desarrollarse para elaborar la propuesta preliminar.
- **Bitácora. -** Este documento registra todas las actividades llevadas a cabo por el equipo inicial del proyecto.
- **Estudio de la situación actual en la universidad. -** Se analizan documentos organizacionales y de tecnología de la universidad para ayudar a definir la demanda y los servicios que brindará el CSIRT académico.
- **Definición de la entidad patrocinadora. -** Se determina la entidad que patrocina al CSIRT**.**

2.5.2 Fase II.- Diseño

- **Plan Estratégico del CSIRT. -** Se elabora el documento que constituye la hoja de ruta de vida del CSIRT en los siguientes años, entre sus componentes están: misión, visión, objetivos, estrategias, políticas e indicadores de medición del cumplimiento de los objetivos y metas trazadas.
- **Plan Operativo Anual. -** Se elabora el POA con proyectos basados en las estrategias del Plan Estratégico creado anteriormente.

- **Análisis y gestión de la demanda. -** Se determina el público al que el CSIRT prestará sus servicios, el alcance y extensión de esta demanda y la proyección de los siguientes años.
- **Portafolio de Servicios. -** Se establecen los servicios reactivos, proactivos y de gestión de calidad de seguridad que sean necesarios para la comunidad.
- **Relación con otros equipos. -** Se identifica las entidades u organizaciones con las que se tendrá alianzas estratégicas.
- **Políticas y Procedimientos. -** Se establecen las directrices o limitaciones derivadas de los objetivos, las estrategias y los servicios propuestos.
- **Modelo organizacional. -** Se detalla el modelo organizacional, la organización por procesos, la ubicación dentro del organigrama de la universidad y las responsabilidades.
- **Clasificación de puestos-especificaciones de clase. -** Se elabora el organigrama posicional del CSIRT y se describe los puestos del personal del equipo.
- **Infraestructura y equipamiento. -** Se determina el espacio físico y el equipamiento que se va a utilizar.
- **Planes de seguridad, recuperación de desastres y continuidad de servicios. -** Se elabora los planes de seguridad física, lógica y de comunicaciones.
- **Presupuesto y Financiamiento. -** Se elabora el presupuesto de inversión inicial y de operación anual del CSIRT.
- **Diseño y cronograma de implantación del proyecto. -** Se elabora el cronograma con las actividades de implantación del proyecto.
- **Definición de indicadores de evaluación de la implantación del proyecto. -** Se establece los indicadores y la forma en la que se evaluará el proyecto.
- **Elaborar el proyecto definitivo de creación del CSIRT. -** Se elabora el proyecto de creación de acuerdo a la plantilla manejada por la universidad.

CAPÍTULO III
ESTRATEGIA Y DISEÑO DEL CSIRT-ESPE

3.1 Introducción

El propósito de este capítulo es mostrar información acerca de los objetivos estratégicos organizacionales establecidos en el Plan Estratégico de la ESPE y los procedimientos de seguridad de la información que maneja la Unidad de Tecnologías de la Información y Comunicación de la ESPE actualmente para obtener un visión completa de la situación actual de la Universidad, permitiendo así una correcta definición de la demanda, políticas, procedimientos y los servicios que el CSIRT brindará, así como su modelo organizacional y recursos.

3.2 Conformación del equipo inicial del proyecto

Los promotores del proyecto que conforman el equipo inicial son:

- Ing. Mario Ron
- Ing. Walter Fuertes
- Ing. Rommel Asitimbay
- Delegado del Vicerrectorado de investigación
- Sr. Mario Parra
- Sr. Hugo de la Torre

3.3 Definición del Plan inicial de trabajo

El Plan inicial de trabajo detalla todas las actividades necesarias que deben desarrollarse para elaborar la propuesta preliminar.

Tabla 5
Plan Inicial de trabajo CSIRT-ESPE

PLAN INICIAL DE TRABAJO			
Semana	**Actividad**	**Objetivo**	**Responsables**
1,2,3	Estudio de la Situación Actual de la Universidad	Recoger información básica de la Universidad que sirva para definir la demanda y los servicios que el CSIRT brindará, así como su estructura y recursos.	Sr. Hugo de la Torre Sr. Mario Parra
4	Definición de la entidad patrocinadora	Determinar la entidad que patrocina el CSIRT.	Ing. Mario Ron
5,6	Elaboración del Plan Estratégico del CSIRT	Definir el documento que constituye la hoja de ruta del CSIRT en los próximos años.	Sr. Hugo de la Torre
7,8	Elaboración del Plan Operativo Anual del CSIRT	Definir los proyectos que se derivan de las estrategias para el primer año.	Sr. Hugo de la Torre
9	Análisis y gestión de la demanda	Determinar la comunidad a la que se prestará servicios.	Sr. Hugo de la Torre
9	Elaboración del portafolio de servicios	Establecer los servicios requeridos por la comunidad.	Sr. Mario Parra
10	Definición de la relación con otros equipos	Identificar a las organizaciones o entidades con las que se tendrá contacto.	Sr. Mario Parra
10	Definición de las políticas y procedimientos	Determinar las directrices o limitaciones de alto nivel que guían la ejecución de procedimientos.	Sr. Mario Parra
11	Elaboración del modelo organizacional	Definir el modelo organizacional en base a los modelos existentes.	Sr. Mario Parra
12	Clasificación de los puestos-especificaciones base	Elaborar el organigrama posicional del CSIRT y las	Sr. Mario Parra

CONTINÚA

		descripciones de puesto del personal del equipo.	
13,14	Especificación de la infraestructura y equipamiento	Especificar un espacio físico para el CSIRT.	Sr. Mario Parra
15,16	Elaboración de los planes de seguridad, de recuperación de desastres y continuidad de servicios	Elaborar los planes de seguridad física, lógica y de comunicaciones.	Sr. Hugo de la Torre
17	Elaboración del presupuesto y financiamiento	Definir el presupuesto de inversión inicial.	Sr. Hugo de la Torre
18	Diseño del cronograma de implantación del proyecto	Determinar las actividades de implantación del proyecto.	Sr. Mario Parra
18	Definición de indicadores de evaluación de la implantación del proyecto	Establecer los indicadores, productos y entregables y la forma de evaluación de la implantación.	Sr. Mario Parra
19,20	Elaboración del proyecto definitivo de creación del CSIRT	Crear el proyecto de acuerdo a la plantilla de la Universidad.	Sr. Hugo de la Torre Sr. Mario Parra

3.4 Bitácora

La bitácora lleva el registro de las reuniones que se han establecido con los integrantes del equipo inicial del proyecto.

Tabla 6
Bitácora reuniones equipo CSIRT-ESPE

Fecha	Ord	Actividad	Participantes
19/03/2018	1	Conformación del equipo inicial.	Todos promotores del proyecto.
19/03/2018	2	Planificación inicial de trabajo.	Ing. Mario Ron Sr. Mario Parra Sr. Hugo de la Torre
19/03/2018	3	Elaboración del Plan inicial de campo.	Sr. Mario Parra Sr. Hugo de la Torre

CONTINÚA

25/03/2018	4	Revisión documentos para Análisis de la situación actual.	Ing. Rommel Asitimbay Sr. Mario Parra Sr. Hugo de la Torre
31/07/2018	5	Revisión de la propuesta de creación.	Ing. Mario Ron Sr. Mario Parra Sr. Hugo de la Torre
06/08/2018	6	Revisión de la propuesta de creación definitiva.	Todos los promotores del proyecto.

3.5 Situación Actual de la ESPE

La información que se presenta a continuación acerca de la ESPE fue tomada de la página institucional en la que se describe: Quién es la Universidad, su misión, visión y sus valores institucionales.

La Universidad de las Fuerzas Armadas ESPE posee más de 90 años de historia, es considerada una de las más representativas del país por su firme innovación y aporte al desarrollo productivo del Ecuador. Se fundó en el año de 1922 y es distinguida por conceder soluciones prácticas a los requerimientos y preocupaciones de la sociedad ecuatoriana, ayudando a la generación de nuevos conocimientos mediante la docencia, la investigación y la vinculación con la sociedad.

En el 2014, fue clasificada por el Ranking Mundial de Universidades QS entre las 250 mejores de América Latina y la 4ta mejor del Ecuador. Actualmente, la universidad dirige la Red de Universidades y Escuelas Politécnicas para la Investigación y Posgrados conformada por más de 20 universidades ecuatorianas.

La Universidad se encuentra regulada por la Constitución de la República del Ecuador y la Ley Orgánica de Educación Superior. Después de la firma del Estatuto de creación, el 26 de junio del 2013, y aprobado por el Consejo de Educación Superior (CES).

Una vez analizado el Plan Estratégico de Tecnologías de la información y comunicaciones de (UTIC ESPE, 2015) se obtuvo la siguiente información organizacional.

Misión

"Formar profesionales e investigadores de excelencia, creativos, humanistas, con capacidad de liderazgo, pensamiento crítico y alta conciencia ciudadana; generar y aplicar el conocimiento científico; y transferir tecnología, en el ámbito de sus dominios académicos, para contribuir con el desarrollo nacional y atender las necesidades de la sociedad y de las Fuerzas Armadas" (ESPE, 2018).

Visión

"La Universidad de las Fuerzas Armadas- ESPE es reconocida, como un referente a nivel nacional y regional por su contribución en el ámbito de sus dominios académicos, al fortalecimiento de la Seguridad y la Defensa, bajo un marco de valores éticos, cívicos y de servicio a la comunidad" (ESPE, 2018).

Valores Institucionales

- Honestidad
- Respeto por la dignidad humana
- Disciplina
- Identidad
- Compromiso institucional
- Responsabilidad social
- Civismo

Estructura Organizacional

En la siguiente ilustración se representa la estructura organizacional por procesos con las respectivas unidades administrativas.

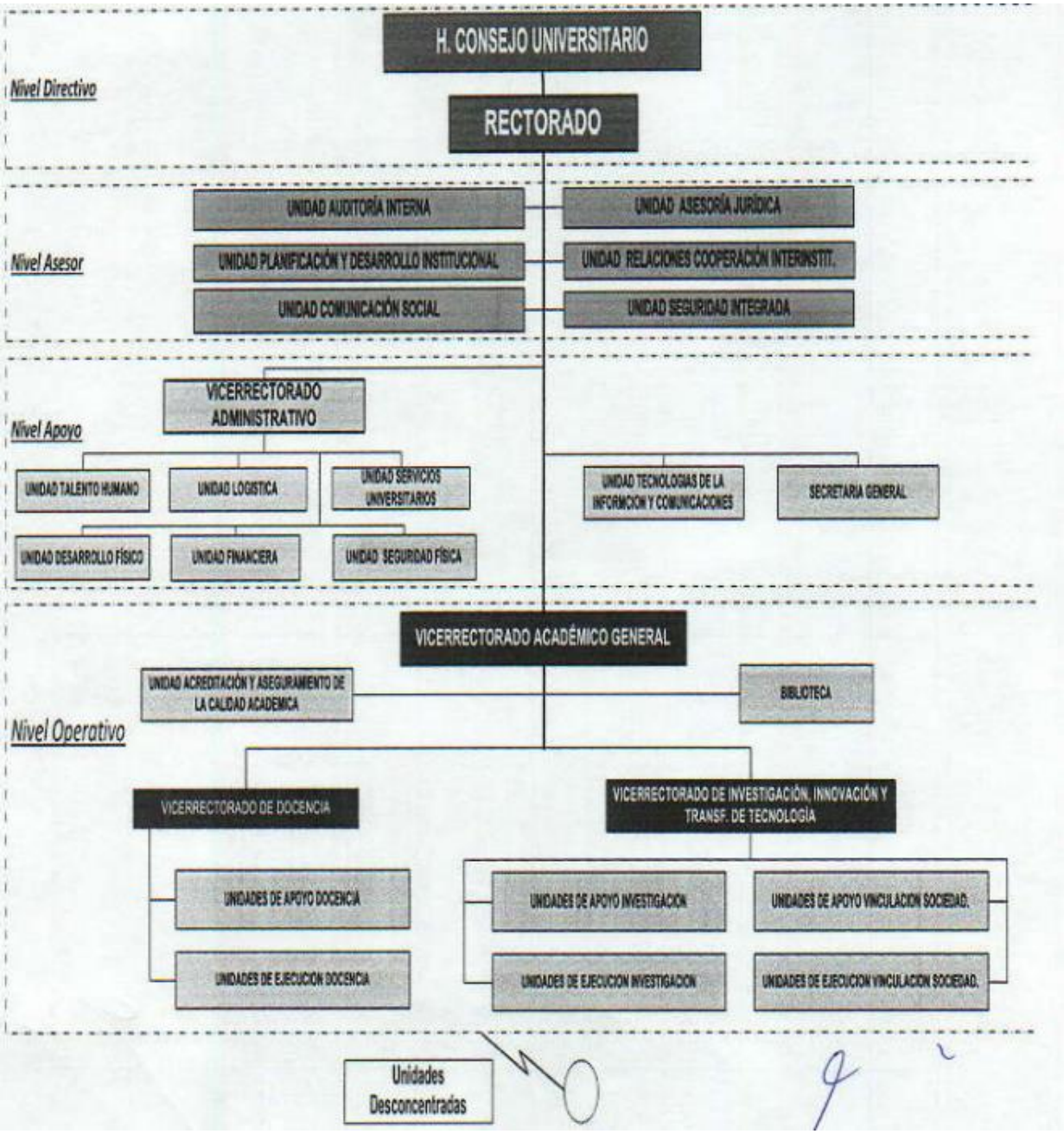

Figura 8. Organigrama Estructural de la ESPE
Fuente: (ESPE, 2015)

Sedes y Estudiantes

La Universidad forma parte del Sistema de Educación Superior del Ecuador, compuesta por el campus matriz en Sangolquí, las sedes Latacunga y Santo Domingo de los Tsáchilas, así como

las Unidades Académicas Especiales y el Instituto de Idiomas; tiene alrededor de 13.000 estudiantes, entre civiles y militares, de ellos 8.309 son hombres y 5.606 son mujeres.

Infraestructura

En el siguiente diagrama se puede observar las redes y comunicaciones de la Universidad, en el cual se visualiza el enlace de internet y algunos de los equipos de seguridad.

