# UNIVERSIDAD NACIONAL DE CHIMBORAZO

## FACULTAD DE INGENIERÍA

### CARRERA DE INGENIERÍA EN SISTEMAS Y COMPUTACIÓN

"Proyecto de Investigación previo a la obtención de título de Ingeniera en Sistemas y Computación"

**TRABAJO DE TITULACIÓN**

# ANÁLISIS DE LAS METODOLOGÍAS ENISA Y APCERT PARA LA CREACIÓN DEL CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS (CSIRT). CASO PRÁCTICO: PROTOTIPO DE UN CSIRT EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO


**Autor:**

Mónica Estefanía Chacha Chunata

**Tutor:**

Ing. Lorena Paulina Molina Valdiviezo, Ph.D.


**Riobamba - Ecuador**

**2019**

Los miembros del Tribunal de Graduación del proyecto de investigación de titulo: **Análisis de las Metodologías ENISA y APCERT para la creación del Centro de Respuesta a Incidentes Informáticos (CSIRT). Caso práctico: Prototipo de un CSIRT en la Universidad Nacional de Chimborazo,** presentado por la Srta. Mónica Estefanía Chacha Chunata y dirigida por: Ing. Lorena Paulina Molina Valdiviezo.

Una vez escuchada la defensa oral y revisado el informe final del proyecto de investigación con fines de graduación escrito en el cual se ha constatado el cumplimiento de las observaciones realizadas, remite la presente para uso y custodia en la biblioteca de la Facultad de Ingeniería de la UNACH.

Para constancia de lo expuesto firman:

Ing. Lorena Molina
**Director del Proyecto**

.....
Firma

Ing. Ana Congacha
**Miembro del Tribunal**

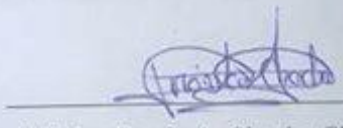
.....
Firma

Ing. Diego Reina
**Miembro del Tribunal**

.....
Firma

## DERECHOS DE AUTORÍA

La responsabilidad del contenido de este proyecto de Graduación corresponde exclusivamente a: la Srta. Mónica Estefanía Chacha Chunata bajo la dirección de la Ing. Lorena Paulina Molina Valdiviezo y el patrimonio intelectual de la misma a la Universidad Nacional de Chimborazo.



Mónica Estefanía Chacha Chunata

060502666-5

## DEDICATORIA

Dedico este proyecto de investigación a nuestro Dios que todo lo puede, por darme la fuerza necesaria para seguir adelante. También dedico a mis padres que con su arduo trabajo confiaron en mí, dándome siempre ánimo, fuerzas y apoyándome siempre en todo para que pueda ser una persona responsable, para así poder lograr todas mis metas. A mis hermanos por ser el complemento fundamental dentro y fuera de casa, por su apoyo incondicional, y por su paciencia. A mi familia y a mis amigos que siempre han estado pendientes no solamente de mí sino de mi familia, apoyando con un granito de arena para poder llegar hasta esta etapa de mi vida, es por lo que les dedico este trabajo de investigación con un gran Dios les pague por todo.

**Mónica Estefanía Chacha Chunata**

## AGRADECIMIENTO

En el presente trabajo de investigación quiero agradecer a Dios por darme la salud, inteligencia, vida y por permitirme hacer realidad el sueño tan anhelado tanto mío, como de mi familia.

Mi más sincero agradecimiento a la Universidad Nacional de Chimborazo, institución que se convirtió en mi segundo hogar abriéndome sus puertas para poder culminar con una etapa más en mi vida, preparándome como persona de bien y como profesional apto para poder servir con la sociedad con conocimientos sólidos y soluciones reales para el progreso del país.

Agradezco a la Ing. Lorena Molina quien aparte de ser una gran docente se convirtió en una gran amiga que con sus palabras y gran conocimiento culminamos con éxito la investigación.

Agradezco a Juan Toaquiza, Julio Sanaguano, Alexis Mata y Mauro Once personas muy importantes en la culminación de esta etapa, ya que me apoyaron de una u otra manera.

**Mónica Estefanía Chacha Chunata**

# ÍNDICE GENERAL

## ÍNDICE DE TABLAS

## ÍNDICE DE ILUSTRACIONES

## RESUMEN

Con el pasar de los años la mayoría de las organizaciones e instituciones tanto públicas como privadas son dependientes de una conectividad digital, también las actividades maliciosas relacionadas con la tecnología han evolucionado exponencialmente provocando enormes gastos y pérdidas en la organización.

Por consiguiente, el presente proyecto de investigación tiene como objetivo la creación de un prototipo CSIRT en la Universidad Nacional de Chimborazo (UNACH), la cual es una institución educativa que brinda servicios a toda la comunidad universitaria con sus sistemas, servicios y lo más importante es que la información este protegida ante cualquier vulnerabilidad.

Durante esta investigación se recopiló información de base de datos científicas tanto de la metodología ENISA y APCERT en las que se encontraron distintos parámetros para su comparación y se seleccionó la metodología siguiendo los pasos los pasos adecuados. Para la creación de dicho CSIRT se consideró tanto software, hardware, equipos de oficina, medidas de control, políticas de seguridad y macro controles. Así como también, métricas de seguridad que debe tener disponible el Departamento de Tecnologías de la Información y Comunicación para su adecuación en la fase inicial del CSIRT.

Después de realizar el estudio comparativo ENISA obtuvo un puntaje de 44 a diferencia de APCERT que obtuvo un puntaje de 34, por consiguiente, se creó el documento en el cual se plasma el prototipo CSIRT siguiendo la metodología ENISA, en el mismo que consta los pasos que se desarrollarán durante las fases requeridas en dicha creación.



**Palabras Clave:** CSIRT, ENISA, APCERT, VULNERABILIDADES, INCIDENTES.

Abstract

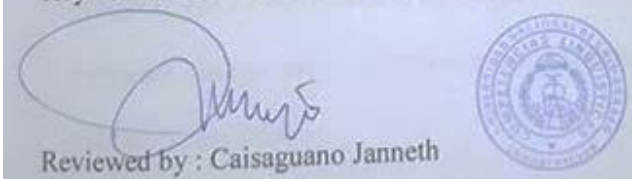
Over the years, most public and private organizations and institutions are dependent on digital connectivity, also the malicious activities related to the technology have evolved exponentially causing enormous expenses and losses in the organization.

Therefore, the present research project aims to create a prototype CSIRT at the National University of Chimborazo, which is an educational institution that provides services to the entire university community with its systems, services and the most important thing is that the information is protected from any vulnerability.

During this investigation, information was collected from the scientific database of both the ENISA and APCERT methodology, in which different parameters were found for comparison and the methodology was selected following the steps suitable. For the creation of such CSIRT was considered both software, hardware, office equipment, control measures, security policies and macro controls. As well as security metrics that must be available to the Department of Information and Communication Technologies for adaptation in the initial phase of the CSIRT.

After carrying out the comparative study ENISA obtained a score of 44 unlike APCERT which obtained a score of 34, therefore, was created the document in which the prototype CSIRT is translated following the methodology ENISA, in the same that consists the steps that will be developed during the phases required in such creation.

Keywords: CSIRT, ENISA, APCERT, vulnerabilities, incidents.



Reviewed by : Caisaguano Janneth

Language Center Teacher

# INTRODUCCIÓN

Con la expansión de los servicios digitales en los últimos años la era de la tecnología ha ido evolucionando notablemente, donde las organizaciones cada vez requieren de un acceso permanente a los servicios a través de la red, dichos beneficiarios intentan adaptarse a los cambios tecnológicos disponiendo de nuevos equipos y herramientas para adaptarse a dicha era tecnológica, debido a que son la principal causa de gastos realizados para la contención, resolución y prevención de daños potenciales, sin considerar la interrupción de los servicios a los clientes.

En la actualidad, la mayor parte de las instituciones educativas están expuestas a realizar actividades en beneficio de la comunidad universitaria optando por tener herramientas tecnológicas que pueden dar un impacto profundo a miles de personas, de igual manera, la Universidad Nacional de Chimborazo ha crecido notablemente en lo que se refiere a la actividad estudiantil, por ello, la institución dispone de espacios físicos y tecnológicos para poder llegar a la comunidad universitaria para que ellos puedan utilizar los servicios que la universidad ofrece con la eficiencia y eficacia correspondiente.

Un CSIRT es un equipo de expertos en seguridad de TI que brindan una solución adecuada ante los ataques en la seguridad informática, debido a que poseen cualidades de averiguar, contrarrestar y solucionar estos ataques con la finalidad de que no se vea afectada la institución.

Los atacantes generalmente no ven el tamaño de la organización ni la importancia del negocio al momento que desean robar información o perjudicarla, una vez notificado este incidente se procede a reaccionar de inmediato para controlar el daño y evitar posibles pérdidas y perjuicios a futuro. A los CSIRT que operan en distintos países se los conoce con distintos nombres (Mejia & Ramirez, 2016) que son: Equipo Respuesta a Emergencias Informáticas (CERT), Equipo de Respuesta a Incidentes Informáticos

(CIRT), Equipo de Respuesta a Incidentes (IRT), Equipo de Respuesta a Emergencias (ERT), Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT), Equipo de Respuesta a Incidentes de Seguridad (SIRT), Equipo de Respuesta a Emergencias de Seguridad (SERT) (De la Torre & Parra, 2018).

Por lo que el presente proyecto de investigación plantea una propuesta de creación de un prototipo CSIRT académico en la Universidad Nacional de Chimborazo (UNACH), el mismo que tendrá un impacto positivo en la comunidad universitaria debido a que dicha institución no tiene un área específica que se encargue de la solución de los incidentes informáticos. Además, la propuesta se encuentra basada en una guía práctica para la creación del CSIRT académico el mismo que fue entregado al director del Departamento de Tecnologías de la Información y Comunicación de la institución.

Este documento está estructurado de la siguiente manera: En el capítulo I se describe el planteamiento del problema, posteriormente en el capítulo II se encuentra el marco teórico a continuación, en el capítulo III se plasma la metodología, más adelante en el capítulo IV se encuentran los resultados y discusión, y finalmente se plasma las conclusiones y recomendaciones.

# CAPITULO I

## 1. PLANTEAMIENTO DEL PROBLEMA

### 1.1. Problema y Justificación

Las instituciones de educación superior en la actualidad están expuestas a una gran cantidad de vulnerabilidades, por ello la Universidad Nacional de Chimborazo (UNACH) no está exenta a las vulnerabilidades porque la comunidad universitaria debe estar conectada a internet para consultar los diferentes servicios que ofrece dicha institución. Con el avance tecnológico han descubierto formas cada vez más complejas de ataques aprovechando las redes para sus propósitos maliciosos, por lo que, en los últimos años las amenazas de seguridad han evolucionado hasta convertirse en complejos sistemas diseñados para robar información mediante una variedad de ataques, por lo tanto, se ha propuesto crear centros de respuesta a incidentes informáticos (CSIRTs), los cuales ayudan a prevenir incidentes en las organizaciones (Chelo, 2004).

Generalmente, los atacantes no ven el tamaño de la organización o la importancia del negocio al momento en que desean perjudicar a la institución una vez detectado y notificado el incidente se procede a dar solución adecuada para que la institución no se vea afectada futuro, de forma paralela la seguridad informática también ha evolucionado, por ende, existen varios equipos de respuestas ante incidentes informáticos en distintos países que ayudan a mitigar estos incidentes (De la Torre & Parra , 2018).

En Ecuador, la mayoría de las instituciones de educación superior no cuentan con estas áreas para dar un tratamiento a la seguridad de la información, por lo cual, no existe mucha información en los distintos parámetros que debe contener y así poder implementar en las instituciones de educación superior (Andrade , 2013).

La Universidad Nacional de Chimborazo al ser una institución de educación supero no cuenta con esta área que se encargue de emitir las alertas acerca de los incidentes

informáticos, los cuales deben ser solucionados de inmediato para que no se vea afectada la institución (Paredes & Andrade , 2013).

Por consiguiente, el presente proyecto de investigación tiene como objetivo la creación de un prototipo CSIRT, que cumpla con los servicios que ofrece el CSIRT, aunque no son todos en especial los reactivos y proactivos para solucionar dichos daños.