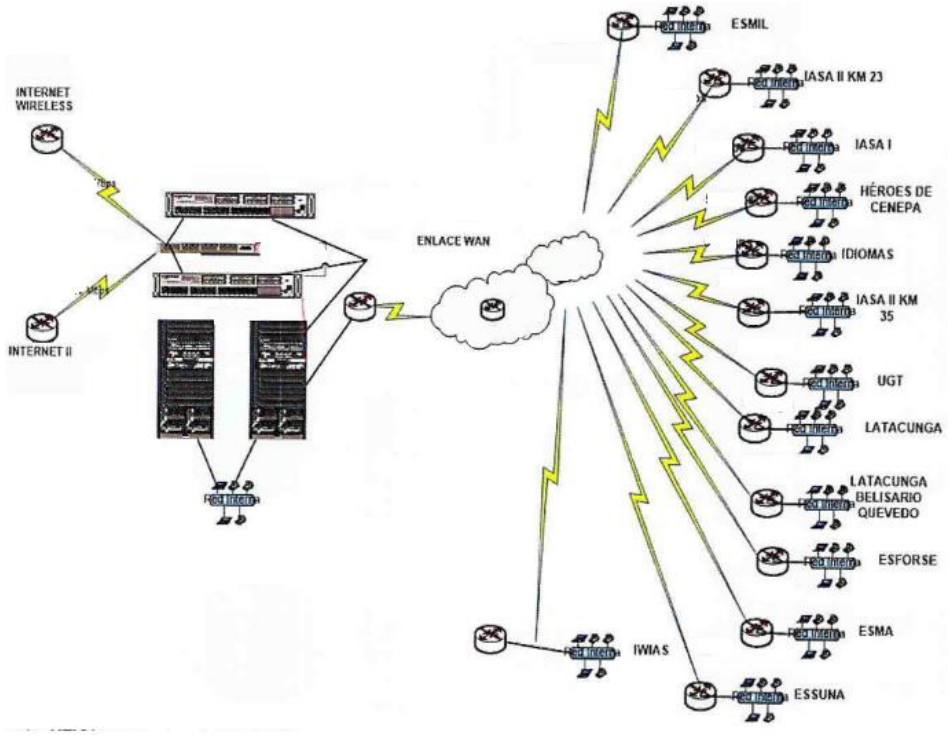

Figura 9. Diagrama de Red de la ESPE
Fuente: (UTIC ESPE, 2015)

El servicio de internet dentro de la Universidad es utilizado mediante cableado o la red inalámbrica, este servicio es brindado en su matriz, sedes, extensiones, unidades académicas externas y especiales.

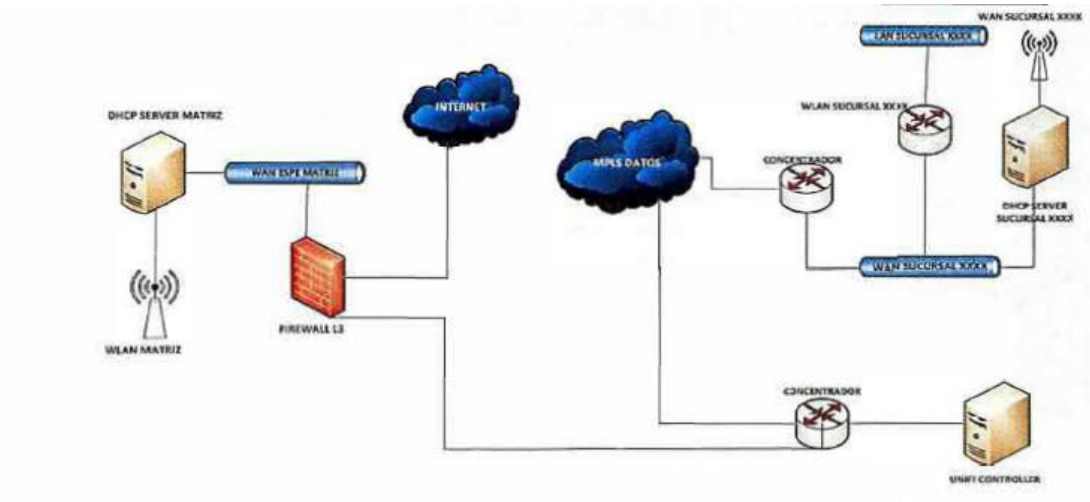

Figura 10. Red Inalámbrica de la ESPE
Fuente: (UTIC ESPE, 2015)

Servidores

Los servidores utilizados por UTIC para los servicios y aplicaciones de tecnologías mencionadas se encuentran instalados en servidores físicos y virtuales. Se muestran a continuación los principales servidores y los que se encuentran virtualizados.

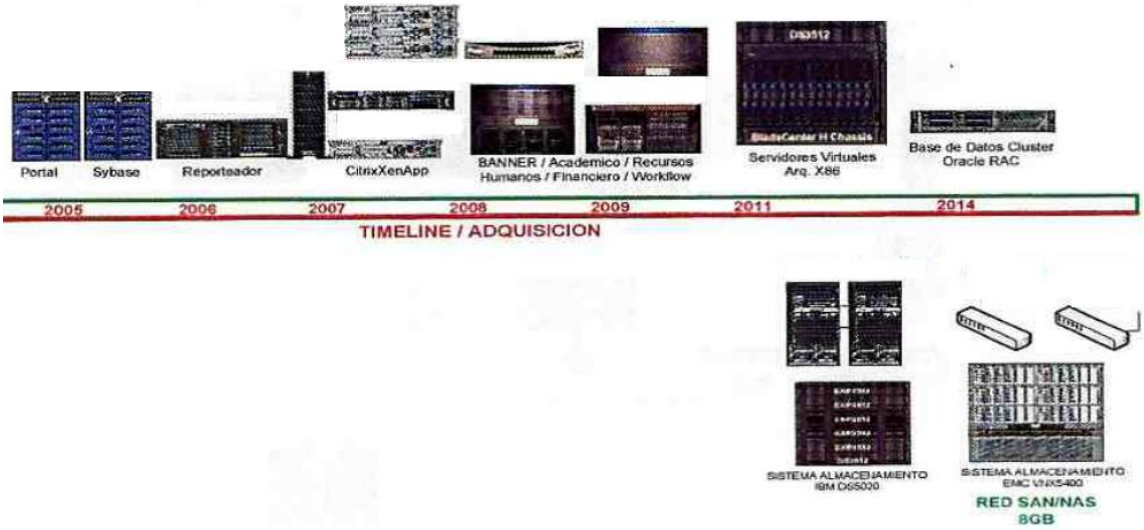

Figura 11. Servicios Físicos Principales ESPE
Fuente: (UTIC ESPE, 2015)

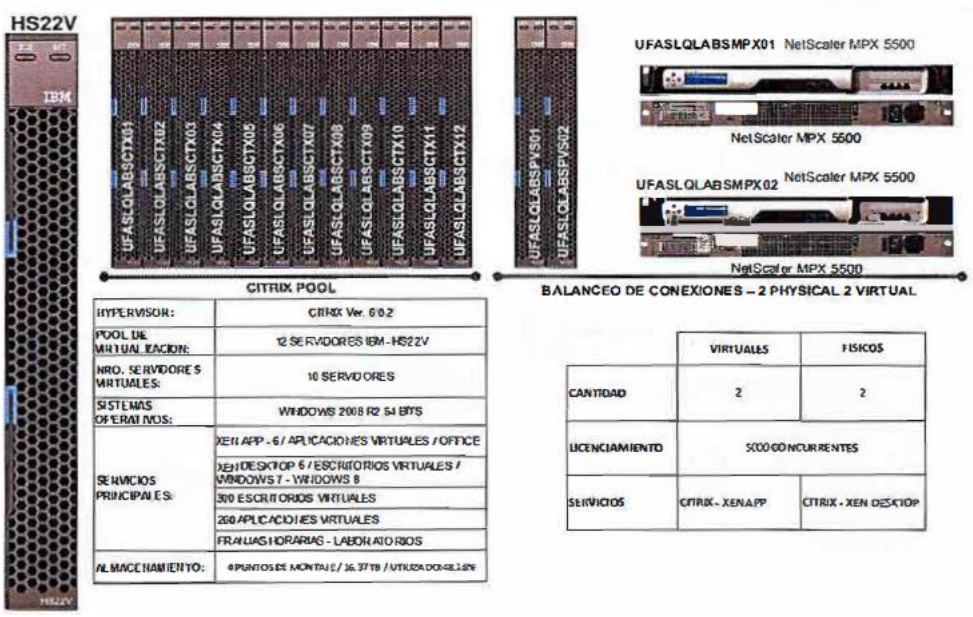

Figura 12. Servidores Virtualización de los laboratorios de computación ESPE
Fuente: (UTIC ESPE, 2015)

Como se puede observar en la figura a continuación, todas las aplicaciones que colaboran en la provisión de los servicios tecnológicos de la ESPE se encuentran alojadas en los servidores mencionados.

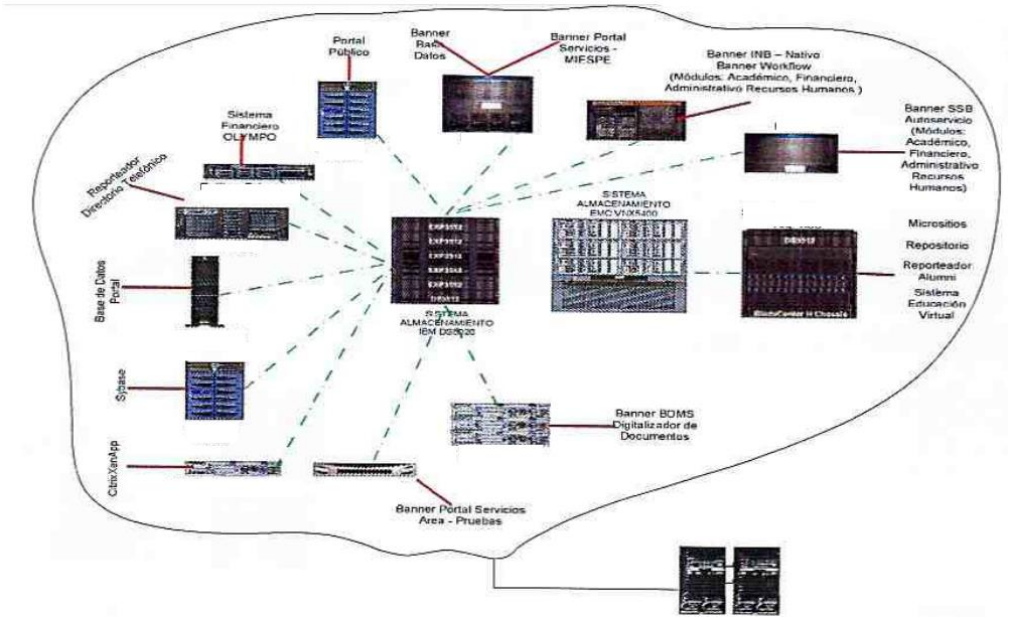

Figura 13. Distribución de las aplicaciones en los servidores ESPE
Fuente: (UTIC ESPE, 2015)

Catálogo de Servicios Tecnológicos

Los servicios de Tecnologías de Información y Comunicación se encuentran detallados a continuación y siendo resaltados los servicios más críticos:

Tabla 7
Catálogo de Servicios Tecnológicos de la ESPE

Servicios	Accesos
Sistemas de Gestión Académica	A través de la web
Servicios Web	A través de la web
Sistemas de Gestión Administrativa	A través de la web
Sistema Banner - Administrativo (RRHH) Sistema Banner - Digitalización Sistema Banner - Workflow Sistema Banner - Autoservicios Sistema Banner - MiESPE Sistema Ex alumnos ALUMNI	A través de la web
Sistemas de Gestión Administrativa Sistema SIFRHE Sistemas Olympo (Contabilidad, Facturación, Inventario, Especies, Activos Fijos)	Dentro de Intranet
Repositorios Digitales de Archivos	A través de la web
Soporte Técnico Mantenimiento	En la Universidad o externa a través de teléfono
Internet/Wifi	- Internet Comercial avanzado a través de Cableado - Wifi requiere de una

CONTINÚA

	autenticación
Correo institucional	A través del portal
Telefonía	Llamadas internas y nacionales, se requiere de una clave.
Videoconferencia	Las salas de videoconferencia existentes
Virtualización de servidores	De acuerdo al requerimiento
Alojamiento de infraestructura	De acuerdo al requerimiento

Fuente: (UTIC ESPE, 2015)

Provisión de servicios

La Unidad de Tecnologías de Información y Comunicación cuenta con una Mesa de Servicios de TI, que se encarga de atender incidentes en software, comunicaciones y aplicativos institucionales de nivel 0 y 1, además atienden incidentes de hardware de nivel 2.

Plan de Contingencia

La Unidad de Tecnologías de Información y Comunicación dentro de su plan de contingencia define fichas para definir las actividades en el momento de una contingencia. Las mencionadas se encuentran definidas para situaciones como:

- Falta de disponibilidad de los sistemas.
- Incendio.
- Sismo.
- Falla en la red de datos.
- Infección de virus.
- Daño en componentes físicos.
- Erupción volcánica.
- Interrupción de energía.

- Falla en motor de base de datos.
- Falla en sistema operativo.
- Ataques informáticos
- Salida de un experto de TI.
- Explosión.
- Pérdida de telefonía IP.
- Pérdida de equipos de seguridad perimetral.

3.6 Definición de la entidad patrocinadora

El Vicerrectorado de investigación innovación y transferencia tecnológica de la Universidad de las Fuerzas Armadas ESPE sería el patrocinador del CSIRT Académico.

3.7 Plan Estratégico

Introducción

En los últimos años se ha podido ver cómo la tecnología crece y avanza rápidamente, y cada día se encuentra algo nuevo para usar o simplemente para obtenerlo. Toda la tecnología ha revolucionado los diferentes aplicativos, programas que diariamente empezamos a usar, creando así, diferentes vulnerabilidades y cierta inseguridad.

Dentro de la Universidad de las Fuerzas Armadas ESPE, mientras el tiempo ha transcurrido se han automatizado procesos para tener toda la información de una manera digital y no de una manera física sino lógica. Dando lugar a que toda la información se la almacene de manera lógicamente en base de datos, se ocupen software para el manejo de la información. Todo esto siempre recae a implementar seguridades informáticas para que dicha información no sea alterada, no sea ultrajada, y tampoco sea manipulada de una forma inadecuada.

Por este motivo se plantea tener un CSIRT en la Universidad de las Fuerzas Armadas ESPE, donde se maneje la seguridad a este tipo de sistemas que manejan la información sensible. Creando servicios de monitoreo y mitigación de los mismos, a continuación, se va a presentar el plan

estratégico para poder formar el CSIRT en la Universidad y que este sea el centro de protección a la información manejada en la comunidad politécnica.

Análisis ambiental

- **Fortalezas**
  - Docentes y profesionales con conocimientos de seguridades informáticas.
  - Equipamiento inicial adecuado para brindar servicios tecnológicos relacionados con seguridades informáticas.
  - Infraestructura física disponible.
- **Oportunidades**
  - Apertura en la investigación y creación de procesos sobre mitigación de ataques informáticos.
  - Apoyo de entidades externas relacionadas con la seguridad de la información.
  - Convenios de la Universidad de las Fuerzas Armadas ESPE con organismos y entidades relacionadas
  - Disponibilidad de equipamiento y software moderno
  - Necesidad de formación y entrenamiento en seguridades para el personal informático de entidades públicas y privadas
  - Costos altos en certificación y entrenamiento de seguridad de la información
  - Falta de servicios de CERT para la Universidad de las Fuerzas Armadas ESPE.
- **Debilidades**
  - Falta de entrenamiento en herramientas especializadas por parte del personal del CERT.
  - Asignación de carga horaria para docentes que participen del proyecto.
- **Amenazas**
  - Escaso presupuesto de la Universidad para proyectos tecnológicos.
  - Falta de una política nacional de ciberseguridad.
  - Falta de acuerdos entre universidades en proyectos de innovación de la seguridad de la información.

Principios

- Nos debemos a la Universidad ecuatoriana, apoyamos sus principios y desarrollo.
- La comunidad de atención debe recibir un servicio de calidad, técnico y garantizado que permita proteger su información.
- La evolución de servicios que brinda el CERT, se traza en función del crecimiento de la comunidad objetivo y sus necesidades.
- El uso de herramientas avanzadas en concordancia con el desarrollo tecnológica de las amenazas es fundamental en la operación del CERT.
- El trabajo conjunto con otros equipos de respuesta y organizaciones relacionadas permite realizar un trabajo efectivo ante las amenazas tecnológicas.

Valores

- **Honestidad. –** Virtud que posee y manifiestan siempre los miembros que pertenecen al CSIRT en cada proceso y en el desarrollo de su trabajo diario. Actuando éticamente y con coherencia entre lo que se siente y piensa.
- **Tenacidad. –** Capacidad con la que trabaja cada miembro del equipo para tener la virtud de llegar a cada objetivo propuesto sin dejarse vencer por cualquier adversidad que se pueda encontrar en el camino.
- **Solidaridad. –** Cualidad que destaca en cada miembro del equipo para poder trabajar en grupo, poder buscar soluciones óptimas para la comunidad.
- **Disciplina. –** Actitud de cada miembro del equipo que trabaja en el CSIRT con el objetivo de obtener hábitos de trabajo y de proactividad dentro del equipo.
- **Lealtad. –** Virtud que mantiene cada miembro de la organización, la cual genera confianza hacia la organización y la capacidad de nunca dar la espalda.

Misión

Brindar servicios que permitan identificar y mitigar ataques al sistema de información de la Universidad de las Fuerzas Armadas ESPE, coadyuvar en la capacitación y formación de personal especializado en respuesta a incidentes informáticos de entidades públicas y privadas.

Visión

Consolidar al CSIRT-ESPE como líder de equipos de respuesta ante incidentes informáticos en el país.

Objetivos Estratégicos, Indicadores y Estrategias

OE1- Incrementar e innovar los servicios de respuesta ante incidentes informáticos, para una comunidad creciente.

Estrategias

- Impulsando nuevos procesos de seguridad dando protección a sistemas informáticos a toda la comunidad.
- Investigando acerca de nuevos métodos de mitigación de ataques informáticos.
- Incrementando la cobertura de servicios a una comunidad creciente.

OE2- Brindar servicios de respuesta ante incidentes informáticos con procesos certificados internacionalmente.

Estrategias

- Implantando estándares mundiales para la respuesta ante incidentes de seguridad de la información.
- Fortaleciendo relaciones internacionales con otros equipos de respuesta y organismos de certificación.
- Evaluando en forma permanente los procesos y aplicando planes de mejora.

OE3- Incrementar el aporte financiero de la comunidad y los recursos para el desarrollo y crecimiento del CSIRT.

Estrategias

- Participando en convocatorias y recursos concursables para proyectos de investigación y vinculación.
- Gestionando el auspicio de publicaciones de artículos científicos relacionados al trabajo del CSIRT.
- Gestionando el presupuesto del CSIRT dentro del presupuesto institucional y de organismos relacionados.

OE4- Incrementar los recursos disponibles tanto humanos como materiales y equipos, para brindar un servicio de calidad.

Estrategias

- Completando el equipamiento de hardware y software especializado.
- Capacitando al personal del CSIRT mediante certificaciones internacionales y entrenamiento relacionado.
- Logrando un espacio físico seguro para el funcionamiento del CSIRT.

3.8 Plan Operativo Anual

Introducción:

En base a la estructuración y los procesos que se manejan dentro un CSIRT se ha realizado el Plan Operativo Anual, el cual permite la mejora de procesos y toma en cuenta los planes de crecimiento que se mantendrá dentro del proceso de creación, obteniendo así, una mejor infraestructura, procesos y servicios que se puedan brindar a la comunidad de la Universidad de las Fuerzas Armadas ESPE.

Proyectos en Base a los Objetivos Estratégicos:

OE1.- Incrementar e innovar los servicios de respuesta ante incidentes informáticos, para una comunidad creciente.

- Analizar y Generar procedimientos adecuados para la mitigación de ataques.
- Plataforma de pruebas de mitigación de ataques.
- Plan de monitoreo constante para ver necesidades de las comunidades que se unen al CSIRT.

OE2.- Brindar servicios de respuesta ante incidentes informáticos con procesos certificados internacionalmente.

- Implantar los estándares aceptados mundialmente para procesos en el CSIRT.
- Charlas o seminarios para compartir conocimientos entre equipos de respuesta mundiales.
- Plan de monitoreo constante de procesos para mitigación de diferentes ataques.

OE3.- Incrementar el aporte financiero de la comunidad y los recursos para el desarrollo y crecimiento del CERT.

- Participando en convocatorias y recursos concursables para proyectos de investigación y vinculación.
- Gestionando el auspicio de publicaciones de artículos científicos relacionados al trabajo del CSIRT
- Gestionando el presupuesto del CSIRT dentro del presupuesto institucional y de organismos relacionados.

OE4.- Incrementar los recursos disponibles tanto humanos como materiales y equipos, para brindar un servicio de calidad.

- Actualización constante de hardware y software para proveer servicios óptimos.
- Cada 3 meses realizar planes de capacitaciones internacionales respecto al manejo y administración de procesos de mitigación de ataques informáticos.
- Gestionar la ubicación física del CSIRT en el Edificio de Investigaciones y Postgrados de la Universidad de las Fuerzas Armadas ESPE.

3.9 Análisis y Gestión de la Demanda

Los organismos cada vez se enfrentan a diferentes necesidades tecnológicas que se van generando con el avance de la tecnología. Por lo cual la Universidad de las Fuerzas Armadas ESPE, dará el servicio de monitoreo de redes para la búsqueda y mitigación de ataques informáticos a los sistemas o bases que maneja la universidad, y la comunidad universitaria a la cual se brinda los servicios.

Las redes de las organizaciones estarán bajo constante monitoreo del CSIRT, tendrán la certeza de estar protegidos ante diferentes ataques cibernéticos, teniendo una alerta inmediata sobre los ataques mitigados y el tratamiento de los mismos.

La información que se maneje de ataques y de procesos para mitigar los mismos servirá a la comunidad para estar informada sobre los ataques y cómo se pueden proteger de cada uno de ellos, así mejorando la protección y confidencialidad de información que se maneja en cada uno de los organismos.

Se debe tomar en cuenta que se debe brindar un asesoramiento puntual a cada uno de los organismos para saber qué servicios puntuales son los que cada una necesitaría, ya que el portafolio de servicios es amplio y no por ello un organismo necesitará todos los servicios que se ofertan.

3.10 Portafolio de Servicios

Para establecer los servicios que se brindarán en el CSIRT-ESPE, es necesario realizar una matriz de impacto entre todos los servicios que puede ofrecer un CSIRT y las necesidades o criterios derivados del análisis de la situación actual de la Universidad. Dentro del análisis realizado se examinó las funcionalidades que cubren cada uno de los servicios y se los relacionó con el nivel de impacto que tendría en las actividades seleccionadas, el análisis mencionado se presenta a continuación:

Tabla 8
Matriz de Impacto Servicios

Servicios / Criterios	Sedes	Comunidad (Demanda)	Infraestructura tecnológica	Servicios tecnológicos	Riesgos tecnológicos	Investigación	Formación profesional
Alertas y Advertencias							
Manejo de Incidentes							
Manejo de Vulnerabilidades							
Manejo de Artifact							
Anuncios							
Observatorio de tecnología							
Evaluaciones o Auditorías de la Seguridad							
Configuración y Mantenimiento de las Herramientas, Aplicaciones, Infraestructuras y Servicios de Seguridad							
Desarrollo de Herramientas de Seguridad							
Detección de intrusos							
Difusión de información relacionada con la Seguridad							
Análisis de Riesgo							
Planificación de la Continuidad del Negocio y Recuperación de desastres							
Consultoría de Seguridad							
Concientización							
Educación / Capacitación							
Evaluación o certificación de productos							

Donde cada criterio se lo interpreta como:

- **Sedes:** Influencia en todas las sedes, extensiones y centros de apoyo de la Universidad.
- **Comunidad:** Influencia en la demanda de estudiantes, docentes, investigadores y personal administrativo de la Universidad.

- **Infraestructura tecnológica:** Influencia en la infraestructura, hardware y software de la Universidad.
- **Servicios críticos:** Ayuda en la mejora de la disponibilidad de los servicios Tic's críticos de la Universidad.
- **Riesgos tecnológicos:** Evita los puntos únicos de fallas principales de la Universidad.
- **Investigación:** Contribución al desarrollo de la investigación relacionada a seguridad de la información.
- **Formación profesional:** Contribución en el desarrollo profesional de estudiantes, docentes, investigadores y personal administrativo de la Universidad.

A continuación, se muestra el cálculo y priorización realizado mediante una escala de colores para la obtención de los servicios que resultan ser fundamentales y básicos en la etapa inicial del CSIRT-ESPE y en la etapa de desarrollo y crecimiento.

Tabla 9
Ponderación Impacto y Priorización Servicios

Servicios / Criterios	**Alto**	**Medio**	**Bajo**	**Valor**
Alertas y Advertencias	4	2	1	17
Manejo de Incidentes	4	2	1	17
Manejo de Vulnerabilidades	4	2	1	17
Manejo de Artifact	2	2	3	13
Anuncios	3	3	1	16
Observatorio de tecnología	2	3	2	14
Evaluaciones o Auditorías de la Seguridad	2	2	3	13
Configuración y Mantenimiento de las Herramientas, Aplicaciones, Infraestructuras y Servicios de Seguridad	1	2	4	11
Desarrollo de Herramientas de Seguridad	2	3	2	14
Detección de intrusos	3	1	3	14
Difusión de información relacionada con la Seguridad	6	1	0	20
Análisis de Riesgo	1	4	2	13
Planificación de la Continuidad del Negocio y Recuperación de desastres	2	4	1	15

CONTINÚA

Consultoría de Seguridad	2	3	2	14
Concientización	5	2	0	19
Educación / Capacitación	3	4	0	17
Evaluación o certificación de productos	1	2	4	11

El análisis del impacto realizado se ha basado en los requerimientos de la universidad y tomando en cuenta diferentes criterios proporcionados por normativas y guías prácticas para la creación de un CSIRT Académico, como el propuesto por la (ENISA, 2006), obteniendo así la definición de los posibles servicios a ofertar por el CSIRT-ESPE, se presenta a continuación los servicios básicos para la etapa inicial planteada.

Tabla 10
Propuesta Servicios Iniciales del CSIRT-ESPE

Tipo Servicio	Servicios
Servicios Reactivos	- Alertas y Advertencias. - Manejo de incidentes. - Manejo de vulnerabilidades.
Servicios Proactivos	- Comunicados, alertas. - Difusión de información relacionada con la seguridad.
Servicios de Gestión de Calidad de la Seguridad	- Sensibilización. - Educación y Capacitación.

Sin embargo, el CSIRT-ESPE en sus etapas de desarrollo y crecimiento debería ir aumentando su portfolio de servicios, esto debido al incremento de recursos y demanda. Acorde al análisis de impacto estos servicios mencionados se detallan a continuación:

Tabla 11
Propuesta Servicios para Desarrollo y Crecimiento del CSIRT ESPE

Tipo Servicio	Servicios
Servicios Reactivos	- Manejo de artifact

CONTINÚA

Servicios Proactivos	- Observatorio de tecnología - Evaluaciones o auditorías de seguridad. - Desarrollo de herramientas de seguridad. - Detección de intrusos.
Servicios de Gestión de Calidad de la Seguridad	- Análisis de riesgos. - Consultoría de seguridad. - Continuidad del negocio y recuperación tras un desastre.