## .1.2 Objetivos

### Objetivo General

- Analizar las metodologías ENISA y APCERT para la creación del Centro de Respuestas a Incidentes Informáticos (CSIRT). Caso Práctico: Prototipo de un CSIRT en la Universidad Nacional de Chimborazo.

### Objetivos Específicos

- Estudiar las metodologías ENISA y APCERT para la creación de un CSIRT académico.
- Seleccionar una metodología para la creación de un prototipo que proteja y asegure los activos críticos de la UNACH.
- Elaborar una guía de implementación de CSIRT en la UNACH.

# CAPITULO II

# 2. MARCO TEÓRICO

El propósito de este capítulo se basa en presentar el marco teórico sobre el cual está apoyado para la creación de un prototipo CSIRT Académico para la Universidad Nacional de Chimborazo (UNACH). Inicialmente se detallará información acerca de los CSIRTs a nivel mundial, las metodologías que vamos a comparar ENISA y APCERT en las cuales se basa la estrategia de diseño y creación de la guía para el prototipo CSIRT de la institución.

## 2.1.Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT)

El CSIRT consta de especialistas en seguridad de la información ellos son responsables de prevenir, identificar y responder los incidentes de seguridad informática (Ramírez & Miranda , 2015). Este centro también contas con distintos servicios los cuales ayudan a contrarrestar dichos incidentes. Ofrece distintos servicios entre los cuales está la gestión de incidentes, elaboración de planes, gestión de estrategias para solucionar vulnerabilidades dentro de la institución (De la Torre & Parra , 2018).

Se utilizan diferentes abreviaturas para el mismo tipo de equipos:

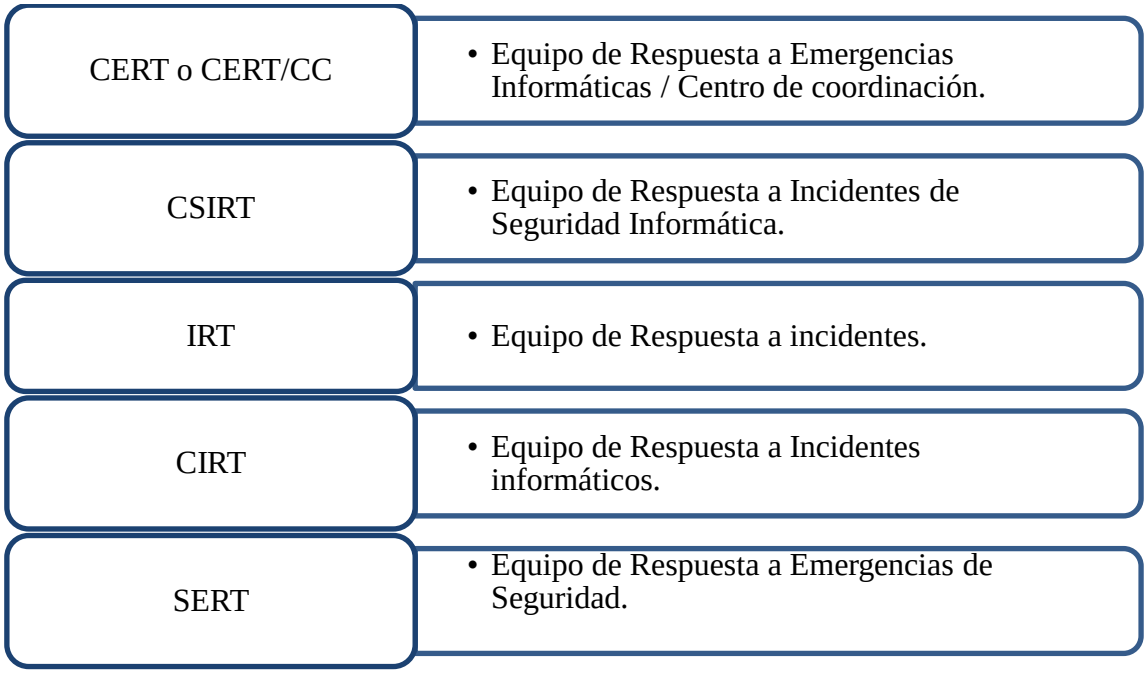



***Ilustración 1.*** *Abreviaturas del CSIRT* (Andrade , 2013)

Como objetivos de esta agencia está definir algunas políticas, distintos procedimientos y diferentes servicios para poder dar una solución óptima al incidente detectado, es decir, (identificarlo, contenerlo y eliminarlo), para recuperarse del incidente se procede a determinar, verificar y la causa probable del incidente para posterior dar una solución a dicho incidente esto conlleva a la identificación de la causa, recolección de evidencia y determinar la culpa y por último ayudar a la prevención de una duplicación del incidente (Carozo, Martínez , & Vidal , 2010).

**2.2. Servicios de un CSIRT**

Los CSRT brindan diferentes servicios de acuerdo con la misión y visión de la organización la cual se va a planificar, crear e implementar, además están alineados a la necesidad de la población sobre la seguridad informática. Son muchos los servicios que ofrece el CSIRT, pero hasta ahora ningún CSIRT ofrece todos, los servicios pueden agruparse en tres categorías (Murquincho, 2019).

Dentro de los servicios de un CSIRT tenemos tres categorías que se distingue dentro de un CSIRT que son: tanto los servicios reactivos, proactivos y los servicios de gestión de la seguridad, aunque no brinda todos los servicios un CSIRT en su mayoría ofrecen más de la mitad (Ramírez & Miranda , 2015).

| Servicios Reactivos | Servicios Proactivos | Servicios de Gestión de la seguridad |
|---|---|---|
| • Alertas y advertencias<br>• Manejo de incidentes<br>• Análisis de incidentes<br>• Respuesta a los incidentes<br>• Soporte de respuesta a incidentes<br>• Manejo de vulnerabilidades<br>• Coordinación de respuesta a vulnerabilidades | • Anuncios y observación de la tecnología<br>• Auditoría y evaluación de la seguridad<br>• Configuración y mantenimiento de las herramientas de apliacación, infraestructura y servicios de seguridad<br>• Desarrollo de herramientas y servicios de DDoS | • Análisis de riesgo<br>• Planificación de la continuidad del negocio y recuperación de desastres<br>• Consultoría de seguridad |

***Ilustración 2.*** *Servicios de un CSIRT***(Guacho, 2014)**

### 2.2.1. Tipos de CSIRT

Dependiendo el ámbito de su implementación existen diferentes tipos de CSIRT los cuales se les clasifica de la siguiente manera.

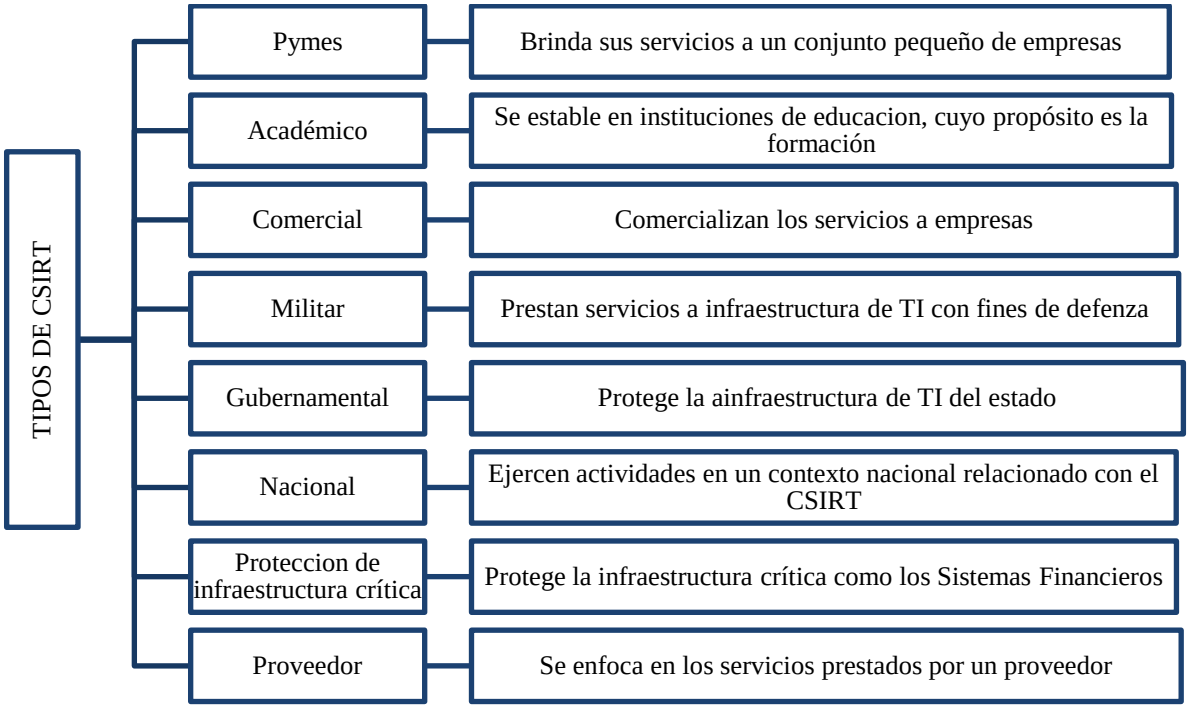



***Ilustración 3.*** *Tipos de CSIRT* (Guacho, 2014)

Como se puede observar existen diferentes tipos de CSIRT, varían en sus características, ámbito de aplicación y en los servicios que ofrece, sin embargo, este proyecto se enfoca en la creación de un prototipo CSIRT académico (MURQUINCHO , CHALÁN, MONTESINOS , & ULLOA, 2018).

#### 2.2.1.1. CSIRT Académico

Los CSIRT Académicos no solo se basa en los servicios relacionados en la gestión de incidentes de la seguridad informática, sino también proporciona entornos favorables para la formación e investigación dentro de la organización. Además, uno de los CSIRT académico se centra en la formación en la cual proporciona un plan de capacitación con los siguientes objetivos.

- Dar a conocer el funcionamiento interno del CSIRT
- Mejorar y ejercitar las habilidades técnicas del personal

- Mantener al tanto de los avances tecnológicos en materia de Ciberseguridad mediante la constante investigación (Salinas & Marin , 2019).

### 2.2.2. Beneficios de un CSIRT

Al contar con un Centro de Respuesta a incidentes informáticos es para que la institución no se vea afectada al momento en que suscite cualquier percance en el cual se puede ver afectada la información y no pueda ser recuperada la misma. Los CSIRT al ser una agencia que permite mitigar estos daños debe compartir información con otros CSIRT que están relacionados así, se ayudan mutuamente para la solución adecuada del incidente, también contribuyen a que los datos estén protegidos para toda la comunidad universitaria al momento en que ellos no necesiten (Carozo, Martínez , & Vidal , 2010).

### 2.2.3. Habilidades que debe poseer el personal que conforma un CSIRT

#### 2.2.3.1.Capacidad

En la actualidad se debe conformación el personal del CSIRT con personas que estén capacitadas en el área y con el personal que la institución tenga disponible, debido a que existen diferentes servicios que debe ser manipulados por expertos, porque su funcionalidad debe ser al máximo.

#### 2.2.3.2.Aptitudes

El personal del CSIRT deben ser personas que este aptas para la solución de cualquier tipo de incidente que se pueda suscitar en la institución para ello se debe conocer las distintas competencias que debe tener el personal, a continuación, se presentan las competencias de cada personal.

***Tabla 1.*** *Competencias personales*

| Competencias personales | Competencias técnicas | Competencias adicionales |
|---|---|---|
| Buen espíritu de equipo | Conocimiento en diferentes tecnologías y protocolos de internet | Alta disponibilidad |
| Altas habilidades analíticas | | Buen nivel de educación |
| Fluida explicación de cuestiones técnicas difíciles | Conocimiento de sistemas operativos | Experiencia en el campo de TI |
| Sentimiento de confidencialidad para la información | Conocimiento de infraestructura de red | |
| Buena organización | Conocimiento de aplicaciones de internet | |
| Alta comunicación y escritura | Conocimiento de amenazas de seguridad | |
| Capacidad de aprendizaje y de mente abierta | Conocimiento de análisis y respuesta a riesgos | |

#### 2.2.3.3.Estructura de la organización del CSIRT

La estructura organizacional debe estar acorde con la infraestructura y el personal de la institución, también se debe tener muy en cuenta los distintos servicios que se va a ofertar y así dar funciones específicas al personal. Dentro de esta estructura se va a establecer los siguientes cargos:

Cargo general, personal, equipo técnico y personal externo.

Dentro de los modelos para los CSIRT son los siguientes:

**Modelo de empresa independiente**

Se basa en un modelo de CSIRT amplio que actúa como una organización independiente, es decir hace uso de sus propios directivos y empleados.

**Modelo incrustado**

Este modelo se utiliza junto al departamento de Tecnologías de la Información y comunicación de la institución que va a ser beneficiada debido a que trabaja con un número de trabajadores específicos los cuales se pueden encargar de las diferentes funcionalidades.

**Modelo universitario**

Este modelo es más para las instituciones educativas para la creación de un CSIRT académico o de investigación, es decir cada institución puede contar una institución beneficiaria que sea el punto de contacto con los demás CSIRTs, esto puede disminuir gastos entre las distintas instituciones.

**Modelo voluntario**

Este modelo lo constituye a un grupo de expertos que se unen a dar asesoría y apoyarse mutuamente, es decir, dependiendo de la motivación que tengan los participantes (Armas , 2012).

### 2.2.4. Modelo organizacional de un CSIRT

Cuando se va a implementar un CSIRT se debe tomar en cuenta la estructura organización de la institución porque existen modelos que nos permiten realizar su implementación sin ningún tipo de inconveniente la cual debe estar en un área específica para su desarrollo.

#### 2.2.4.1.Equipos de seguridad para su implementación

Se puede implantar en instituciones pequeñas que el objetivo sea una necesidad específica, como la seguridad que debe tener toda organización, lo primero que se debe hacer es implementar equipos con componentes de infraestructura como puede ser los firewalls, redes privadas (VPN) y los sistemas de detección de intrusos (IDS).

#### 2.2.4.2.Modelo distribuido de un CSIRT

Este modelo se compone por distintas personas que trabajan en distintas organizaciones tanto públicas como privadas, este modelo se basa especialmente porque debe cumplir distintas políticas, procedimientos y diferentes formas de manejar un incidente las instituciones y finalmente un gerente de CSIRT designado para supervisar y miembros del equipo que son encargados de asignar tareas de manejo especifico de incidentes.

#### 2.2.4.3.Modelo centralizado de un CSIRT

En este modelo se tiene personal especializado y capacitado el cual se encuentra designado con tareas y responsabilidades específicas para poder tratar los incidentes dentro de la organización. Lo más importante es que facilita la agrupación para sintetizar y diseminar la información en la empresa. El CSIRT tiene como finalidad informar sobre los distintos ataques o vulnerabilidades que está sufriendo la institución, los cuales deben ser solucionados lo más rápido posible. El equipo tiene la opción de tomar decisiones sobre la estrategia de recuperación y mitigación de los incidentes siempre y cuando sea autorizado por la gerencia.

#### 2.2.4.4.Modelo combinado de un CSIRT

La estrategia se centra en que tiene interacción con los miembros de cada área de la organización, la cual realiza un análisis de alto nivel y realiza recomendaciones estratégicas de recuperación y solución del incidente.

#### 2.2.4.5.Modelo coordinador de un CSIRT

Con este modelo se puede trabajar con personal de otras instituciones como apoyo debido a que nos pueden facilitar información acerca de cómo gestionar un incidente. Existen varios modelos de un CSIRT y cada uno contienen niveles de autoridad en la comunidad objetivo.

- **Primer nivel:** sirve a un grupo de personas que son los beneficiarios dentro de la institución, ayuda a las autoridades del CSIRT a que tomen soluciones ante los incidentes de pueden ocurrir en la institución y deben darles una solución adecuada.
- **Segundo nivel:** sirve a un grupo de personas que están conformados por las fuerzas militares y sus contribuyentes.
- **Tercer nivel:** sirve a las personas que viven dentro de un país, provincia y ciudad, las autoridades que la precedan no son relevantes porque no tiene control sobre la zona a la que se está aplicando (Cormack, Kossakowski, Maj, Parker , & Stikvoort, 2005-2017)

### 2.2.5. CSIRT del sector académico

Este CSIRT no solo brinda servicios a las instituciones educativas a las que pertenece, también se puede contribuir con información a las entidades que están vinculadas con los CSIRT porque se archivan documentos en los cuales estos solucionados incidentes con sus respectivas bitácoras.

Cuando una institución quiere realizar la creación de estos centros se ve truncada porque no existe el apoyo necesario de las autoridades de la institución, no cuenta con el personal adecuado capacitado sobre el tema, tampoco cuenta con todas las políticas y procedimientos a nivel internacional en tema de la seguridad, tampoco cuenta con el proceso de creación de proyectos a largo plazo porque no cuenta con el capital necesario. Al momento de proteger los sistemas de información que tiene una organización se va a tener algunas dificultades, por el hecho de que la tecnología evoluciona dentro del cibercrimen. Por ende, se ha visto afectado el cibercrimen por las siguientes situaciones.

- En la actualidad el robo de la información es un tipo de robo con fines de lucro que es bien recompensado por la información ya sea de tarjetas de crédito, robo de la información, entre otros.
- Existe un crecimiento del hacking ya sea en lo político o social, esto genera una gran desconfianza al personal del CSIRT porque debe estar en constante capacitación.
- Las amenazas cada vez van en aumento, es decir, se debe evitar que grupos criminales tengan la facilidad de tener información confidencial o que se encuentran en los sistemas informáticos los cuales están relacionados con las entidades gubernamentales.
- Los sistemas de información en una empresa u organización tienen conexiones con el sector público y privado, lo cual ya no existe una protección de satos individual, sino más bien se debe proteger la información de los sistemas en toda la red, es decir, se debe generar responsables en cada dominio de seguridad (Palacio , 2018).

### 2.3. Metodología ENISA

El objetivo principal de la Agencia Europea de Seguridad de las Redes y la Información (ENISA) es ayudar a las instituciones a nivel nacional e internación que la seguridad de sus datos este protegido, los únicos beneficiarios serían las instituciones que están estrechamente relacionadas con el CSIRT, también las instituciones tanto públicas como privadas que pertenecen a la UE.

Esta agencia funciona como un punto de contacto que sirve para dar asesoramiento a las instituciones desde cómo realizar la creación de un CSIRT, en aspectos de seguridad de la información y la solución de algunas vulnerabilidades que puedan estar afectando a la institución en especial a los datos.

Entre las principales tareas de esta agencia están:

- Asesoramiento y análisis de la información relevante que tiene como objetivo la seguridad de la información y los riesgos procedentes.
- Crea asociaciones entre las organizaciones del sector público y privado, es decir, con las empresas que están vinculadas con la UE a nivel mundial.
- Dar a conocer a los usuarios sobre la problemática de las redes de la información, promover métodos que ayuden a solucionar los mismos y mejor las practicas con el objetivo de encontrar soluciones a estos riesgos

### 2.3.1. Objetivos de ENISA

Al crear esta agencia se tiene como objetivo ayudar a las instituciones relacionadas a la solución acerca de los problemas relacionados con la seguridad informática, se debe dar un seguimiento, asistencia y asesoramiento con lo que respecta a la seguridad de las redes y la información, también ayuda a incrementar la asociación entre el sector público y privado, se debe tener un mantenimiento adecuado acerca del material relacionado con la seguridad de las redes y la información dentro de la agencia.

La agencia tiene algunas tareas importantes que debe cumplir:

- Archivar y documentar los distintos ataques o vulnerabilidades que se han presentado en la institución sobre la seguridad informática tanto en redes, infraestructura y los sistemas de información y por último se debe reportar este incidente con las autoridades de la institución y de la agencia.
- Facilitar asesoramiento y asistencia en relación con los objetivos asignados a al Parlamento Europeo, a la comisión y a otros organismos relacionados.
- Promover la cooperación entre agentes que operan en el sector como por ejemplo las organizaciones, las empresas y hasta las universidades, las cuales ayudan a que esta información se divulgue y así ayudar a las instituciones que están siendo

atacadas o vulneradas para que puedan solucionar el problema sin que afecte a la institución.

- Para que las instituciones no se vean afectadas por el ataque durante un periodo largo de tiempo se debe intercambiar buenas prácticas de cómo solucionar el incidente, debido que ahí debe contar como identificar el tipo de ataque y cuál es el medio que utilizan para atacar y contrarrestarlo.
- Asistir a las capacitaciones de las instituciones tanto públicas como privadas que existen en cada país sobre la gestión de problemas de seguridad y los programas informáticos.
- Se debe realizar un seguimiento a la creación de normas para los productos y servicios en materia de la seguridad y las actividades de evolución de los riesgos.
- Ayudar en la cooperación a terceros países y organizaciones internacionales relacionadas a un enfoque sobre la problemática de la seguridad (Castillo, 2010).

## 2.4. Metodología APCERT

La misión del Equipos de respuesta de Emergencia por computadora en Asia y el Pacífico (APCERT) es mejorar la sensibilización y la capacidad de la región en relación con los incidentes de seguridad informática mediante el fomento de la cooperación regional e internacional en materia de seguridad de la información en Asia y el Pacífico.

Para ayudar a contrarrestar los incidentes de seguridad tanto regionales o a gran escala se debe tomar en cuenta lo siguiente:

Ayuda en el intercambio de información y tecnología, incluida la seguridad de la información, el virus informático y el código malicioso entre sus miembros.

Promueve la colaboración en la investigación y el desarrollo sobre temas de interés para sus miembros.

Ayudar a otros CERT y CSIRTS de la región a llevar a cabo una respuesta informática de emergencia eficiente y eficaz.

Aporta con recomendaciones para ayudar a abordar cuestiones jurídicas relacionadas con la seguridad de la información y la respuesta de emergencia a través de las fronteras regionales (Bada , Creese, Goldsmith, Mitchell, & Phillips, 2014).

Los medios de comunicación han informado sobre las supuestas medidas independientes adoptadas por un miembro de la APCERT en cuanto a la divulgación más amplia de información confidencial. APCERT no participó en la respuesta ni en la coordinación de la respuesta de las advertencias de manejo de información para la información recibida de los miembros. Debido a las diferencias en las políticas y regulaciones de los diferentes equipos dentro de APCERT, cualquier acción tomada por los equipos miembros se hace exclusivamente a su discreción (Incidente APCERT, 2019).

### 2.4.1. Objetivos de la agencia

Dentro de los objetivos de APCERT es tener una red limpia de sistemas infectados, compartir información fiable, canales de comunicación seguros y medir sus sistemas (APCERT, 2019).

El equipo de APCERT está capacitado para brindar diferentes servicios entre los cuales la comunicación es importante:

- Incidentes y/o problemas de seguridad cibernética graves y críticos en el tiempo con el fin de ayudar a resolver o investigar un incidente.
- Vulnerabilidades de seguridad cibernética graves y críticas en el tiempo, cuyo conocimiento aún no es de dominio público.
- Amenazas cibernéticas graves y de tiempo crítico para proporcionar alerta temprana a los constituyentes del POC (Acuerdos de puntos de contacto) y/o a otros POC dentro de su grupo regional CERT/CSIRT.

- Estar disponible y ser contactable 24x7.
- Proporcionar números de contacto telefónicos genéricos, direcciones de correo electrónico y claves PGP para el POC y números de teléfono compatibles con SMS cuando sea posible
- Disponer de mecanismos de apoyo para apoyar los arreglos del POC.
- Los POC deben proporcionar contactos de habla inglesa siempre que sea posible.
- Establecer procedimientos de escalonamiento para que se puedan adoptar medidas inmediatas u obtener una autorización adecuada para actuar con un mínimo de retraso (APCERT POC Arrangements Policy, 2013).

# CAPITULO III

# 3. METODOLOGÍA

## 3.1.Tipo de estudio

El tipo de estudio es descriptivo porque se identificó componentes y características para la solución del problema.

Además, es explicativo porque se demostró las definiciones y servicios que tiene las dos metodologías con los componentes que tiene la institución educativa.

Los tipos de estudio se detallan a continuación.