3.11 Relación con otros equipos

A nivel mundial existen distintos CSIRTs Académicos y Nacionales, establecer una relación con algunos de estos equipos de respuesta ya establecidos formalmente resulta fundamental, porque funcionarían como sponsor para que el CSIRT-ESPE pueda ingresar al FIRST. Como etapa inicial se pueden establecer comunicaciones con el Centro de respuesta a Incidentes informáticos de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CSIRT-CEDIA), con el EcuCERT por su cercanía al encontrarse en Ecuador y con el Centro de Respuestas de Incidentes de Seguridad (CSIRT) académico de la Universidad Nacional de La Plata (CERTUNLP) por su relación con la ESPE en sus programas de maestría y doctorado.

Una forma de establecer comunicaciones con otros equipos de respuesta es mediante la publicación e intercambio de reportes de alertas e incidentes, así como de información acerca del CSIRT-ESPE, para lo cual es necesario mantener un micrositio web en donde se publique toda la información manejada por el CSIRT acerca de incidentes, alertas, vulnerabilidades y otros más.

3.12 Políticas y Procedimientos

Las políticas y procedimientos propuestos para la etapa inicial del CSIRT-ESPE son derivadas de las estrategias y los servicios que se prestarán, estos instructivos son necesarios para que empiece el funcionamiento del CSIRT, acorde a esto se elaboraron las siguientes políticas y procedimientos (Ver Anexo A: Políticas y Procedimientos):

- Política de formación y educación.

- Política de divulgación y distribución de información
- Política de manejo de incidentes.
- Procedimiento de manejo de incidentes

3.13 Estructura Organizacional

Modelo Organizacional

El modelo organizacional será el Interno Centralizado, debido a la provisión de servicios de TI que maneja la ESPE desde su matriz hacia sus diferentes sedes y extensiones. Es decir, el CSIRT-ESPE y sus recursos se ubicarán en un sitio central, recopilando información de una amplia variedad de fuentes para sintetizarla y diseminarla en toda la institución educativa. Además, el equipo mantendrá la responsabilidad en el manejo de todos los informes, análisis de incidentes y vulnerabilidades que se presenten, teniendo la autoridad para publicar advertencias, mejores prácticas, pasos de respuesta y recuperación de seguridad.

El CSIRT-ESPE centralizado propuesto trabajará estrechamente con los expertos de sistemas y plataformas de la Universidad (UTIC) según sea necesario. Al encontrarse la institución geográficamente dispersa no podría proporcionar razonablemente una respuesta a incidentes en el sitio, pero puede actuar de manera eficiente en le provisión de servicios de coordinación de respuesta de incidentes y vulnerabilidades.

Organización por procesos

La Organización por procesos del CSIRT quedaría establecida de la siguiente forma:

a) **Procesos Gobernantes**

Descripción: Asesoría y Coordinación de procesos estratégicos del CSIRT.

Responsable: Miembros del Comité de Tecnología.

Descripción: Administración y Gestión del Laboratorio, organización y control de la provisión de servicios proactivos, reactivos y gestión de calidad de seguridad.

Responsable: Director General.

b) Procesos Generadores de Valor

Descripción: Preparación, monitorización y detección de eventos de seguridad que puedan reflejar incidentes de seguridad informática.

Responsable: Monitor de redes**.**

Descripción: Preparación, análisis, manejo y prevención de incidentes de seguridad informática y vulnerabilidades.

Responsable: Analista Servicios Especiales**.**

Descripción: Planificación e investigación acerca de incidentes de seguridad de la información.

Responsable: Investigador**.**

Descripción: Preparación, ejecución talleres, cursos y tutoriales acerca de actividades principales de la seguridad de la información.

Responsable: Capacitador**.**

Descripción: Preparación, ejecución reuniones, seminarios, boletines, sitios web u otros que sensibilicen el cumplimiento de buenas prácticas de seguridad informática.

Responsable: Concientizador**.**

c) Procesos de apoyo

Descripción: Planificación, organización y control de presupuestos y financiamientos del laboratorio**.**

Responsable: Analista Administrativo Financiero**.**

Jerarquía Organizacional

Dentro de la red organizacional de la Universidad de las Fuerzas Armadas ESPE, el CSIRT es jerárquicamente dependiente del Departamento de Ciencias de la Computación con una

dependencia técnica importante del Vicerrectorado de Investigación a través de la línea jerárquica del DECC.

Se presenta a continuación la Red Organizacional de la ESPE y el organigrama del CSIRT.

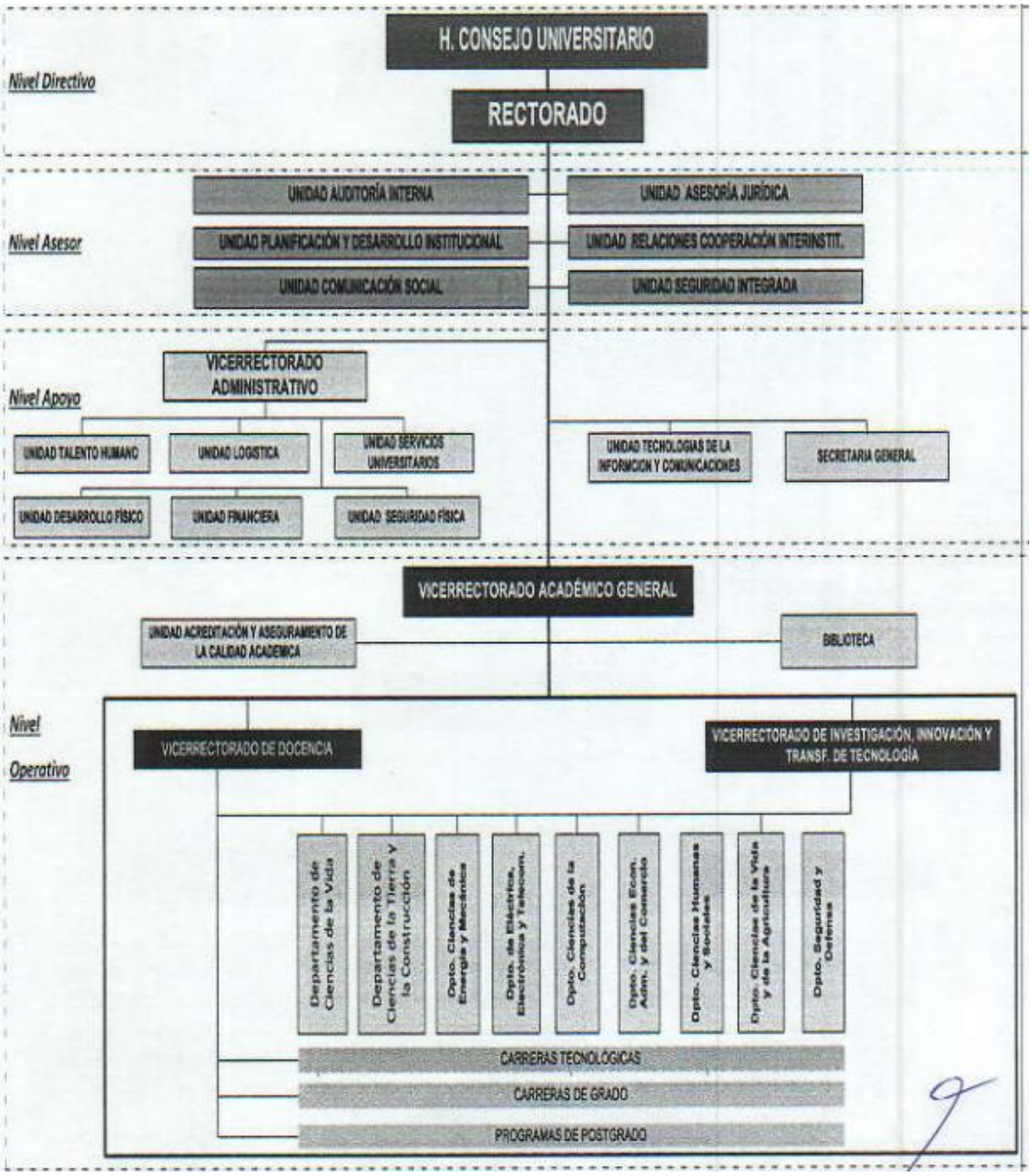

Figura 14. Red Organizacional de la ESPE
Fuente: (ESPE, 2015)

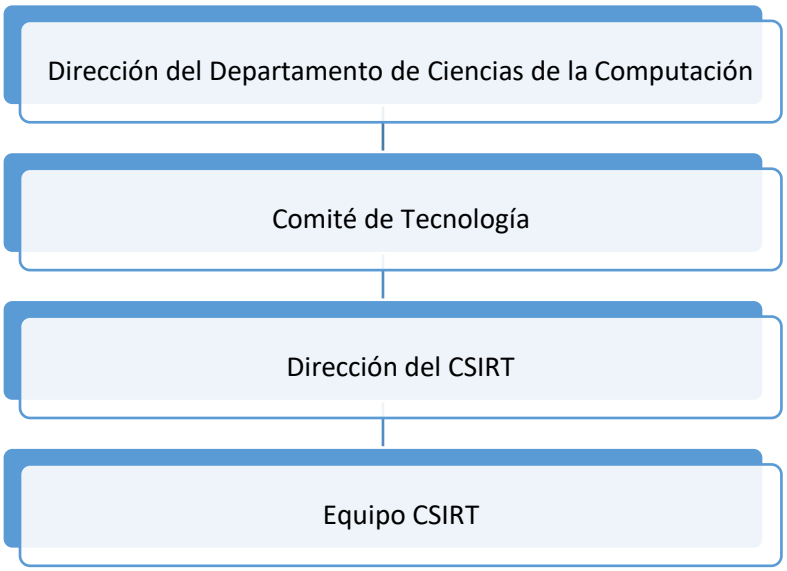

Figura 15. Propuesta Jerarquía Organizacional del CSIRT

Responsabilidades del CSIRT

- Monitorizar, analizar y dar tratamiento a incidentes y vulnerabilidades.
- Difundir información, alertas y advertencias relacionadas a la seguridad de la información.
- Brindar consultoría y asesoramiento en temáticas referidas a la seguridad de la información.
- Mantener conocimiento actualizado de implementación de procedimientos para una respuesta efectiva a incidentes.
- Mantener confidencialidad acerca de conocimientos relacionados a incidentes de seguridad.
- Interactuar con la comunidad de CSIRT Nacionales e Internacionales.

3.14 Clasificación de puestos-especificaciones de clase

El CSIRT-ESPE al tener una ubicación central se encarga de coordinar las actividades en toda la empresa. Su personal contendría probablemente las siguientes personas:

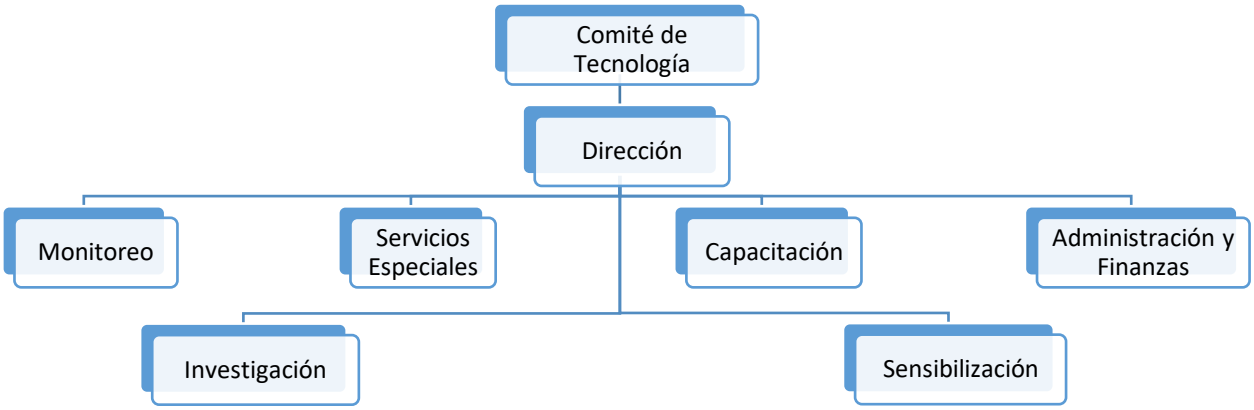

Figura 16. Propuesta Organigrama del CSIRT

Se detallan a continuación cada uno de los puestos-especificaciones de clase:

Tabla 12
Especificaciones Puesto Miembro del Comité de Tecnología

No	1
Denominación del puesto:	Miembro del Comité de Tecnología
Objetivo	Funcionar como miembro asesor y de coordinación para temas estratégicos del CSIRT.
Responsabilidades	– Asesorar la planificación del CSIRT. – Recomendar y asesorar al CSIRT en tema de políticas, lineamientos o directrices. – Valorar un reporte de riesgos. – Recomendar, asesorar y aprobar Planes correctivos/preventivos. – Recomendar prioridades para el CSIRT. – Monitorear la dirección del CSIRT.
Características del puesto	Es el responsable de asistir al CSIRT en su planeación y desarrollo.
Competencias técnicas/actitudinales	– Docente titular a tiempo completo o dedicación exclusiva. – Grado académico de Magíster en Informática o afines. – Capacidad de actuar autónomamente. – Tener iniciativa para aportar soluciones o alternativas novedosas.

CONTINÚA

	– Capacidad de comunicación efectiva. – Capacidad de relación interpersonal. – Capacidad de razonamiento y diseño para resolución de problemas. – Demostrar conocimiento y comprensión del CSIRT.
Autoridad y accesos	Para recomendar y asesorar al CSIRT.

Tabla 13
Especificaciones Puesto Director General

No	**2**
Denominación del puesto:	Director General
Objetivo	Controlar y organizar los procesos del laboratorio CSIRT.
Responsabilidades	– Planificar y organizar al equipo. – Aprobar acciones del CSIRT. – Llevar el control de avance del equipo. – Verificar el cumplimiento de las actividades programadas. – Elaborar informes y reportes periódicos – Aplicar estrategias con la aprobación de la alta gerencia. – Notificación a los administradores de unidades divisionales y funcionales.
Características del puesto	Es el responsable de la administración y gestión del laboratorio CSIRT.
Competencias técnicas/actitudinales	– Docente titular a tiempo completo o dedicación exclusiva. – Grado académico de Magíster en Informática o afines. – Capacidad de actuar autónomamente. – Tener iniciativa para aportar soluciones o alternativas novedosas. – Capacidad de comunicación efectiva. – Capacidad de relación interpersonal. – Tener motivado al equipo de trabajo. – Capacidad de razonamiento y diseño para resolución de problemas. – Demostrar conocimiento y comprensión del CSIRT
Autoridad y accesos	A toda la información del CSIRT.