### 3.1.1. Según el objetivo de estudio

- **Investigación de Campo:** Es el proceso de recolección de los distintos componentes que obtuvo los criterios de las metodologías y la estructura organizacional.
- **Investigación Aplicada:** Es porque se dió solución al problema antes mencionado.

### 3.1.2. Según la fuente de investigación

- **Investigación Bibliográfica:** Se realizó la recolección de la información, utilizando técnicas y estrategias para acceder a documentos como: tesis, libros, journals y artículos.

### 3.1.3. Según el nivel de conocimientos:

- **Investigación Descriptiva:** Se analizó y comparó diferentes componentes de las metodologías y la estructura organizacional.

### 3.2.Según el método a utilizar

- **Método Deductivo:** Se usó este método para conocer la problemática propuesta por este proyecto, con el fin de proponer un comité de respuesta a incidentes informáticos en la cual se ayudó a plantear, desarrollar y mitigar los posibles problemas y dar una solución adecuada.
- **Método Inductivo:** Con este método se conocieron las necesidades y problemas que actualmente tiene la comunidad universitaria de la UNACH en temas relacionados a la seguridad informática.
- **Método Bibliográfico:** Se llevó a efecto la revisión literaria en diferentes bases de datos científicas para la resolución de esta investigación.

### 3.3. Procedimientos

#### 3.3.1. Técnica de Investigación

- **Técnica de Observación**. – Con esta técnica se basó en observar los diferentes componentes entre las dos metodologías comparando con los componentes de la UNACH con el fin de obtener información y luego procesarla para la creación de prototipo CSIRT académico.

#### 3.3.2. Instrumentos de Recolección de Datos

- Este instrumento de recolección de datos fue necesario para investigar los criterios de las metodologías, en la cual se utilizó una escala de valoración y asumir la mejor metodología después de la comparación.

## 3.4.Procesamiento y Análisis

### 3.4.1. Revisión la parte literaria sobre el tema de investigación

En este punto de la investigación se tuvo como objetivo indagar en los diferentes repositorios y base de datos científicos los documentos que se hayan realizado anteriormente con el propósito de tener una idea más acertada de los criterios a comparar para tener una idea más clara del objetivo a lograr.

### 3.4.2. Análisis de las metodologías para esta investigación

En este punto de la investigación se tuvo como propósito analizar las dos metodologías y sacar los diferentes componentes que tiene cada uno, también se realizó una escala de valoración para seleccionar la mejor metodología y por último se realizó una guía práctica del prototipo CSIRT para la UNACH.

### 3.4.3. Parámetros de las metodologías ENISA y APCERT

En la investigación realizada se determinó los siguientes componentes de las dos metodologías las cuales vamos a comparar para seleccionar la más idónea en la creación del prototipo CSIRT académico en la UNACH.

**Metodología ENISA. –** Dentro de esta metodología se estableció los siguientes parámetros de evaluación dependiendo la revisión literaria (parámetros ENISA, 2017).

**Categoría software**

- Escáner de puestos
- Escáner de vulnerabilidades
- Herramientas de monitoreo
- Crack

- Sniffers
- Criptografía
- Sistema de seguimiento de incidentes
- Herramientas para administrar políticas de seguridad, evaluación de riesgos y planes de contingencia.
- Herramientas de auditoria de seguridad

**Categoría hardware**

Equipos y medios de conectividad

- Routers de borde/Core
- Switch de acceso y distribución
- Cableado estructurado
- Enlace de internet

Servidores

- Correo electrónico
- WEB, NTP, DNS
- Intranet

Herramientas de protección

- Firewall
- IDS, IPS

Estación de trabajo y equipos portátiles

- Estación de trabajo
- Accesorios CD, DVD, discos duros externos

Equipos de seguridad física

- Caja de seguridad para almacenamiento de documentos y copias de seguridad
- Infraestructura y protección contra incendios
- Sistema de aire acondicionado
- Protección de energía eléctrica (UPS)

**Categoría equipos de oficina**

- Computadoras
- Teléfonos
- Impresoras multifuncional
- Sillas giratorias para escritorio
- Sillas de espera
- Archivadores
- Suministros de oficina (arriendo, agua, energía eléctrica, pago de sueldos)

**Categoría medidas de control**

- Medidas preventivas
    - Medidas técnicas o de ingeniería
    - Medidas organizativas o administrativas
- Medidas de protección
    - Medidas colectivas
    - Medidas individuales
- Medidas de mitigación
    - Plan de emergencia
    - Planificación de evaluación
    - Sistemas de alerta y simulaciones

**Categoría macro controles**

- Políticas de seguridad
- Gestión de activos
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de acceso

**Categoría política de seguridad**

- Política de clasificación de información
- Política externa para el acceso de la información
- Política de aislamiento de la información
- Política de seguridad del internet
- Política de notación y tratamiento de incidentes
- Política de capacitación
- Política de selección del personal
- Política de despido
- Política de seguridad de las computadoras personales
- Política de uso de los correos electrónicos
- Políticas de la seguridad de la red de computadores
- Política de telecomunicaciones de la información
- Políticas de uso de dispositivos móviles

**Metodología APCERT. –** Los parámetros de esta metodología se representan a continuación de acuerdo con la revisión literaria (APCERT Repositorio CIMAT, 2018).

**Categoría software**

- Soporte a varios SO
- Software libre
- Soporta varias plataformas
- Sistemas operativos prioritarios

**Categoría hardware**

Equipos y medios de conectividad

- Routers
- Switch
- Cableado estructurado
- Enlace a internet independiente y redundante

Equipos de seguridad perimetral

- Firewall, IDS/IPS

Servidores

- WEB, MAIL, NTP, DNS
- Registro de eventos
- Respaldo de información

Computadores y accesorios

- Estaciones de trabajo
- Computadores portátiles
- Pen drive, discos duros externos, CD, DVD
- Proyector portátil
- Impresora multifuncional
- Dispositivos para realizar copias de seguridad
- Trituradora de papel

- Pizarra digital interactiva
- Video Wall para monitoreo

Equipos para seguridad en el ambiente físico

- Caja fuerte
- Estructura de protección contra incendios
- Sistema de aire acondicionado en el Data Center
- Infraestructura de protección contra interrupciones del suministro de energía eléctrica
- Sistema de video vigilancia
- Puertas de seguridad de control de acceso

**Categoría medidas de control**

- Riesgos laborales
- Peligro laboral
- Evaluación de riesgos
- Seguridad laboral
- Enfermedad profesional
- Accidente laboral
- Medidas preventivas
- Medidas de protección
- Medidas de mitigación

**Categoría macro controles y políticas de seguridad**

- Identificar, autenticar y autorizar el acceso a los sistemas de información solo a personas autorizadas a dicho acceso
- Identificar al remitente y destinatario de las comunicaciones electrónicas, especialmente correo electrónico

- Controlar el acceso para restringir la utilización y el acceso a datos e informaciones a las personas autorizadas y proteger los procesos informáticos frente a manipulaciones no autorizadas
- Mantener la integridad de la información y elementos del sistema, para prevenir alteraciones o pérdidas de los datos e informaciones
- Garantizar la disponibilidad de la información y de las aplicaciones
- Prevenir la interceptación, alteración y acceso no autorizado a la información
- Proporcionar el conjunto de medidas organizativas y técnicas de seguridad de la información que garanticen el cumplimiento de los requisitos legales para la validez y eficacia de los procedimientos administrativos
- Facilitar la adopción de medidas organizativas y técnicas que aseguren la protección de su información frente a los riesgos propios de los sistemas y aplicaciones informáticas que maneje
- Gestión de incidentes de seguridad
- Auditoría y control de la seguridad

## 3.5 Comparaciones de acuerdo con los parámetros establecidos de las dos metodologías.

Los parámetros establecidos para la investigación son: software, hardware, equipos de oficina, macro controles, aspectos y políticas de seguridad.

Se va a realizar una comparación de los parámetros en base a la revisión literaria de la metodología ENISA (CSIRT_setting_up_guide_ENISA, 2010) y la metodología APCERT (Asia Pacific Computer Emergency Response Team (APCERT), 2017).

A continuación, se ve plasmado un cuadro comparativo de las dos metodologías, esta comparación se hizo a través de la revisión literaria de dichas metodologías calificando de 1 si consta en la metodología y 0 si no consta en la metodología

***Ilustración 4.*** *Comparación categoría software*

| Categoría software | | |
|---|---|---|
| **Parámetros** | **Metodología** | |
| | **ENISA** | **APCERT** |
| Escáner de puertos y vulnerabilidades | 1 | 1 |
| Herramientas de monitoreo | 1 | 1 |
| Herramientas hacking (crack, sniffers, IDS y criptografía) | 1 | 0 |
| Sistema de seguimiento de incidentes | 1 | 1 |
| Herramienta para administración de políticas de seguridad, evaluación de riesgos y planes de contingencia | 1 | 0 |
| Herramientas de auditoria de seguridad | 1 | 0 |
| Multiplataforma | 0 | 1 |
| Software libre | 0 | 1 |
| **TOTAL** | **6** | **5** |

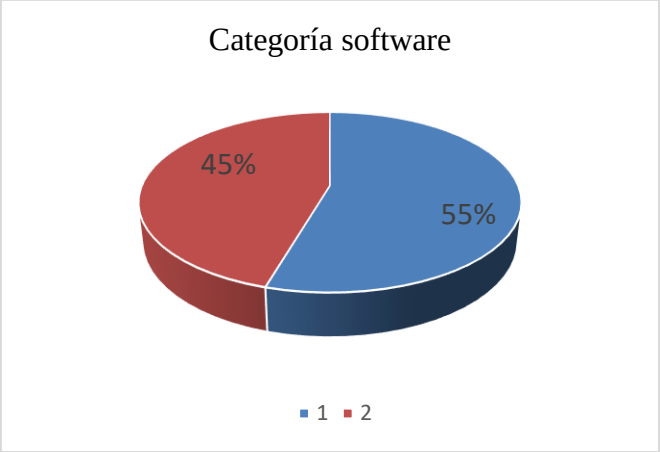



***Ilustración 5.*** *Comparación categoría software*

Dentro de la categoría software se puede observar que la metodología ENISA cumple con 7 parámetros dentro de la revisión literaria no cuenta que sea multiplataforma y que tenga software libre frente a la metodología APCERT que cumple 5 parámetros en la cual, no tiene herramientas de hacking y herramientas para administrar políticas de evaluación de riesgos y contingencia.

***Ilustración 6.****Comparación categoría hardware*

| Categoría hardware | | |
|---|---|---|
| **Parámetros** | **Metodología** | |
| | **ENISA** | **APCERT** |
| Equipos y medios de conectividad | 1 | 1 |
| Servidores | 1 | 1 |
| Computadores y accesorios | 1 | 1 |
| Herramientas de protección | 1 | 1 |
| Estación de trabajo y equipos portátiles | 1 | 1 |
| Equipo de seguridad física | 1 | 1 |
| Equipos adicionales | 0 | 1 |
| **TOTAL** | **6** | **7** |

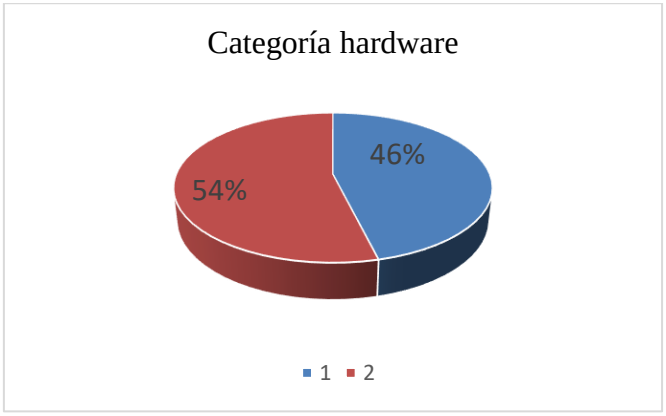



***Ilustración 7.*** *Comparación categoría hardware*

Al momento que se realizó la comparación de los componentes de las dos metodologías se observó que la metodología APCERT cumple con 7 parámetros, frente a la metodología ENISA que tiene 6 parámetros en la que no consta de equipos adicionales.