Tabla 14
Especificaciones Puesto Monitor de redes

No	3
Denominación del puesto:	Monitor de redes
Objetivo	Monitorear y detectar eventos que puedan reflejar incidentes de seguridad informática.
Responsabilidades	– Realizar tareas de detección de posibles incidentes de seguridad. – Establecer procedimientos operativos para garantizar una efectiva monitorización. – Coordinar, dirigir, planear y evaluar la utilización de las herramientas de monitoreo. – Administrar y resguardar información sensible de monitoreo. – Recomendar mejoras para el proceso de monitoreo. – Recopilar, investigar y analizar nuevos desarrollos técnicos, actividades de intrusos y tendencias relacionadas para ayudar a identificar futuras amenazas. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos.
Características del puesto	Es el responsable de la monitorización de las redes de la Universidad.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de monitorización de redes. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de razonamiento, resolución y análisis
Autoridad y accesos	A toda las redes para monitorización.

Tabla 15
Especificaciones Puesto Investigador

No	4
Denominación del puesto:	Investigador
Objetivo	Realizar labores de investigación científica y tecnológica.
Responsabilidades	– Diseñar e implementar proyectos de investigación. – Fortalecer la investigación del CSIRT. – Realizar investigación para la publicación de alertas y advertencias de seguridad. – Reportar el avance de sus tareas. – Participar en evento de difusión de proyectos. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos.
Características del puesto	Es el responsable de los procesos de investigación del CSIRT.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de investigación. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Colaborar con otros grupos o investigadores.
Autoridad y accesos	A información para la mejora de la seguridad informática.

Tabla 16
Especificaciones Puesto Analista Servicios Especiales

No	5
Denominación del puesto:	Analista Servicios Especiales
Objetivo	Realizar labores de análisis de incidentes y vulnerabilidades.

CONTINÚA

Responsabilidades	– Localizar vulnerabilidades y su posible explotación. – Ejecutar análisis técnicos de hardware y software. – Ejecutar simulaciones de prueba para obtener puntos estratégicos de mejora para la seguridad. – Identificar alcance, extensión de daño, estrategias y soluciones para un incidente. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de efectuar procedimientos de análisis técnicos para incidentes y vulnerabilidades.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de análisis. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de razonamiento, resolución y análisis
Autoridad y accesos	A todos los incidentes u eventos. A hardware y software para análisis técnico. Ambientes de prueba.

Tabla 17
Especificaciones Puesto Capacitador

No	**6**
Denominación del puesto:	Capacitador
Objetivo	Proveer información acerca de actividades principales de la seguridad de la información.
Responsabilidades	– Dar capacitaciones en seguridad informática.

CONTINÚA

	– Ejecución de talleres, cursos, tutoriales. – Transmisión de pautas para la resolución de incidentes. – Recomendar mejoras para los procesos de capacitación. – Recopilar, investigar y analizar nuevos desarrollos técnicos, actividades de intrusos y tendencias relacionadas para ayudar a identificar futuras amenazas. – Llevar un control de las capacitaciones. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de brindar formación y capacitación en seguridad de la información.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de liderazgo. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de comunicación efectiva. – Capacidad de relación interpersonal.
Autoridad y accesos	A toda la información de seguridad informática, mejores prácticas de seguridad. A documentar el desempeño de los aprendices.

Tabla 18
Especificaciones Puesto Concientizador

No	7
Denominación del puesto:	Concientizador
Objetivo	Orientar el cumplimiento de buenas prácticas de seguridad informática.

CONTINÚA

Responsabilidades	– Buscar oportunidades para generar conciencia de seguridad. – Sensibilizar el cumplimiento de prácticas de seguridad. – Sensibilizar la comprensión de problemas de seguridad que puedan generarse. – Ejecutar reuniones, seminarios, boletines, sitios web u otros más. – Recopilar, investigar y analizar nuevas prácticas de seguridad de organismos internacionales. – Llevar un control de las reuniones, seminarios, otros. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de generar conciencia a quienes conforman la organización en ámbito de seguridad informática.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de sensibilización. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de comunicación efectiva. – Capacidad de relación interpersonal.
Autoridad y accesos	A toda la información de seguridad informática, mejores prácticas de seguridad. A documentar el desempeño de los sensibilizados.

Tabla 19
Especificaciones Puesto Analista Administrativo Financiero

No	**8**
Denominación del puesto:	Analista Administrativo Financiero

CONTINÚA 

Objetivo	Coordinar servicios administrativos y de apoyo logístico.
Responsabilidades	– Registrar plan de compras de bienes. – Planificar, organizar, dirigir y controlar presupuestos y financiamientos del CSIRT. – Proponer mejoras para optimizar recursos y servicios. – Establecer cronogramas de ejecución. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de apoyar en las actividades de manejo de servicios administrativos y de apoyo logístico.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad administrativa y financiera. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación.
Autoridad y accesos	A toda la información de infraestructura, equipamiento, presupuesto y financiamiento.

3.15 Infraestructura y equipamiento

a) Infraestructura del centro de datos del DECC

La infraestructura de Networking y almacenamiento de computación distribuida de alto rendimiento del Centro de datos del DECC se encuentra disponible para el uso del laboratorio CSIRT-ESPE; esta infraestructura cuenta con redes de nueva generación que incluye computación distribuida, virtualización de escritorios y servidores, para procesamiento, almacenamiento y

respaldo de datos. Este equipamiento de tecnología de avanzada, permite brindar servicios para el proceso de monitorización e investigación del equipo de respuesta.

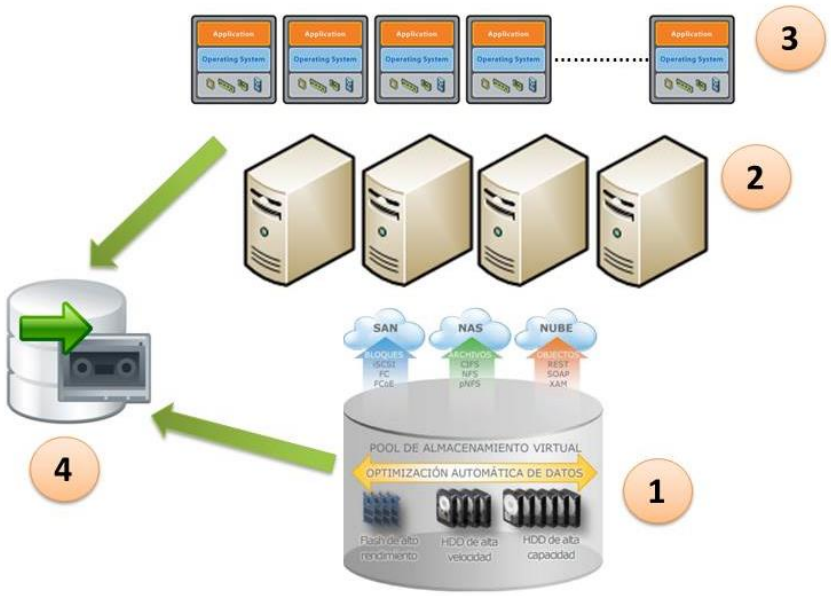

Figura 17. Centro de datos del DECC
Fuente: (Departamento de Ciencias de la Computación, 2018)

Componentes

- Sistema de almacenamiento unificado EMC VNX
- Infraestructura Blade HP, proveen 92 núcleos y 448GB de memoria como recurso de procesamiento. Además provee conectividad LAN Ethernet a 10Gbps y SAN Fibre Channel a 8Gbps.
- Hipervisor tipo 1 (bare metal), provee virtualización de servidores con características de alta disponibilidad.
- Sistema de respaldo EMC AVAMAR, es una solución integrada hardware y software para respaldo a disco.

b) Infraestructura del laboratorio CSIRT-ESPE

Infraestructura inicial

Para la provisión de los servicios básicos en la etapa inicial del CSIRT, se propone una infraestructura de red simple como se muestra en la ilustración a continuación.

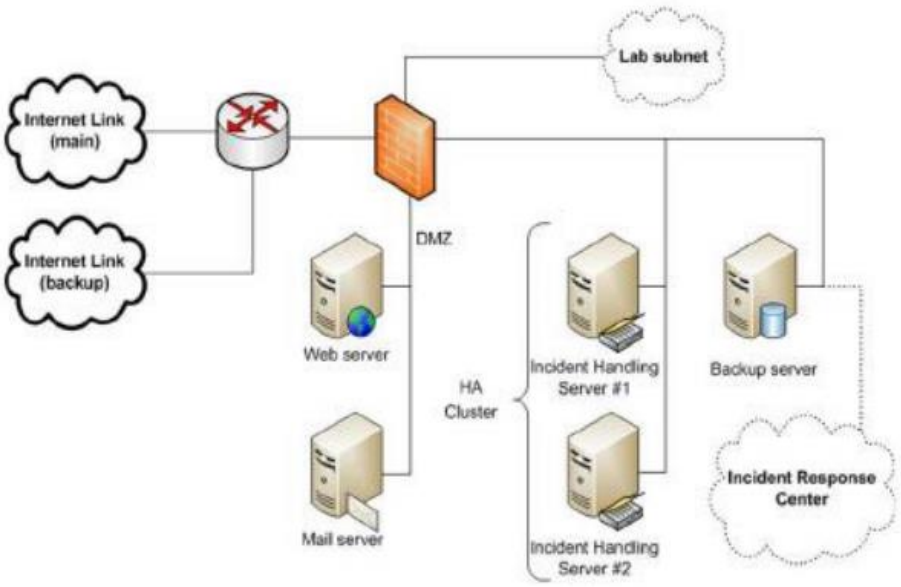

Figura 18. Infraestructura inicial
Fuente: (ENISA, 2016)

Infraestructura etapa crecimiento y desarrollo

Sin embargo, el CSIRT-ESPE en sus etapas de desarrollo y crecimiento debería ir mejorando su infraestructura de red, esto debido al incremento de recursos y personal que se estima obtener. Dado esto puede optar por una infraestructura que incluya virtualización de tecnologías como en la ilustración a continuación.

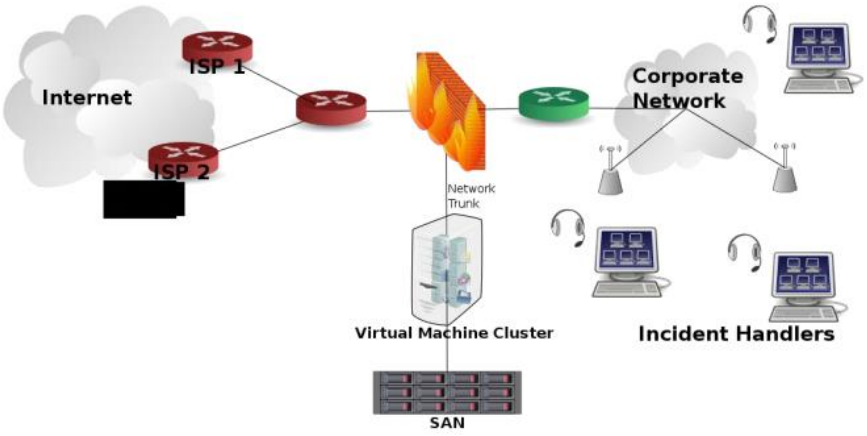

Figura 19. Infraestructura Futura
Fuente: (ENISA, 2016)

Hardware

- Servidor web
- Servidor de correo
- Servidor de manejo de incidentes (2)
- Servidor de backup
- Computadores de escritorio Dell.
- Notebook Dell
- Impresora Laser Jet

Software

De igual manera para las herramientas seleccionadas para la respuesta a incidentes informáticos del CSIRT-ESPE se escogió software de código abierto para evitar costo de adquisición.

- Software escaneo de puertos (nmap)
- Software escaneo de redes (nagios)
- Software gestión de vulnerabilidades (nessus, metasploit, kali,)
- Software detección de intrusos (snort, tripwire)
- Software seguimiento incidentes (request tracker, OTRS)

- Software almacenamiento datos (mysql)

c) Propuesta de ubicación física

El laboratorio se alojará en el aula H-402 del cuarto piso del bloque H, del departamento de Ciencias de la Computación, acondicionándolo de manera adecuada. Se escogió este lugar debido a que se encuentra protegido físicamente, con acceso independiente y monitoreo mediante cámaras de seguridad, además posee acceso a las redes de telefonía y datos y cuenta con espacio para los equipos y el personal.

3.16 Planes de seguridad, recuperación de desastres y continuidad de servicios

3.16.1 Plan de Seguridad

Los riesgos en la actualidad se presentan a todo lo relacionado con sistemas e infraestructura informática ya que la información que maneja cada organización es importante y sería un punto crítico al cual se busca cuidar y que la misma no sufra alteraciones, pérdida, o que la misma sea extraída par aun uso inadecuado sin el consentimiento la organización.

Este Plan de Seguridad es aplicable a toda la organización en su totalidad a las áreas que más están propensas a sufrir algún tipo de violación, a normas, o procesos para el manejo de la información, las políticas que se presentan en el plan su cumplimiento es de carácter obligatorio. (Ver Anexo B. Plan de Seguridad)

3.16.2 Plan de Recuperación de Desastres

Los sistemas informáticos no están libres de daños por un desastre natural, o un desastre provocado el cual llega a tener repercusiones en la organización como pérdida de datos, pérdida de información y hasta pérdida de parte o de toda su infraestructura.

El Plan de Recuperación de Desastres se centra en recuperar una parte de los procesos para que la organización siga funcionando mientras dure el desastre para que al momento de que este pase poner en marcha el plan de continuidad y así lograr obtener una recuperación total de procesos. Se debe tomar en cuenta que este plan de recuperación es importante ya que sin la debida

planificación del mismo las organizaciones no han logrado recuperarse de dichos desastres. (Ver Anexo C. Plan de Recuperación de Desastres)

3.16.3 Plan de Continuidad de Servicios

Muchas organizaciones, y empresas que no tienen recursos e infraestructura para implementar sus propios servicios en la parte informática, o ciertos procesos de seguridad que les brindara una tranquilidad que la información está respaldada, cuidada y no va a ser usada de una manera equivocada.

El CSIRT-ESPE al brindar los servicios de protección, mitigación de ataques informáticos se ve con el compromiso social de siempre mantener activos sus servidores con el fin de tener una alta disponibilidad de los mismos. Logrando así, dar un servicio de calidad, y dar la confianza a las organizaciones que dependen de estos servicios la confianza de que estarán protegidos y tendrán la información en cada momento que la necesiten.

Por tal motivo en este Plan de continuidad de Servicios se exponen las diferentes estrategias que se usan para solventar alguna caída de un servicio, que el mismo se logre recuperar en una cantidad de tiempo mínima, pero mientras transcurra esto, el servicio pueda ejecutarse de manera paralela y logrando así que los usuarios no tengan conocimiento que hubo una caída del servicio principal, ya que siempre existirá un proceso para que entre un servicio auxiliar que manejará la información hasta que se restablezca el servicio principal. (Ver Anexo D. Plan de Continuidad de Servicios)

3.17 Presupuesto y Financiamiento

Tomando en consideración que el laboratorio CSIRT-ESPE se encontrará alojado en su etapa inicial en un espacio existente, perteneciente al Departamento de Ciencias de la Computación, adecuándolo con los muebles de oficina que se posee al momento, además dentro de la adquisición de hardware y software se utilizará la infraestructura de networking y almacenamiento de alto rendimiento del Departamento de Ciencias de la Computación y se ha optado por el uso de

herramientas de código abierto que no tienen costo, a partir de esto se realizó un presupuesto referencial para la implementación del CSIRT-ESPE presentado en las tablas a continuación.

Tabla 20
Presupuesto referencial Equipos de Oficina

Equipos de oficina	Cantidad	Precio Unitario	Sub Total
Computadores de escritorio Dell	8	325	2600
Impresora multifuncional	1	650	650
Sillas	8	40	320
Escritorios de trabajo	8	150	1200
Archivadores de pared	4	75	300
Armario	1	250	250
Suministros de oficina			1200
TOTAL			6520

Tabla 21
Presupuesto referencial Hardware

Hardware	Cantidad	Precio Unitario	Sub Total
Servidores físicos			20000
Sistema de almacenamiento unificado EMC VNX	1		8000
Sistema de respaldo EMC AVAMAR	1		8000
TOTAL			36000

Tabla 22
Presupuesto referencial Servicios Básicos

Servicios Básicos	Meses	Precio Mensual	Sub Total
Luz	12	120	1440
Internet	12	120	1440
TOTAL			2880

Tabla 23
Presupuesto referencial Software

Software	Cantidad	Precio Unitario	Sub Total
NUIX	1	20000	20000
Soporte herramientas código abierto	12	200	2400
TOTAL			22400

3.18 Diseño y Cronograma de implantación del proyecto

Tabla 24
Cronograma implantación del proyecto CSIRT-ESPE

Ord	Tarea	Duración (semanas)	Inicia	Termina
1	Presentación y aprobación del proyecto	2	01/03/2018	14/10/2018
2	Comunicar la visión y plan operativo del CSIRT	1	15/10/2018	21/10/2018
3	Asignación de recursos	2	22/10/2018	04/11/2018
4	Adquisiciones, contrataciones	3	05/11/2018	25/11/2018
5	Instalación y configuraciones	2	26/11/2018	09/12/2018
6	Capacitación	2	10/12/2018	23/12/2018
7	Elaboración de pruebas	3	03/01/2019	24/01/2019
8	Establecimiento Acuerdos de Niveles de Servicio	2	25/01/2019	07/02/2019
9	Evaluación y Operación	3	08/03/2019	22/02/2019

3.19 Definición de indicadores de evaluación de la implantación del proyecto

Tabla 25
Indicadores evaluación de la implantación del proyecto CSIRT-ESPE

Metas	Resultados	Índices de medición
Creación formal del equipo CSIRT-ESPE	Equipo de respuesta conformado y establecido formalmente.	Acta de aprobación del proyecto.

CONTINÚA

Comunicar el Plan Estratégico del CSIRT	Publicación del Plan Estratégico (misión, visión, valores, objetivos estratégicos, estrategias) por medios de comunicación interna de la Universidad (correo, radio difusión, página institucional).	Cantidad de personas informadas del CSIRT. **Indicador** Número de estudiantes, docentes, investigadores y personal administrativo informados frente al número de total de estudiantes, docentes, investigadores y personal administrativo de la Universidad.
Asignación de recursos	Adecuación de las instalaciones y oficinas.	Laboratorio CSIRT proporcionado.
Adquisiciones, contrataciones	Adquisición de equipamiento presentado a los procedimientos logísticos de la Universidad.	Cantidad de equipos, materiales de oficina, hardware, software y otros entregados en relación a los requeridos.
Instalaciones y configuraciones	Instalación y configuración completada del software y hardware.	Cantidad de software y hardware instalado frente al software y hardware requerido.
Capacitación	Capacitaciones en los procesos diseñados con el personal asignado.	Actas de capacitación elaboradas.
Elaboración de pruebas	Realización de pruebas y validaciones (satisfactorias, erróneas, corregidas).	Número de pruebas satisfactorias frente al número de pruebas realizadas.
Establecimiento Acuerdos de Niveles de Servicio	Conciencia del tipo y calidad de servicios que se brindará por los representantes de la comunidad y proveedores internos, externos.	Cantidad de (SLA, OLA) firmados con los clientes.
Evaluación	Parámetros de diseño establecidos evaluados por el personal designado.	Informe de procesos.

CAPÍTULO IV
PROPUESTA PARA LA IMPLANTACIÓN DEL CSIRT-ESPE

4.1 Introducción

De acuerdo al formulario que utiliza la Universidad de las Fuerzas Armadas ESPE para la presentación de proyectos, se elaboró el proyecto definitivo para la creación del laboratorio CSIRT-ESPE con todos los elementos que ya se configuraron anteriormente. Posteriormente el documento será presentado a las autoridades respectivas de aprobación de proyectos de la Universidad, conjuntamente con una presentación que permita explicar el proyecto de una manera adecuada.

4.2 Proyecto de Creación

UNIVERSIDAD DE FUERZAS ARMADAS – ESPE

FORMULARIO DE PRESENTACIÓN DE PROYECTOS

I N F O R M A C I Ó N G E N E R A L

1. **NOMBRE DEL PROYECTO:**

   Creación del Laboratorio CSIRT-ESPE (LABCSIRT).

2. **FECHA:** 09 de Agosto del 2018
3. **ÁREA DE GESTIÓN ESTRATÉGICA:** Seguridad de la información
4. **OBJETIVO ESTRATÉGICO**

   O3: Incrementar la producción científica, académica y tecnológica de calidad, con énfasis en el ámbito de la seguridad y la defensa.

5. **ESTRATEGIA:**

   E3. Fortaleciendo los centros de investigación tecnológica aplicada a la industria de la defensa.

6. **UNIDADES RESPONSABLES:**

   Departamento de Ciencias de la Computación (DECC)

7. **RESPONSABLE DEL PROYECTO:**

   Ing. Mario B. Ron Egas – Docente Tiempo Completo DECC

I N F O R M A C I Ó N E S P E C Í F I C A

8. **PERFIL DEL PROYECTO ELABORADO POR:**

   Ing. Mario B. Ron Egas – Docente Tiempo Completo DECC

9. **PERSONAL COLABORADOR:**

   Docentes investigadores y estudiantes del DECC

10. **LOCALIZACIÓN GEOGRÁFICA:**

    Universidad de las Fuerzas Armas ESPE – Campus Sangolquí

11. **ÁREA DE INFLUENCIA:**

    Nivel nacional e internacional

12. ANTECEDENTES

Con la expansión de los servicios digitales, cada vez más organizaciones requieren de un acceso permanente y su infraestructura crítica depende de las posibilidades que tienen sus usuarios para acceder a internet (Van der Heide, 2017). En consecuencia, los procesos y actividades fundamentales de las empresas para proporcionar sus servicios se han vuelto dependientes de su conectividad digital; una interrupción en ella puede provocar grandes pérdidas económicas. Las actividades maliciosas asociadas a la tecnología se han incrementado y son la principal causa de gastos realizados para su contención, resolución y daños potenciales, sin considerar el lucro cesante al interrumpir los servicios a los clientes. En la actualidad, cada vez que ocurre un incidente de seguridad en la información, la rápida y eficaz respuesta es clave. Por tal motivo entran en contexto los CSIRT, un equipo de expertos de seguridad de TI que dan respuesta a incidentes o amenazas de seguridad de la información, que poseen el conocimiento y capacidad para detectar y manejar los incidentes, que ayudan a mitigar las vulnerabilidades y los riesgos que podrían presentarse.

Los ataques suceden, aunque no se desee que ocurran, los atacantes por lo general son oportunistas, sin importar el tamaño de la organización o la importancia del negocio. Una vez realizado el ataque se debe reaccionar rápidamente para controlar el daño actual y evitar posibles daños futuros. Existen varios nombres con los que se dan a conocer los equipos de respuesta ante incidentes informáticos (Rajnovic, 2011), entre ellos están: CERT (Equipo Respuesta a Emergencias Informáticas), CIRT (Equipo de Respuesta a Incidentes Informáticos), IRT (Equipo de Respuesta a Incidentes), ERT (Equipo de Respuesta a Emergencias), CSIRT (Equipo de Respuesta a Indicentes de Seguridad Informática), SIRT(Equipo de Respuesta a Indicentes de Seguridad), SERT (Equipo de Respuesta a Emergencias de Seguridad).

De acuerdo con (Ron Egas, Vásquez Cañas, Lanfranco, Macía, & Díaz , 2017) en varios países latinoamericanos se han implementado CSIRT Nacionales para dar atención a requerimientos de seguridad en organismos del estado. Sin embargo, no han proporcionado el resultado que se esperaba, en muchos casos por falta de formación técnica o recursos, lo que ha llevado a varias Universidades de la región a tomar conciencia de la no existencia de mecanismos adecuados que permitan proteger la información, especialmente de sus sistemas

más críticos. En cada país de la región apenas una o dos Universidades han creado CSIRTs Académicos de forma efectiva, propiciando el uso de las buenas prácticas de seguridad y la formación de un personal idóneo que fortalezca las unidades de seguridad de la información.

13. PROYECTOS RELACIONADOS

- Creación del grupo de investigación en Seguridad de la Información y Auditoría.
- Creación del Laboratorio de Investigación de Seguridad de la Información y Auditoría de Sistemas Tecnológicos (LABSIA).

14. JUSTIFICACIÓN E IMPORTANCIA

La Universidad de las Fuerzas Armadas ESPE brinda diferentes servicios a los estudiantes y público en general en su mayor parte mediante la Internet, mediante procesos y operaciones que tienen un grado de importancia para el adecuado funcionamiento de la Universidad. Los avances tecnológicos y principalmente el crecimiento de la Internet han generado que la ESPE tenga cierto nivel riesgo ante incidentes informáticos debido a un mal manejo de los recursos o por actividades externas maliciosas.

De acuerdo a la problemática actual de la Universidad no existe un grupo que se encargue de emitir alertas o de dar un tratamiento adecuado de los incidentes de seguridad informática, es decir no se tiene un área formalmente establecida en donde se pueda reportar estos incidentes y darles un seguimiento apropiado.

Ante estas situaciones resulta primordial la creación de un grupo de respuesta que cumpla actividades proactivas y reactivas que permitan estar preparados para una adecuada mitigación de los daños de un posible incidente informático que se pueda ocasionar, con el apoyo de reportes emitidos por CSIRTs Nacionales e investigaciones propias que contribuyan una mejora en la seguridad de los sistemas de información de la ESPE.

15. DISEÑO ORGANIZACIONAL DEL LABORATORIO.

a. Direccionamiento Estratégico.

1) VISION

Brindar servicios que permitan identificar y mitigar ataques al sistema de información de la Universidad de las Fuerzas Armadas ESPE, coadyuvar en la capacitación y formación de personal especializado en respuesta a incidentes informáticos de entidades públicas y privadas.

2) MISION

Consolidar al CSIRT-ESPE como un equipo de respuesta ante incidentes informáticos en el país.

3) OBJETIVOS.

OE1- Incrementar e innovar los servicios de respuesta ante incidentes informáticos, para una comunidad creciente.

OE2- Brindar servicios de respuesta ante incidentes informáticos con procesos certificados internacionalmente.

OE3- Incrementar el aporte financiero de la comunidad y los recursos para el desarrollo y crecimiento del CSIRT.

OE4- Incrementar los recursos disponibles tanto humanos como materiales y equipos, para brindar un servicio de calidad.

4) PROYECTOS DE INVESTIGACIÓN

El Laboratorio CSIRT-ESPE, se encuentra en capacidad de realizar investigación, innovación y desarrollo en las siguientes áreas en forma inicial y no exclusiva, sin deslindar su cobertura a otras relacionadas que se presenten en el futuro:

Seguridad de la Información y Comunicaciones:

- Alertas y advertencias reactivas ante ataques informáticos, vulnerabilidades de seguridad.
- Manejo de incidentes (Análisis, clasificación y respuesta).
- Manejo de vulnerabilidades (Análisis, clasificación y respuesta).

- Anuncios proactivos (alertas de intrusión, advertencias de vulnerabilidad, avisos de seguridad).
- Difusión de información relacionada con la seguridad (Documentos de alertas, advertencias, archivos de mejores prácticas, orientación en seguridad informática, estadísticas actuales y tendencias de incidentes informáticos).
- Concientización en seguridad de la información.
- Educación/Capacitación en seguridad de la información
- Políticas de Seguridad,
- Seguridad en bases de datos,
- Seguridad en redes y comunicaciones,
- Ciber defensa.
- Seguridad en sistemas financieros.

b. <u>Estructura Organizacional:</u>

1) RESPONSABILIDADES GENERALES DEL LABORATORIO.