***Ilustración 8.*** *Comparación categoría equipos de oficina*

| Categoría equipos de oficina | | |
|---|---|---|
| **Parámetros** | **Metodología** | |
| | **ENISA** | **APCERT** |
| Suministros de oficina | 1 | 1 |
| Servicios básicos | 1 | 0 |
| Estaciones de trabajo | 1 | 1 |
| **TOTAL** | **3** | **2** |

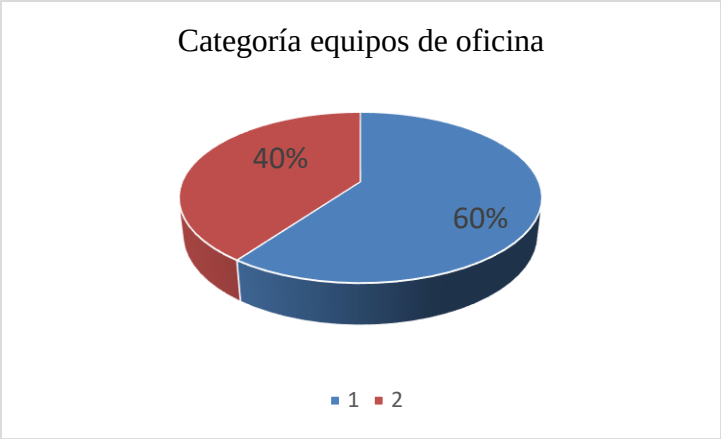



***Ilustración 9.*** *Comparación categoría equipos de oficina*

Dentro de la categoría equipos de oficina la metodología ENISA cumple con 3 parámetros frente a la metodología APCERT que solo tiene 2 parámetros la cual, no cumple en la literatura con la contratación de los servicios básicos debido a que lo esencial y fundamental es el suministro de oficina.

***Ilustración 10.*** *Comparación medidas de control*

| **Categoría medidas de control** | | |
|---|---|---|
| **Parámetros** | **Metodología** | |
| | **ENISA** | **APCERT** |
| Riesgos laborales | 1 | 1 |
| Peligro laboral | 1 | 1 |
| Evaluación de riesgos | 1 | 1 |
| Seguridad laboral | 1 | 1 |
| Enfermedad profesional | 1 | 1 |
| Accidente laboral | 1 | 1 |
| Medidas preventivas | 1 | 1 |
| Medidas de protección | 1 | 1 |
| Medidas de mitigación | 1 | 1 |
| **TOTAL** | **9** | **9** |

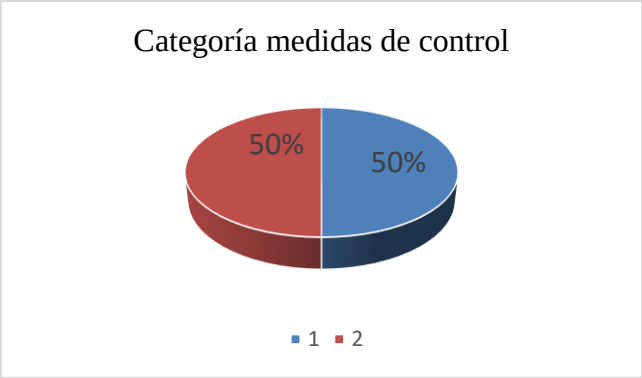



***Ilustración 11.*** *Comparación medidas de control*

En la categoría medidas de control se puede observar que las dos metodologías brindan estos servicios o componentes, es decir, para esas agencias es importante la seguridad de los empleados al momento de trabajar por ello, al momento de comparar dichos componentes se obtiene un valor de 9 puntos para cada metodología.

**Ilustración *12.*** *Comparación categoría macro controles*

| **Categoría macro controles** | | |
|---|---|---|
| **Parámetros** | **Metodología** | |
| | **ENISA** | **APCERT** |
| Políticas de privacidad | 1 | 0 |
| Gestión de activos | 1 | 0 |
| Seguridad física y del entorno | 1 | 1 |
| Gestión de comunicaciones y operaciones | | |
| Control de acceso | 1 | 1 |
| Disponibilidad de la información | 1 | 1 |
| Gestión de incidentes de seguridad | 0 | 1 |
| Adquisición, desarrollo y mantenimiento de los sistemas informáticos | 1 | 0 |
| Auditar y controlar la seguridad | 0 | 1 |
| **TOTAL** | **6** | **5** |

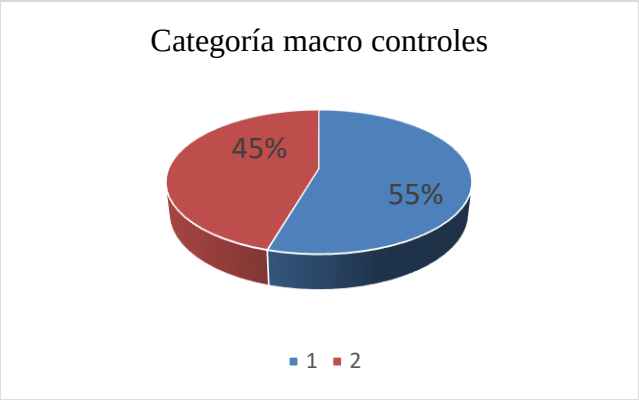



***Ilustración 13.*** *Comparación categoría macro controles*

Dentro de los parámetros macro controles se puede visualizar que la metodología ENISA cumple con 6 puntos dentro de los cuales no toma en consideración dentro de la literatura revisada los incidentes de seguridad y la auditoría y control de la seguridad, en la metodología APCERT tiene 5 puntos en los que no se toma en cuenta las políticas de seguridad, gestión de activos y dar mantenimiento a los sistemas informáticos que van en decadencia.

***Ilustración 14.*** *Comparación categoría políticas de seguridad*

| **Categorías políticas de seguridad** | | |
|---|---|---|
| **Parámetros** | **Metodología** | |
| | **ENISA** | **APCERT** |
| Política de clasificación de información | 1 | 1 |
| Política externa para el acceso de la información | 1 | 1 |
| Política de aislamiento de la información | 1 | 0 |
| Política de seguridad del internet | 1 | 0 |
| Política de notación de incidentes | 1 | 0 |
| Política de tratamiento de incidentes | 1 | 0 |
| Política de entrenamiento y capacitación | 1 | 1 |
| Política de selección de personal | 1 | 1 |
| Política de despido | 1 | 1 |
| Política de seguridad de la computadora personal | 1 | 0 |
| Políticas de uso de correo electrónico | 1 | 0 |
| Política de la seguridad de la red de computadores | 1 | 0 |
| Política de telecomunicaciones de la información | 1 | 1 |
| Políticas de uso de dispositivos móviles | 1 | 0 |
| **TOTAL** | **14** | **6** |

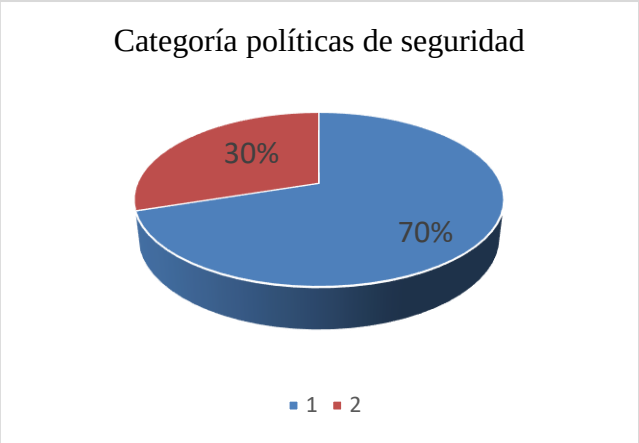



***Ilustración 15.*** *Comparación categoría políticas de seguridad*

Dentro de la categoría políticas de seguridad se puede observar que la metodología ENISA cumple con 14 puntos esenciales dentro de la creación de un CSIRT, a diferencia de la metodología APCERT que cumple con 6 puntos en los que no toma en cuenta dentro de la literatura el aislamiento de la información, seguridad en el internet, la notación y tratamiento de incidentes, la seguridad de los computadores, el uso del correo electrónico dispositivos móviles.

# CAPITULO IV

# 4. RESULTADOS Y DISCUSIÓN

## 4.1.Resultados y discusión

Los resultados se obtienes después de comparar los 6 criterios con sus respectivos ítem y en la tabla 9 se obtuvo los resultados con un puntaje de 44 la metodología ENISA es la seleccionada para la creación de la guía del prototipo CSIRT para la UNACH, en comparación con la metodología APCET que obtuvo un puntaje de 34 siendo descartada para la creación de este.

Con estos resultados se creó un documento en el cual, se plasma la metodología ENISA con sus respectivos pasos para la creación de este prototipo CSIRT en el cual también consta de un Plan estratégico y Plan Operativo que se debe tomar en cuenta porque esta acoplado a los distintos parámetros que tiene el departamento de Tecnologías de la Información y Comunicación de la UNACH, también se entregó este documento al director del departamento DTIC de la institución para que sea evaluado y puesto en conocimiento a las autoridades para su posterior desarrollo, implementación y evaluación del mismo, a continuación, se muestra los distintos componentes que se utilizó para la comparación de las dos metodologías.

***Ilustración 16.*** *Comparación de los parámetros de las dos metodologías*

| Parámetros | ENISA | APCERT |
|---|---|---|
| Categoría software | 6 | 5 |
| Categoría hardware | 6 | 7 |
| Categoría equipos de oficina | 3 | 2 |
| Categoría medidas de control | 9 | 9 |
| Categoría macro controles | 6 | 5 |
| Categoría aspectos de seguridad | 14 | 6 |
| **Total** | **44** | **34** |

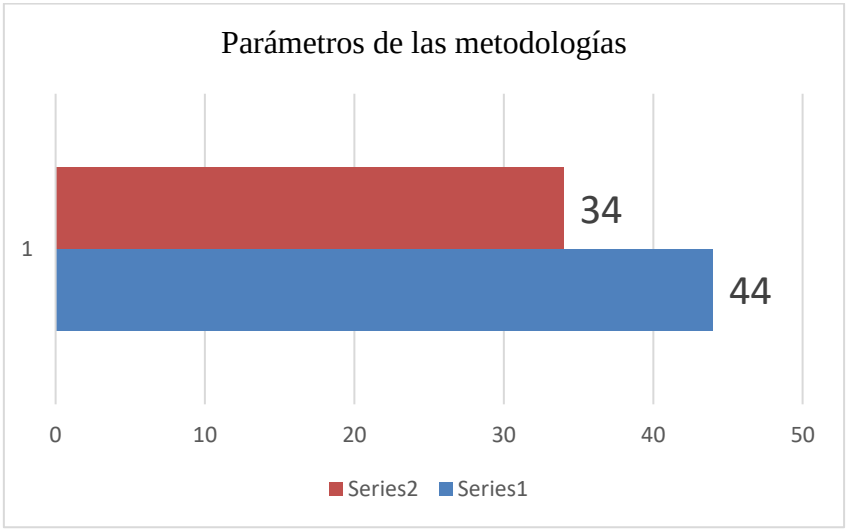



***Ilustración 17.*** *Porcentaje de la comparación de ENISA y APCERT*

Dentro de la categoría software se puede observar que la metodología ENISA cumple con 7 parámetros dentro de la revisión literaria no cuenta que sea multiplataforma y que tenga software libre frente a la metodología APCERT que cumple 5 parámetros en la cual, no tiene herramientas de hacking y herramientas para administrar políticas de evaluación de riesgos y contingencia.

Al momento que se realizó la comparación de los componentes de las dos metodologías se observó que la metodología APCERT cumple con 7 parámetros, frente a la metodología ENISA que tiene 6 parámetros en la que no consta de equipos adicionales.

Dentro de la categoría equipos de oficina la metodología ENISA cumple con 3 parámetros frente a la metodología APCERT que solo tiene 2 parámetros la cual, no cumple en la literatura con la contratación de los servicios básicos debido a que lo esencial y fundamental es el suministro de oficina.

En la categoría medidas de control se puede observar que las dos metodologías brindan estos servicios o componentes, es decir, para esas agencias es importante la seguridad de los empleados al momento de trabajar por ello, al momento de comparar dichos componentes se obtiene un valor de 9 puntos para cada metodología.