Se establecen como responsabilidades generales del LABCSIRT:

- Monitorizar, analizar y dar tratamiento a incidentes y vulnerabilidades.
- Difundir información, alertas y advertencias relacionadas a la seguridad de la información.
- Brindar consultoría y asesoramiento en temáticas referidas a la seguridad de la información.
- Mantener conocimiento actualizado de implementación de procedimientos para una respuesta efectiva a incidentes.
- Mantener confidencialidad acerca de conocimientos relacionados a incidentes de seguridad.
- Interactuar con la comunidad de CSIRT Nacionales e Internacionales.

2) ORGANIGRAMA ESTRUCTURAL Y JERARQUÍA ORGANIZACIONAL.

Dentro de la Red Organizacional de la Universidad de las Fuerzas Armadas ESPE, el LABCSIRT, es jerárquicamente dependiente del Departamento de Ciencias de la Computación con una dependencia técnica importante del Vicerrectorado de Investigación a través de la línea jerárquica del DECC.

Se presenta a continuación la Red Organizacional de la ESPE y el Organigrama Estructural del Laboratorio, dependiente de la Dirección del Departamento de Ciencias de la Computación.

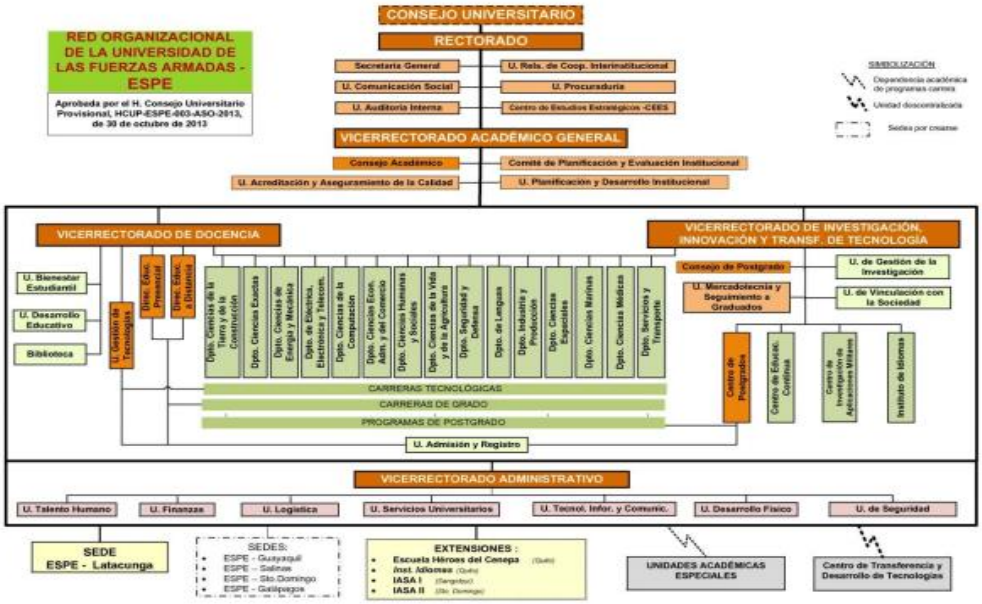

Figura 20. Red Organizacional de la ESPE
Fuente: (ESPE, 2015)

Figura 21. Propuesta Organigrama del CSIRT

3) ORGANIZACIÓN POR PROCESOS

Procesos Gobernantes

Descripción: Asesoría y Coordinación de procesos estratégicos del CSIRT.

Responsable: Miembros del Comité de Tecnología.

Descripción: Administración y Gestión del Laboratorio, organización y control de la provisión de servicios proactivos, reactivos y gestión de calidad de seguridad.

Responsable: Director General.

Procesos Generadores de Valor

Descripción: Preparación, monitorización y detección de eventos de seguridad que puedan reflejar incidentes de seguridad informática.

Responsable: Monitor de redes**.**

Descripción: Preparación, análisis, manejo y prevención de incidentes de seguridad informática y vulnerabilidades.

Responsable: Analista Servicios Especiales**.**

Descripción: Planificación e investigación acerca de incidentes de seguridad de la información.

Responsable: Investigador**.**

Descripción: Preparación, ejecución talleres, cursos y tutoriales acerca de actividades principales de la seguridad de la información.

Responsable: Capacitador**.**

Descripción: Preparación, ejecución reuniones, seminarios, boletines, sitios web u otros que sensibilicen el cumplimiento de buenas prácticas de seguridad informática.

Responsable: Concientizador**.**

Procesos de apoyo

Descripción: Planificación, organización y control de presupuestos y financiamientos del laboratorio**.**

Responsable: Analista Administrativo Financiero**.**

4) DESCRIPCIÓN DE CARGOS

a) ***Miembro del Comité de Tecnología***

Tabla 26
Especificaciones Puesto Miembro del Comité de Tecnología

No	1
Denominación del puesto:	Miembro del Comité de Tecnología
Objetivo	Funcionar como miembro asesor y de coordinación para temas estratégicos del CSIRT.
Responsabilidades	– Asesorar la planificación del CSIRT. – Recomendar y asesorar al CSIRT en tema de políticas, lineamientos o directrices. – Valorar un reporte de riesgos. – Recomendar, asesorar y aprobar Planes correctivos/preventivos. – Recomendar prioridades para el CSIRT. – Monitorear la dirección del CSIRT.
Características del puesto	Es el responsable de asistir al CSIRT en su planeación y desarrollo.
Competencias técnicas/actitudinales	– Docente titular a tiempo completo o dedicación exclusiva. – Grado académico de Magíster en Informática o afines. – Capacidad de actuar autónomamente. – Tener iniciativa para aportar soluciones o alternativas novedosas. – Capacidad de comunicación efectiva. – Capacidad de relación interpersonal. – Capacidad de razonamiento y diseño para resolución de problemas. – Demostrar conocimiento y comprensión del CSIRT.
Autoridad y accesos	Para recomendar y asesorar al CSIRT.

b) ***Director General del Laboratorio***

Tabla 27
Especificaciones Puesto Director General

No	2
Denominación del puesto:	Director General
Objetivo	Controlar y organizar los procesos del laboratorio CSIRT.
Responsabilidades	– Planificar y organizar al equipo. – Aprobar acciones del CSIRT. – Llevar el control de avance del equipo. – Verificar el cumplimiento de las actividades programadas. – Elaborar informes y reportes periódicos – Aplicar estrategias con la aprobación de la alta gerencia. – Notificación a los administradores de unidades divisionales y funcionales.
Características del puesto	Es el responsable de la administración y gestión del laboratorio CSIRT.
Competencias técnicas/actitudinales	– Docente titular a tiempo completo o dedicación exclusiva. – Grado académico de Magíster en Informática o afines. – Capacidad de actuar autónomamente. – Tener iniciativa para aportar soluciones o alternativas novedosas. – Capacidad de comunicación efectiva. – Capacidad de relación interpersonal. – Tener motivado al equipo de trabajo. – Capacidad de razonamiento y diseño para resolución de problemas. – Demostrar conocimiento y comprensión del CSIRT
Autoridad y accesos	A toda la información del CSIRT.

c) Monitor de redes

Tabla 28
Especificaciones Puesto Monitor de redes

No	3
Denominación del puesto:	Monitor de redes
Objetivo	Monitorear y detectar eventos que puedan reflejar incidentes de seguridad informática.
Responsabilidades	– Realizar tareas de detección de posibles incidentes de seguridad. – Establecer procedimientos operativos para garantizar una efectiva monitorización. – Coordinar, dirigir, planear y evaluar la utilización de las herramientas de monitoreo. – Administrar y resguardar información sensible de monitoreo. – Recomendar mejoras para el proceso de monitoreo. – Recopilar, investigar y analizar nuevos desarrollos técnicos, actividades de intrusos y tendencias relacionadas para ayudar a identificar futuras amenazas. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos.
Características del puesto	Es el responsable de la monitorización de las redes de la Universidad.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de monitorización de redes. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Tener motivación. – Capacidad de razonamiento, resolución y análisis
Autoridad y accesos	A toda las redes para monitorización.

d) Investigador

Tabla 29
Especificaciones Puesto Investigador

No	4
Denominación del puesto:	Investigador
Objetivo	Realizar labores de investigación científica y tecnológica.
Responsabilidades	– Diseñar e implementar proyectos de investigación. – Fortalecer la investigación del CSIRT. – Realizar investigación para la publicación de alertas y advertencias de seguridad. – Reportar el avance de sus tareas. – Participar en evento de difusión de proyectos. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos.
Características del puesto	Es el responsable de los procesos de investigación del CSIRT.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de investigación. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Colaborar con otros grupos o investigadores.
Autoridad y accesos	A información para la mejora de la seguridad informática.

e) Analista Servicios Especiales

Tabla 30
Especificaciones Puesto Analista Servicios Especiales

No	5
Denominación del puesto:	Analista Servicios Especiales
Objetivo	Realizar labores de análisis de incidentes y vulnerabilidades.
Responsabilidades	– Localizar vulnerabilidades y su posible explotación. – Ejecutar análisis técnicos de hardware y software. – Ejecutar simulaciones de prueba para obtener puntos estratégicos de mejora para la seguridad. – Identificar alcance, extensión de daño, estrategias y soluciones para un incidente. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de efectuar procedimientos de análisis técnicos para incidentes y vulnerabilidades.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de análisis. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de razonamiento, resolución y análisis
Autoridad y accesos	A todos los incidentes u eventos. A hardware y software para análisis técnico. Ambientes de prueba.

f) Capacitador

Tabla 31
Especificaciones Puesto Capacitador

No	6
Denominación del puesto:	Capacitador
Objetivo	Proveer información acerca de actividades principales de la seguridad de la información.
Responsabilidades	– Dar capacitaciones en seguridad informática. – Ejecución de talleres, cursos, tutoriales. – Transmisión de pautas para la resolución de incidentes. – Recomendar mejoras para los procesos de capacitación. – Recopilar, investigar y analizar nuevos desarrollos técnicos, actividades de intrusos y tendencias relacionadas para ayudar a identificar futuras amenazas. – Llevar un control de las capacitaciones. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de brindar formación y capacitación en seguridad de la información.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de liderazgo. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de relación interpersonal.
Autoridad y accesos	A toda la información de seguridad informática, mejores prácticas de seguridad. A documentar el desempeño de los aprendices.

g) Concientizador

Tabla 32
Especificaciones Puesto Concientizador

No	7
Denominación del puesto:	Concientizador
Objetivo	Orientar el cumplimiento de buenas prácticas de seguridad informática.
Responsabilidades	– Buscar oportunidades para generar conciencia de seguridad. – Sensibilizar el cumplimiento de prácticas de seguridad. – Sensibilizar la comprensión de problemas de seguridad que puedan generarse. – Ejecutar reuniones, seminarios, boletines, sitios web u otros más. – Recopilar, investigar y analizar nuevas prácticas de seguridad de organismos internacionales. – Llevar un control de las reuniones, seminarios, otros. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de generar conciencia a quienes conforman la organización en ámbito de seguridad informática.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad de sensibilización. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación. – Capacidad de comunicación efectiva. – Capacidad de relación interpersonal.
Autoridad y accesos	A toda la información de seguridad informática, mejores prácticas de seguridad. A documentar el desempeño de los sensibilizados.

h) ***Analista Administrativo Financiero***

Tabla 33
Especificaciones Puesto Analista Administrativo Financiero

No	8
Denominación del puesto:	Analista Administrativo Financiero
Objetivo	Coordinar servicios administrativos y de apoyo logístico.
Responsabilidades	– Registrar plan de compras de bienes. – Planificar, organizar, dirigir y controlar presupuestos y financiamientos del CSIRT. – Proponer mejoras para optimizar recursos y servicios. – Establecer cronogramas de ejecución. – Reportar el avance de sus tareas. – Cumplir con las actividades programadas. – Elaborar informes y reportes periódicos
Características del puesto	Es el responsable de apoyar en las actividades de manejo de servicios administrativos y de apoyo logístico.
Competencias técnicas/actitudinales	– Docente, profesional o estudiante. – Experiencia y formación en el área. – Tener iniciativa y ser resolutivo. – Capacidad administrativa y financiera. – Actuar con responsabilidad y ética profesional. – Capacidad de integrarse rápidamente. – Trabajo en equipo. – Poseer habilidades de aprendizaje. – Tener motivación.
Autoridad y accesos	A toda la información de infraestructura, equipamiento, presupuesto y financiamiento.

5) IMPACTO EN LA MASA SALARIAL Y PRESUPUESTO DE PERSONAL

a) ***Análisis legal***

Los participantes para el laboratorio CSIRT-ESPE forman parte del Departamento de Ciencias de la Computación, con relación de dependencia con la Universidad de las Fuerzas Armadas requieren una designación formal o contrato para el cargo.

b) ***Análisis técnico***

No aplica.

6) RECURSOS TECNOLÓGICOS REQUERIDOS.

a) ***Infraestructura del Centro de Datos del DECC.***

La infraestructura de Networking y almacenamiento de computación distribuida de alto rendimiento del Centro de datos del DECC se encuentra disponible para el uso del laboratorio CSIRT-ESPE; esta infraestructura cuenta con redes de nueva generación que incluye computación distribuida, virtualización de escritorios y servidores, para procesamiento, almacenamiento y respaldo de datos. Este equipamiento de tecnología de avanzada, permite brindar servicios para el proceso de monitorización e investigación del equipo de respuesta.