Dentro de los parámetros macro controles se puede visualizar que la metodología ENISA cumple con 6 puntos dentro de los cuales no toma en consideración dentro de la literatura revisada los incidentes de seguridad y la auditoría y control de la seguridad, en la metodología APCERT tiene 5 puntos en los que no se toma en cuenta las políticas de seguridad, gestión de activos y dar mantenimiento a los sistemas informáticos que van en decadencia.

Dentro de la categoría políticas de seguridad se puede observar que la metodología ENISA cumple con 14 puntos esenciales dentro de la creación de un CSIRT, a diferencia de la metodología APCERT que cumple con 6 puntos en los que no toma en cuenta dentro de la literatura el aislamiento de la información, seguridad en el internet, la notación y tratamiento de incidentes, la seguridad de los computadores, el uso del correo electrónico dispositivos móviles.

Después de haber realizado la comparación de las metodologías con un total de 44 puntos la metodología ENISA es la seleccionada sobre la metodología APCERT que obtuvo un puntaje de 34 por ello, se procede a la creación del prototipo CSIRT con la metodología ENISA, tal como se lo muestra en el ANEXO 3.

## 5. CONCLUSIONES

- Con la investigación de las dos metodologías tanto ENISA y APCERT se conoce las definiciones, características y aspectos importante para cada una de ellas, debido a que son dos metodologías diferentes porque son utilizadas en distintos países, pero con un mismo objetivo y es contrarrestar a los ataques tanto internos y externos en las organizaciones que deciden implementar un centro de Respuesta a Incidentes de Seguridad Informática.
- Al momento de la selección de una de las metodologías se comparó algunos componentes tanto software, hardware, equipos de oficina, medidas de control, macro controles y políticas de seguridad en el cual, se obtuvo un puntaje de 44 de la metodología ENISA frente a la metodología APCERT con un puntaje de 34 es decir, el prototipo CSIRT se realizó con dicha metodología siguiendo todos los pasos y acoplando con los parámetros e infraestructura que tiene la UNACH para la creación del prototipo CSIRT de acuerdo con el departamento de tecnologías de la Información y Comunicación.
- Una vez seleccionada la metodología se procede a la creación del documento denominado prototipo CSIRT según la metodología ENISA, dicho documento tiene como objetivo dar a conocer paso a paso las actividades que debe seguir para que el proyecto sea de éxito, el mismo que cuenta con un plan estratégico que debe acoplar el departamento de Tecnologías de la Información y Comunicación.

## 6. RECOMENDACIONES

- Las instituciones educativas deben tener implementado un Centro de Respuestas a Incidentes de Seguridad Informáticos los cuales ayuden a mitigar los ataques que puedan ocurrir dentro de la organización para tener sus datos e información protegida al momento en que la comunidad universitaria desee ocuparlos, la implementación de este centro es muy costoso y la institución debe realizar un financiamiento el cual ayudaría a la institución y en especial al Departamento de Tecnologías de la Información y Comunicación.
- Una vez concluido el documento de la propuesta de la creación del prototipo CSIRT el departamento de Tecnologías de la Información y Comunicación de la UNACH se debe realizar una reunión con las partes interesadas a crear este centro que ayudará a mitigar los incidentes de seguridad para tener protegido sus activos.
- Todo el personal debe estar especialmente capacitado para poder dirigir correctamente esta área si se lo a implementar porque entre una de sus prioridades es mantener protegida la información de toda la comunidad universitaria y que esté disponible al momento que lo quieran utilizar.

## 7. BIBLIOGRAFÍA


Andrade , R. (2013). Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) para la escuela politécnica del ejercito. *ESPE*, 1-111. Obtenido de https://docplayer.es/6807913-Escuela-politecnica-del-ejercito-vicerrectorado-deinvestigacion-y-vinculacion-con-la-colectividad-unidad-de-gestion-de-posgrados.html

*APCERT*. (2018). Obtenido de APCERT: http://www.apcert.org/about/mission/index.html

*APCERT*. (2019). Obtenido de APCERT: https://www.apcert.org/documents/pdf/apcert-vision-march30.pdf

*APCERT POC Arrangements Policy*. (2013). Obtenido de APCERT POC Arrangements Policy: https://www.apcert.org/documents/pdf/APCERT_POC_Arrangements_Policy(20131204).pdf

*APCERT Repositorio CIMAT*. (2018). Obtenido de APCERT Repositorio CIMAT: file:///D:/Users/Monica%20Chacha/Downloads/ZACTE42%20(3).pdf

Armas , H. (2012). GESTIÓN DE SEGURIDAD EN LA RED DE DATOS DE LA CORTE COSNTITUCIONAL MEDIANTE EL DISEÑO DE UN CSIRT (EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD). *Repositorio Institucional de la Universidad Politécnica Salesiana*, 139-200. Obtenido de https://dspace.ups.edu.ec/bitstream/123456789/3776/6/UPS%20-%20ST000898.pdf

*Asia Pacific Computer Emergency Response Team (APCERT)*. (2017). Obtenido de Asia Pacific Computer Emergency Response Team (APCERT): http://www.apcert.org/documents/pdf/APCERT%20Operational%20Framework%20November%202017.pdf

Bada , M., Creese, S., Goldsmith, M., Mitchell, C., & Phillips, E. (2014). Computer Security Incident Response Teams(CSIRTs). *Global Cyber Security*, 1-23. Obtenido de https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/CSIRTs.pdf

Carozo, E., Martínez , C., & Vidal , L. (2010). CERTuy: Hacia un CSIRT Nacional. *telcom*, 1-6. Obtenido de https://iie.fing.edu.uy/eventos/telcom2006/trabajos/mvdtelcom-013.pdf

Castillo, C. (2010). LA AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN. *Iustel*, 1-16. Obtenido de http://www.juntadeandalucia.es/institutodeadministracionpublica/anuario/articulos/ descargas/01_EST_02_castillo.pdf

Chelo, M. (2004). Organización y operación de un CSIRT. *Rediris*, 1-81. Obtenido de https://www.rediris.es/cert/doc/reuniones/fs2004/archivo/csirt.pdf

Cormack, A., Kossakowski, K., Maj, M., Parker , D., & Stikvoort, D. (2005-2017). CCoP - CSIRT Code of Practice. *TLP:WHITE*, 1-5. Obtenido de https://www.trusted-introducer.org/TI-CCoP.pdf

*CSIRT_setting_up_guide_ENISA*. (2010). Obtenido de CSIRT_setting_up_guide_ENISA: file:///D:/Users/Monica%20Chacha/Downloads/CSIRT_setting_up_guide_ENISA-ES%20.pdf

De la Torre, H., & Parra , M. (2018). Estrategias y diseño de un equipo de respuestas ante incidentes de seguridad informatica (CSIRT) academico para la Universidad de las Fuerzas armadas ESPE. *ESPE*, 1-131. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/15071/1/T-ESPE-040447.pdf

De la Torre, H., & Parra, M. (2018). ESTRATEGIA Y DISEÑO DE UN EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMATICA (CSIRT) ACADEMICO PARA LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE. *Repositorio ESPE*, 1-131. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/15071/1/T-ESPE-040447.pdf#page=28&zoom=100,0,242

*ENISA*. (2016). Obtenido de ENISA: https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport

*Enisa*. (2017). Obtenido de Enisa: https://www.enisa.europa.eu/about-enisa

*Europa*. (2004). Obtenido de Europa: https://europa.eu/european-union/about-eu/agencies/enisa_es

Guacho, D. (2014). Guacho Morocho, D. D. (2014). Diseño de un Sistema de Seguridad de la Información para EcuCERT. *EPN*, 26-34. Obtenido de https://bibdigital.epn.edu.ec/bitstream/15000/8855/1/CD-5930.pdf

*Incidente APCERT*. (2019). Obtenido de Incidente APCERT: https://www.apcert.org/documents/pdf/20090908-Recent_Information_Sharing_Incident.pdf

Mejia , J., & Ramirez, H. (2016). Estableciendo controles y perímetro de seguridad para una página web de un CSIRT. *RISTI*, 1-15. Obtenido de http://www.scielo.mec.pt/scielo.php?script=sci_arttext&pid=S1646-98952016000100002&lng=es&nrm=iso&tlng=es

MURQUINCHO , D., CHALÁN, F., MONTESINOS , M., & ULLOA, C. (26 de 03 de 2018). *studocu*. Obtenido de studocu: https://www.studocu.com/es/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/reporte-tecnico-de-vulnerabilidades-informaticas/4496587/view?fbclid=IwAR1ZfM21t2yPkvzyYwabjTMNQUqFpMEV-r7gLSd7PiTiFrvDl4wAfE13SOA

Murquincho, D. (12 de 02 de 2019). *studocu*. Obtenido de studocu: https://www.studocu.com/es/document/universidad-nacional-de-loja/seguridad-de-la-informacion/resumenes/articulo-revision-sistematica-csirt/4027803/view?fbclid=IwAR1ZfM21t2yPkvzyYwabjTMNQUqFpMEV-r7gLSd7PiTiFrvDl4wAfE13SOA

Palacio , P. (2018). "EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMATICOS PARA LA UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES "UNIANDES". *DSpace*, 1-110. Obtenido de http://dspace.uniandes.edu.ec/handle/123456789/8158

*parámetros ENISA*. (2017). Obtenido de parámetros ENISA: https://www.ituser.es/seguridad/2017/06/enisa-publica-una-nueva-guia-practica-para-medir-la-madurez-de-los-csirt

Paredes , O., & Andrade , R. (2013). Artículo científico - Diseño y dimensionamiento de un equipo de respuesta ante incidentes de seguridad informática (CSIRT) para la Escuela Politécnica del Ejército. *ESPE*, 1-20. Obtenido de http://repositorio.espe.edu.ec/handle/21000/6972

Ramírez , H., & Miranda , J. (2015). Propuesta de infraestructura técnica de seguridad para un Equipo de Respuesta ante Incidentes de Seguridad (CSIRT). *Centro de Investigación en Matemáticas (CIMAT)*, 1-16. Obtenido de https://docplayer.es/141012964-Departamento-de-ciencias-de-la-computacion.html

Salinas , E., & Marin , E. (2019). MODELO DE ANÁLISIS Y SELECCIÓN DE HERRAMIENTAS DE CIBERSEGURIDAD PARA UN CSIRT ACADÉMICO:

CASO CSIRT-ESPE. *Repositorio ESPE*, 1-184. Obtenido de http://repositorio.espe.edu.ec/bitstream/21000/20843/1/T-ESPE-039768.pdf

Sasia, D. (2015). Obtenido de https://es.slideshare.net/danielsasia/gestin-de-incidentes-de-seguridad-de-la-informacin-cert-csirt

*Terena_ENISA*. (2018). Obtenido de Terena_ENISA: https://www.terena.org/activities/tf-csirt/starter-kit.html

*UNACH*. (2019). Obtenido de UNACH: http://sgc.unach.edu.ec/sgc_estructura_org/

*welivesecurity*. (2015). Obtenido de welivesecurity: https://www.welivesecurity.com/la-es/2015/05/18/que-es-como-trabaja-csirt-respuesta-incidentes/

## Anexos

### Anexo N.° 1

### AGENCIA EUROPEA DE SEGURIDAD DE LAS REDES Y DE LA INFORMACIÓN (ENISA) Y SU METODOLOGÍA

Al momento de construir un CSIRT académico se debe tomar en cuenta la declaración de la misión, visión, unidad constitutiva y organizaciones relacionadas, es decir, esto está dentro del plan estratégico en el cual consta la categorización del incidente, las políticas de divulgación y los procedimientos de escalación, esto va acompañado de la implementación del sistema de manejo de incidentes y capacitación del personal clave, así como establecer el contacto con otros CSIRT (Terena_ENISA, 2018). La agencia trabaja con los estados miembros y el sector privado para ofrecer asesoramiento y soluciones en el tema de ciberseguridad, en el desarrollo y la evaluación de estrategias nacionales de ciberseguridad, la cooperación de los CSIRT, estudio de la infraestructura inteligente que aborda problemas de protección de datos, tecnología que mejore la privacidad y privacidad en tecnologías emergente (Enisa, 2017). Para la creación del CSIRT se debe seguir la metodología ENISA que se presenta a continuación en la cual se describe paso a paso como se debe crear este prototipo CSIRT (CSIRT_setting_up_guide_ENISA, 2010):