CENTRO DE DATOS DEL DECC

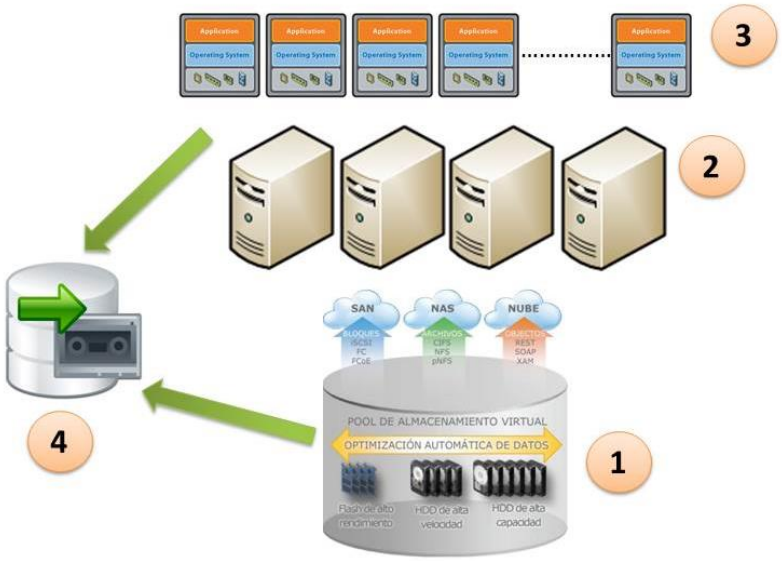

Figura 22. Centro de datos del DECC
Fuente: (Departamento de Ciencias de la Computación, 2018)

Componentes:

(1) Sistema de almacenamiento unificado EMC VNX, permite que clientes Windows, Linux y UNIX compartan archivos en ambientes multiprotocolo (NFS y CIFS). Además, es compatible con acceso iSCSI, Fibre Channel y FCoE para aplicaciones en bloque, vulnerables a la latencia y de gran ancho de banda.

(2) Infraestructura Blade HP, conformada por servidores de mediana altura y altura completa, proveen 92 núcleos y 448GB de memoria como recurso de procesamiento. Además provee conectividad LAN Ethernet a 10Gbps y SAN Fibre Channel a 8Gbps.

(3) Hipervisor tipo 1 (bare metal), provee virtualización de servidores con características de alta disponibilidad.

(4) Sistema de respaldo EMC AVAMAR, es una solución integrada hardware y software para respaldo a disco. Duplica los datos en origen para optimizar el espacio en disco y la red de datos (LAN y WAN). Permite sacar respaldos completos todo el tiempo porque no duplica la información respaldada anteriormente.

b) ***Infraestructura del Laboratorio LABCSIRT:***

(1) *Hardware*

- Servidor web
- Servidor de correo
- Servidor de manejo de incidentes (2)
- Servidor de backup
- Computadores de escritorio Dell.
- Notebook Dell
- Impresora Laser Jet

(2) *Software*

- Software escaneo de puertos (nmap)
- Software escaneo de redes (nagios)
- Software gestión de vulnerabilidades (nessus, metasploit, kali,)
- Software detección de intrusos (snort, tripwire)
- Software seguimiento incidentes (request tracker, OTRS)
- Software almacenamiento datos (mysql)

c) ***Propuesta de ubicación física***

El laboratorio se alojará en el aula H-402 del cuarto piso del bloque H, del departamento de Ciencias de la Computación, acondicionándolo de manera adecuada. Se escogió este lugar debido a que se encuentra protegido físicamente, con acceso independiente y monitoreo mediante cámaras de seguridad, además posee acceso a las redes de telefonía y datos y cuenta con espacio para los equipos y el personal, posteriormente se trasladará al Centro de Investigaciones y posgrado

7) PRESUPUESTO DE GASTO CORRIENTE E INVERSIÓN PARA LA UNIDAD

No aplica a la creación de este laboratorio.

8) DISPONIBILIDAD PRESUPUESTARIA

No aplica a la creación de este laboratorio.

9) PROPUESTA DE REFORMAS A LA REGLAMENTACIÓN DE LA UNIVERSIDAD

No aplica a la creación de este laboratorio.

16. CRONOGRAMA DE IMPLANTACIÓN DEL LABORATORIO

Tabla 34

Cronograma implantación del proyecto CSIRT-ESPE

Ord	Tarea	Duración (semanas)	Inicia	Termina
1	Presentación y aprobación del proyecto	2	01/03/2018	14/10/2018
2	Comunicar la visión y plan operativo del CSIRT	1	15/10/2018	21/10/2018
3	Asignación de recursos	2	22/10/2018	04/11/2018
4	Adquisiciones, contrataciones	3	05/11/2018	25/11/2018
5	Instalación y configuraciones	2	26/11/2018	09/12/2018
6	Capacitación	2	10/12/2018	23/12/2018
7	Elaboración de pruebas	3	03/01/2019	24/01/2019
8	Establecimiento Acuerdos de Niveles de Servicio	2	25/01/2019	07/02/2019
9	Evaluación y Operación	3	08/03/2019	22/02/2019

17. MATRIZ DE RIESGOS DEL PROYECTO

Tabla 35

Matriz riesgos implantación del proyecto CSIRT-ESPE

IDENTIFICACIÓN Y GERENCIA DE LOS RIESGOS						
ORD	**ACTIVIDADES PROYECTO**	**RIESGO**	**PROBAB. RIESGO**	**PRIORIDAD RIESGO**	**ESTRATEGIA A SER IMPLEMENTADA**	**PRESUPUESTO**
1	Aprobaciones formales	No aprobación del proyecto	10%	6	Explicar el proyecto	0,00
2	Nombramiento personal adscrito.	Nombramiento no adecuado	10%	5	Demostrar y explicar alternativas	0,00
3	Adecuación física de mobiliario	Falta de mobiliario	20%	2	Realizar adquisición	8.000,00
4	Instalación de Hardware	Fallas en el Hardware	10%	4	Realizar mantenimiento	400,00
5	Instalación de Software	Licencias no actualizadas	30%	1	Pago de licencias	4.000,00
6	Inicio de actividades.	Retraso actividades previas	20%	3	Readecuar actividades	0,00
	TOTAL		100%			12.400,00

18. BIBLIOGRAFÍA

- Andrade, R., & Fuertes, W. (2013). Diseño y dimensionamiento de un equipo de un equipo de respuesta ante incidentes de seguridad informática (CSIRT). Caso de estudio: ESPE. Congreso de ciencia y tecnología de la ESPE, 9.
- Fuertes, W., Reyes, F., Valladares, P., Tapia, F., Toulkeridis, T., & Pérez, E. (2017). An Integral Model to Provide Reactive and Proactive Services in an Academic CSIRT Based on Business Intelligence. Systems (ISSN 2079-8954) is an international open access journal on systems engineering and systems management, published quarterly online by MDPI. , 20.
- Google. (2018). Google Drive. Recuperado el 08 de Marzo de 2018, de https://www.google.com/intl/es_ALL/drive/using-drive/
- Latorre, A. (2003). Investigación Acción. Graó.
- Microsoft. (2018). Microsoft Word. Recuperado el 08 de Marzo de 2018, de https://products.office.com/es/word
- Murillo, W. (2008). La investigación científica. Recuperado el 08 de Marzo de 2018, de http//www.monografias.com/trabajos15/invest-científica/investcientífica.shtm
- Rajnovic, D. (2011). Computer Incident Response and Product Security. Indianapolis, IN 46240: Cisco Systems Inc.
- Ron Egas, M., Vásquez Cañas, R., Lanfranco, E., Macía, N., & Díaz , J. (2017). Practical Guide To Implement An Academic Computing Security Incident Response Team (Academic CSIRT).
- van der Heide, M. (2017). Establishing a CSIRT. Forum of Incident Response and Security Teams (FIRST).
- Vargas Codero, Z. R. (2009). LA INVESTIGACIÓN APLICADA: UNA FORMA DE CONOCER LAS REALIDADES CON EVIDENCIA CIENTÍFICA. Educación 33(1), 155-165.
- Wara, Y. M., & Singh, D. (2015). A guide to establishing computer security incident response team (CSIRT) for national research and education network (NREN). African Journal of Computing & ICT, 8(2), 1-8.

19. RESPONSABILIDADES

Tabla 36
Firma responsabilidades del proyecto CSIRT-ESPE

R E S P O N S A B I L I D A D E S	
ELABORADO: NOMBRE: ING. MARIO B. RON E. MSc FUNCIÓN: DOCENTE FECHA: 09-AGO-2018	REVISADO: NOMBRE: FUNCIÓN: DOCENTE FECHA: 09-AGO-2018
REVISADO: NOMBRE: FUNCIÓN: DIRECTOR DECC FECHA: 09-AGO-2018	REVISADO: NOMBRE: FUNCIÓN: VICERECTOR INVESTIGACIÓN FECHA: 09-AGO-2018
APROBADO: NOMBRE: FUNCIÓN: VICERRECTOR GENERAL DE LA ESPE FECHA: 09-AGO-2018	
AUTORIZADO: NOMBRE: FUNCIÓN: RECTOR DE LA ESPE FECHA: 09-AGO-2018	

CAPÍTULO V
CONCLUSIONES Y RECOMENDACIONES

5.1 Introducción

En este capítulo se exponen las conclusiones y recomendaciones procedentes de la información presentada en los capítulos anteriores del documento. El contenido expone criterios acerca de la importancia de los CSIRT Académicos y de la implantación de una solución progresiva, eficiente y eficaz en la comunidad universitaria. Posteriormente continúa con ideas clave que colaborarían al fortalecimiento de la implantación del proyecto del laboratorio CSIRT-ESPE en la Universidad.

5.2 Conclusiones

Debido al desarrollo tecnológico constante en las actividades de la sociedad, resulta primordial asegurar el uso adecuado de los sistemas de información y garantizar su seguridad mediante la implementación de mecanismos adecuados.

Es importante la concordancia del Plan Estratégico del CSIRT que constituye la hoja de ruta para alcanzar sus propósitos y objetivos, con el Plan Estratégico de la Universidad y el de la Unidad de Tecnologías de la Información y Comunicación, para mantener así una adecuada ejecución de sus procesos y procedimientos.

La implementación de un CSIRT académico completo y robusto requiere de una alta inversión que resulta difícil de aprobar por una institución académica pública, debido a la infraestructura y equipamiento necesario para su operación. Sin embargo, plantear una solución inicial que reutilice componentes, herramientas y personal que ya posee la Universidad conjuntamente con una solución futura que se desarrollará y obtendrá progresivamente resulta positivo para la aprobación de la comisión de proyectos.

El establecimiento de relaciones con otras organizaciones o entidades resulta fundamental para la generación de alianzas estratégicas y políticas que permitan mejorar los procedimientos del CSIRT académico.

5.3 Recomendaciones

Establecer reuniones con las partes interesadas de la Universidad y otras relacionadas que tienen interés en el proyecto, para recibir observaciones en el diseño elaborado para el CSIRT académico.

Como parte de la contribución que mantienen los CSIRT académicos no solo se debe tomar en cuenta la prestación de servicios de respuesta a incidentes informáticos en las instituciones académicas, sino también la generación y difusión de conocimiento en ámbitos de seguridad informática

Se recomienda realizar capacitaciones continuas al personal asignado para el CSIRT académico para la mejora de los procesos diseñados.

Se puede contar con la presencia de expertos de otros CSIRT académicos al momento de realizar las actividades de prueba y validación en la fase de implantación del proyecto.

Se recomienda crear capacitaciones relacionadas al uso adecuado de los sistemas de información para la comunidad universitaria de la Universidad de las Fuerzas Armadas ESPE, mejorando así sus conocimientos, habilidades y actitudes para una disminución de incidentes de seguridad informática.

5.4 Bibliografía

Asia Pacific Computer Emergency Response Team. (2018). *APCERT*. Recuperado el 17 de Agosto de 2018, de www.apcert.org

Banco Interamericano de Desarrollo (BID), & Organización de los Estados Americanos. (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe?* .

Bronk, H., Thorbruegge, M., & Hakkaja, M. (2006). *A Step by step approach on how to set up a CSIRT.* European Union: ENISA.

Campbell, T. (Marzo de 2003). An Introduction to the Computer Security Incident Response Team (CSIRT) Set-Up and Operational Considerations.

Carozo, E., Martinez, C., & Vidal, L. (2008). *Análisis del Desarrollo de un Centro de Respuesta Nacional para la.* Montevideo.

Centro Criptológico Nacional (CCN Cert) y TB-Security. (2011). *Guía de creación de un CERT/CSIRT.* Madrid: Secretaría General Técnica España.

ENISA. (2006). *European Union Agency for Network and Information Security.* Recuperado el 17 de Julio de 2018, de https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

ENISA. (2016). *Developing CSIRT Infraestructure.* Recuperado el 05 de Agosto de 2018, de https://www.enisa.europa.eu/topics/trainings-for-cybersecurity-specialists/online-training-material/documents/2016-resources/developing_csirt_infrastructure-toolset

ESPE. (2015). *Reglamento Orgánico de Gestion Organizacional por procesos de la ESPE, codificado.*

ESPE. (2018). *Plan Estratégico de Desarrollo Institucional.* Sangolquí.

FIRST. (2018). Recuperado el 05 de Agosto de 2018, de https://www.first.org/members

Killcrece, G. (2003). Organizational Models for Computer Security Incident Response Teams (CSIRTs). En G. Killcrece, *Organizational Models for Computer Security Incident Response Teams (CSIRTs)* (pág. 158). Handbook CMU/SEI-2003-HB-001.

OGC. (2007). *ITIL Version 3 Service Design.* TSO.

OGC. (2007). *ITIL Version 3 Service Transition.* TSO.

OGC. (2011). *ITIL Version 3 Service Strategy.* Londres: TSO.

Quiñonez, F. (2015). Recuperado el 31 de Julio de 2018, de http://faquinones.com/gestiondeserviciosit/itilv3/index.htm

Rajnovic, D. (2011). *Computer Incident Response and Product Security*. Indianapolis, IN 46240: Cisco Systems Inc.

Ron Egas, M., Vásquez Cañas, R., Lanfranco, E., Macía, N., & Díaz , J. (2017). Practical Guide To Implement An Academic Computing Security Incident Response Team (Academic CSIRT).

UTIC ESPE. (2015). *Plan Estratégico de Tecnologías de la Información y Comunicaciones.*

van der Heide, M. (2017). *Establishing a CSIRT*. Thailand: Thailand Computer Emergency Response Team.

West-Brown, M. J., Stikvoort, D., Kossakowski, K.-P., Killcrece, G., Ruefle, R., & Zajicek, M. (Abril de 2003). Handbook for Computer Security Incident Response Teams (CSIRTs).