#### METODOLOGIA ENISA UTILIZADA PARA EL PROTOTIPO CSIRT

Introducción

- Público destinatario

Estrategia para crear un CSIRT mediante una planificación

- Recopilación de la información del CSIRT
- Características y beneficios de la institución al contar con un CSIRT
- Tipo de CSIRT a utilizar

- Servicios con los que va a contar el CSIRT dentro de la institución
- Personal del CSIRT y descripción de los servicios

Desplegar un plan comercial en la institución

- Delimitar el modelo financiero dentro de la institución
- Precisar la estructura organizativa de la institución
- Desarrollar políticas de seguridad para la información
- Buscar entidades patrocinadoras para el CSIRT

Iniciar el plan comercial en la institución

- Describir todo lo que contiene un plan y bajo la dirección de quién está el desarrollo

Pasos para los procedimientos operativos y técnicos

- Evaluación e instalación del personal del CSRT
- Servicios que va a brindar el CSIRT (generación de alertas y advertencias, tratamiento de incidentes, plan de respuesta y herramientas disponibles en la institución)

Alinear al personal adecuado con las instituciones internacionales

- TRANSITS
- CERT/CC

**Anexo N.° 2**

## EQUIPO DE RESPUESTA A EMERGENCIAS INFORMÁTICAS DE ASIA PACÍFICO (APCERT) Y SU METODOLOGÍA

El equipo de respuesta a emergencias informáticas de Asia Pacífico mantiene una red confiable de contactos con los expertos en seguridad informática de la misma región para mejorar la conciencia y competencia de la región en relación con incidentes informáticos. También desarrolla medidas para hacer frente a los incidentes de seguridad de redes a gran escala o regionales, facilita el intercambio de información y tecnología incluida la seguridad de la información, virus informáticos y código malicioso entre sus miembros. También promueve la investigación y el desarrollo en temas de seguridad informática en la cual ayuda a otros CERT y CSIRT de la región a realizar una respuesta de emergencia informática eficiente y efectiva, proporciona aportes y recomendaciones para ayudar a abordar problemas legales relacionados con la seguridad informática y la respuesta a emergencias a través de las fronteras regionales (APCERT, 2018). A continuación, se presenta la propuesta de creación del CSIRT con la metodología descrita (Asia Pacific Computer Emergency Response Team (APCERT), 2017):

### METODOLOGÍA APCERT

Dentro de la metodología APCERT conta de los siguientes pasos que son: Marco operativo, políticas y procedimientos

**APCERT Marco Operativo**

Miembros

- Categorías de miembros y asociaciones
- Formulario de Solicitud para Miembros Operativos
- Memorando de entendimiento para los asociados
- Lista de verificación de solicitudes de membresía (para patrocinador)

- Preguntas frecuentes sobre la membresía

Estructura organizativa

Misión

Código de conducta

Listas de distribuciones

- Procedimientos de listas de correo

Disposiciones relativas a los puntos de contacto

- Política de acuerdos de puntos de contacto (POC)
- Directrices para los acuerdos de puntos de contacto
- Directrices para los asociados estratégicos y de enlace
- Formulario de punto de contacto (POC)

**Procedimientos para cambiar las políticas y procedimientos de la APCERT**

Procesos electorales

- Procedimientos para la elección de los miembros del Comité Directivo de la APCERT

Archivo

- Propuesta de creación de la APCERT.

**Anexo N.° 3**

**UNIVERSIDAD NACIONAL DE CHIMBORAZO**

**DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

# GUÍA DEL PROTOTIPO CSIRT SEGÚN LA METODOLOGÍA ENISA


**Autor:**

Mónica Estefanía Chacha Chunata

**Tutor:**

Ing. Lorena Paulina Molina Valdiviezo, Ph.D.


**Año:**

2019

# PROTOTIPO CSIRT SEGÚN LA METODOLOGÍA ENISA

## 1. Introducción

En el transcurso de los años la tecnología avanza con una capacidad impresionante por lo que las empresas deben estar a la vanguardia para que no sufran ningún ataque o vulnerabilidad dentro de su organización. Por ello existen distintas organizaciones que ayudan a la creación de centros de respuesta a incidentes informáticos, como es el caso de la Agencia de Seguridad de las Redes y de la Información de la Unión Europea (ENISA). Esta agencia ayuda a que las organizaciones estén preparadas para prever, detectar y dar solución a los problemas de seguridad de la información, también brinda asesoramiento ante cualquier vulnerabilidad presentada la cual es documentada y con su respectivo informe para su resolución.

Esta organización ha formado una amplia red de interesados para consultas en el ámbito público y privado con el objetivo de crear experiencia, políticas, capacidad y comunidad entre sus interesados. Los principales beneficiarios son el sector público que brindan servicio a los gobiernos e instituciones de los países en la Unión Europea, asimismo brinda servicio a la industria de Tecnologías de la Información y Comunicación (Europa, 2004).

La Universidad Nacional de Chimborazo al ser una institución de educación superior está en la necesidad de contar con este centro, la cual está expuesta a diversas vulnerabilidades y ataques ya sea por robo de información o por alterar los datos y que estos no estén disponibles cuando la comunidad universitaria lo requiera, por esta razón vamos a seguir la metodología ENISA para crear un prototipo el cual será analizado y valorado para que la Universidad vea si es necesario o no su implementación.

### 1.1. Público destinatario

Los principales beneficiarios de este proyecto es la Universidad Nacional de Chimborazo (UNACH) la cual cuenta con su departamento de Tecnologías de la Información y Comunicación (DTIC), los cuales van a ser los encargados de valorar este documento y ver si la Universidad requiere implementar este Centro de Respuesta a Incidentes Informáticos.

## 2. Estrategia general de planificación y creación de un CSIRT

Con el proceso de creación del CSIRT se debe tener en cuenta al grupo de clientes atendidos, es decir, la comunidad universitaria, el DTIC, docentes, administrativos y estudiantes debido a que ellos van a ser los principales beneficiarios porque se va a tener un mejor tratamiento de los servicios que proporciona la Universidad para que no sufra ninguna vulnerabilidad o ataque, con ello los datos y servicios están disponibles al momento en que lo necesiten,

### 2.1. Definición del CSIRT

Es un equipo de respuesta ante incidentes de Seguridad Informática es un equipo de expertos responsables de desarrollar medidas preventivas y reactivas ante incidentes de seguridad en los sistemas de información, también estudia el estado de seguridad global de redes y ordenadores, los cuales proporciona servicios de respuesta ante incidentes a víctimas y ataques en la red y publica alertas relativas de seguridad en los sistemas.

La principal característica para destacar por la que se crean estos Centros de Respuesta a Incidentes de Seguridad Informática es que existe un incremento de las amenazas informáticas, la aparición de leyes y regulaciones que están orientadas a la protección de la información (welivesecurity, 2015).

## 2.2. Ventajas de contar con un CSIRT

- La respuesta está focalizada
- Respuesta rápida, coordinada y generalizada
- Equipo estable de saber cómo gestionar el incidente
- Lugar estratégico de coordinación y diseminación de información
- Colaboración con la comunidad de seguridad informática (Sasia, 2015)

## 2.3. Descripción del CSIRT académico

Estos centros optan por tener bajo su responsabilidad a instituciones educativas que están conformadas por estudiantes y personal de Universidades o Colegios, es decir se dimensiona por la comunidad y los servicios que va a brindar el CSIRT (De la Torre & Parra, 2018).

## 2.4. Servicios posibles de un CSIRT

Son muchos los servicios que brinda el CSIRT para tener a la organización protegida ante cualquier tipo de imprevisto que se presente ya sea de un ataque o vulnerabilidad, como son muchos los servicios que ofrece el CSIRT a continuación se describe brevemente cuales son:

**Servicios reactivos**

Este servicio se inicia ante un evento o pedido, es como un informe de un computador el cual tiene distintos componentes esenciales los cuales están siendo vulnerables, los servicios reactivos son el componente principal del trabajo del CSIRT, los principales servicios reactivos son:

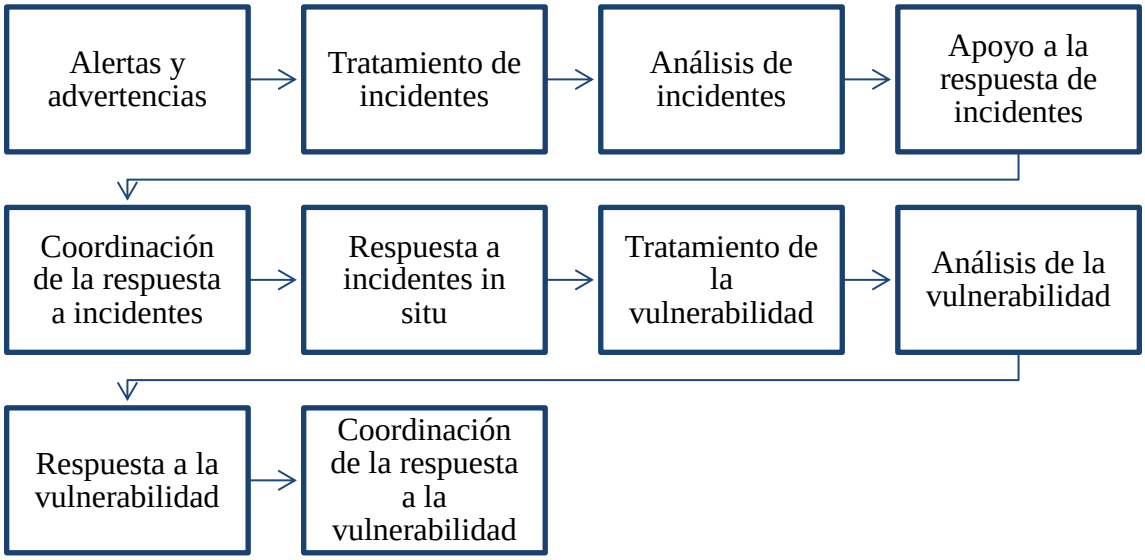



***Ilustración 18.*** *Servicios reactivos*

**Servicios proactivos**

Este servicio ofrece asistencia e información para ayudar a preparar, proteger y asegurar los sistemas de los miembros del área de cobertura los cuales pueden anticipar ataques, problemas o cualquier vulnerabilidad, estos servicios reducirán la cantidad de incidentes en el futuro, los principales servicios proactivos son:

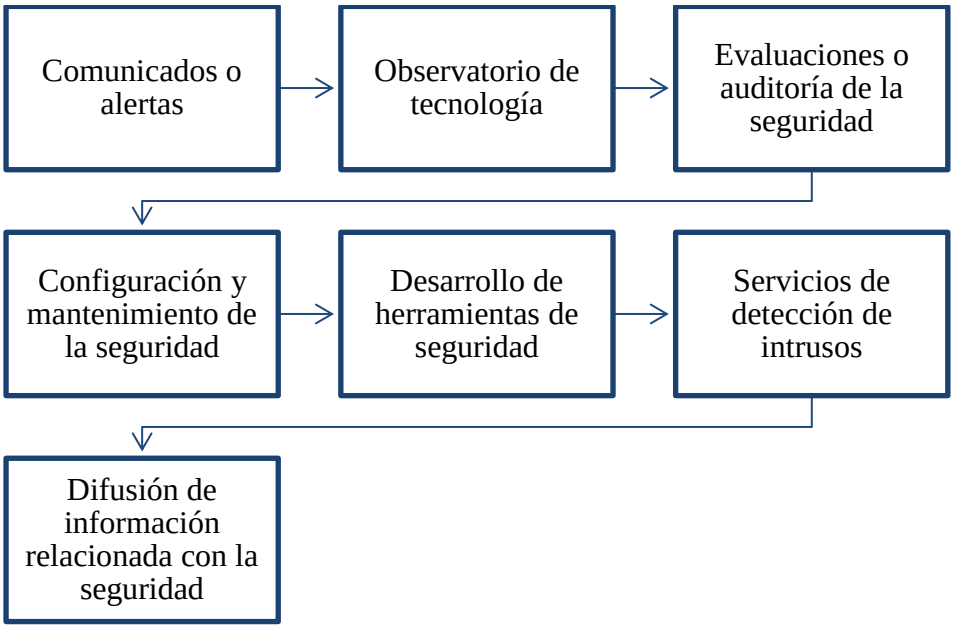



***Ilustración 19.*** *Servicios proactivos*

**Servicios para la gestión de la calidad de la seguridad**

Estos servicios son independientes del manejo de incidentes debido a que son llevados a cabo por otras áreas de una organización tales como el departamento de Tecnologías de la Información y Comunicación, auditoria de la Universidad y por medio del departamento de capacitación, dentro de los servicios para la gestión de la seguridad de la información se obtiene:

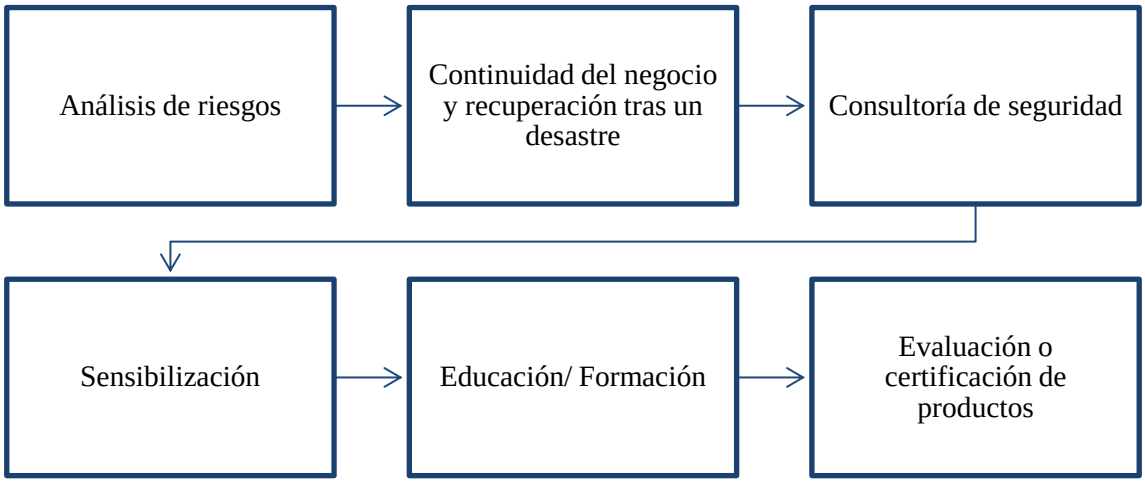



***Ilustración 20**. Servicios para la gestión de la calidad de la información*

**2.5. Analizar del grupo de clientes atendidos y declarar los servicios**

En este apartado se va a definir el enfoque de la organización, es decir el grupo de clientes atendidos, definir los procesos, preparar el plan estratégico, definir los servicios, la estructura organizacional, las políticas de seguridad de la información, controlar el personal adecuado, adecuación de las oficinas y la permanente colaboración con otros CSIRT nacionales, como se ve plasmado en el plan estratégico

## 3. Desarrollar un plan comercial

### 3.1. Definir el modelo financiero

En este paso se procede a reflexionar acerca de la financiación con que se va a realizar este proyecto, los parámetros que se va a implementar para que sus servicios sean asequibles y adecuados. Este financiamiento debe ser debidamente planificado por el departamento de Tecnologías de la Información y Comunicación de la Universidad para que sea considerado en el presupuesto de la Institución.

### 3.2. Definir la estructura organizativa

Al momento de definir la estructura organizativa del CSIRT se debe tomar en cuenta el grupo de clientes atendidos, y si la organización está en posibilidades de contratar expertos para estas áreas y cubrir todas las necesidades que hagan falta. Dentro de un CSIRT se tienen las siguientes funciones que debe tener un equipo.

**General**

- Director del departamento de Tecnologías de la Información y Comunicación

**Personal a nivel institucional**

- Asesor para la contabilidad
- Asesor de las distintas instituciones relacionadas
- Asesor legal

**Equipo técnico del CSIRT en la UNACH**

- Director del equipo técnico
- Expertos del CSIRT, ellos son los encargados de prestar los servicios del CSIRT
- Investigadores en temas de ataques informáticos

**Consultores externos**

- Se contrata cuando sea necesario

Dependiendo del conocimiento que tengan el personal del Departamento de Tecnologías de la Información y Comunicación de la UNACH se verá en la obligación de contratar personal adecuado para que desarrollen las funciones requeridas del CSIRT y así poder brindar diferentes servicios para la comunidad universitaria, también es necesario contar con un abogado dentro de este equipo porque nos puede ayudar a evitar problemas legales los cuales puedan afectar a la organización.

### 3.3. Contratar al personal adecuado

Para todos los servicios que va a brindar el CSIRT se debe tener el personal adecuado, por ende, se debe hacer la contratación adecuada de los expertos que van a dar tratamiento y solución a cualquier tipo de ataque o vulnerabilidad que se presente dentro de la institución.

### 3.4. Uso y equipamiento de la oficina

Dentro de este apartado se podrá definir las oficinas, los laboratorios, la seguridad física y lógica que debe tener el área en que se va a implementar el CSIRT.

Al momento de preparar el edificio se debe considerar un lugar que este protegido de cualquier desastre natural al que pueda estar expuesto, también de que exista una infraestructura en perfectas condiciones, con instalaciones de energía eléctrica en la cual se pueda operar de una eficiente y eficaz. Las oficinas donde se va a implementar el CSIRT debe tener normas generales del edificio, el equipamiento tanto software y hardware, debe estar en un constante mantenimiento de los canales de comunicación y los sistemas de localización de registros los cuales deben funcionar correctamente.

### 3.5. Desarrollar una política de seguridad de la información

Para desarrollar una política de seguridad que se va a implementar en el CSIRT académico se debe tener en cuenta que existen diferentes normas a las cuales se debe regir, las políticas que existen son: nacionales, europeas, internacionales y las normas. Para conocer si el CSIRT cumple las políticas tanto nacionales e internacionales se debe tener en cuenta la siguiente información, como se va a clasificar y manejar la información, que se debe realizar si es revelada la información confidencial a otros dispositivos o sitios relacionados con incidentes de seguridad, que consideraciones legales se toma a la hora de que la información no ha sido encriptada, debido a que los archivos, los datos y correo electrónico son vulnerables, posee una custodia de las claves de terceros y la desencriptación en caso de que haya una controversia.

### 3.6. Buscar la colaboración con otros CSIRT y participar en iniciativas nacionales

Para buscar la colaboración de otros CSIRT es necesario contar primeramente con una institución que nos colabore como es el caso de la organización CEDIA a la cual pertenece la UNACH, por medio de esta institución se podría hacer convenios y contratos con los CSIRT tanto nacionales e internacionales, los cuales nos pueden ayudar con capacitación y ver la mejor manera de que el proyecto salga a flote y no se quede en una propuesta.

## 4. Promover el plan comercial

Dentro de este proceso lo que se debe determinar es un plan de negocio que sirva para que se lleve a cabo este proyecto, el cual debe servir para que otras instituciones colaboren y apoyen a la gestión y lo más importante es para que exista el financiamiento necesario. Para tener un modelo de negocios se debe tener en cuenta al grupo de clientes atendidos, los servicios y productos que se va a ofertar al

momento de crear el CSIRT, por ello se debe tener la colaboración de todos para que este proyecto se lleve a cabo de la mejor manera, para que no exista ninguna dificultad se debe tener en cuenta que se necesita un constante apoyo del departamento de Tecnologías de la Información y Comunicación (DITC) de la universidad.

### 4.1. Describir los planes de negocios

Se debe describir una presentación a la dirección del DTIC para la promoción del CSIRT, en donde ellos se comprometen a ayudar a la creación de este, se debe socializar este plan también al grupo de clientes atendidos para que ayude a la orientación y dirección al momento que se decida crear el CSIRT.

Dentro del plan se debe tener en cuenta en que consiste el problema, que objetivos le gustaría alcanzar con los clientes atendidos, que pasa si no se hace o si se reaccionada ante un ataque o vulnerabilidad, el costo, que se conseguirá en un fututo y cuál es el calendario que se debe seguir.

## 5. Procedimientos operativos y técnicos

Dentro de este apartado se verá el CSIRT en funcionamiento, es decir, con los métodos, procedimientos, para tratar una vulnerabilidad, aquí es donde el CSIRT va a brindar tres aspectos fundamentales para solucionar una vulnerabilidad que son: alertas y advertencias, tratamiento de los incidentes y el comunicado o solución.

### 5.1. Evaluación de la base de instalación del grupo de clientes atendidos

Se procede a conocer todos los servicios y sistemas que tiene instalado el DTIC de la universidad, de este modo el CSIRT podrá evaluar la información que se filtre o devolver la información necesaria de acuerdo con estos equipos.

Esta área debe contar principalmente con estos equipos, servicios y accesorios.

- Computadores personales

- Computadores portátiles
- Data center
- Red
- Telefonía
- Servidores
- Servicios

### 5.2. Generación de alertas, advertencias y comunicados

Para la generación de alertas y advertencias se sigue un esquema que está determinado por el CSIRT que conta de cuatro pasos:

- **Recopilación de la información**

  Al momento en que se produzca una vulnerabilidad la empresa y su infraestructura se verá vulnerable, es decir toca identificar la fuente por la cual se está transmitiendo esta vulnerabilidad, las fuentes por las que se puede realizar una vulnerabilidad son: correos electrónicos, los proveedores de los productos, sitios web e información de internet ya sea en sitios públicos o privados.

- **Evaluación de la información de la pertinencia y la fuente**

  Se procede a identificar la vulnerabilidad antes de ser transmitida al grupo de clientes atendidos, se debe determinar si la fuente es confiable porque no se puede generar alertas innecesarias las cuales producirían molestias para el grupo de clientes atendidos y la empresa se vería perjudicada.

  Para tener una pertinencia de la vulnerabilidad se debe utilizar tanto el software y hardware instalado para filtrar la información, para dar una oportuna solución de esta. Se debe clasificar la información porque los

informes de incidentes que llega a otros equipos son restringidos, es decir, al manejar la información siempre se debe tener en consideración las políticas de la institución y de los beneficiarios al momento de distribuir la información si no tiene claro que se debe hacer, y si tiene duda preguntar al remitente o a la persona que está dirigiendo el incidente.

- **Evaluación del riesgo sobre la información que se tiene**

  Existen varas formas de determinar los riesgos y las consecuencias que puede ocasionar una vulnerabilidad, los factores que se debe tener en cuenta son: si la vulnerabilidad es reconocida, si es extendida, es fácil de explorar y si se trata de una vulnerabilidad que se puede explorar de forma remota.

  Con una vulnerabilidad grave se puede tener daños potenciales que son: acceso no autorizado a los datos, denegación de servicios (DOS) y la obtención o ampliación de permisos.

- **Distribución de la información**

  Cada CSIRT tiene sus métodos para distribuir la información ya sea al grupo de clientes atendidos o a su propia organización, esta información puede ser distribuida por medio de sitios web, correos electrónicos, informes y archivos e investigaciones.

### 5.3. Tratamiento de los incidentes

Para realizar el tratamiento de los incidentes se debe realizar un informe por parte de la organización o las personas que están llevando ese tipo de incidente, posteriormente se pide ayuda al grupo de clientes atendidos porque ellos tienen informes de otros incidentes relacionados, por lo general la información que se solicita circula por correo electrónico, por fax o por teléfono. Al momento que se

recibe información de un incidente por teléfono se debe generar un número de incidente, el cual servirá de referencia en las posteriores comunicaciones, porque todos los informes de incidentes se reportan con un número de incidente que queda registrado para su posterior generación de reporte.

Para realizar un tratamiento de incidentes se debe generar la siguiente información:

- **Recepción de los informes de incidentes**

  Los comunicados de los incidentes siempre van a llegan al CSIRT por diferentes canales de comunicación que son muy usuales como son correo electrónico, teléfono o fax. Para recibir el incidente se debe generar un modelo de informes de incidentes en el cual se va a anotar toda la información necesaria para asegurar que no se olvide ningún dato importante.

- **Evaluación del incidente**

  En este paso se identifica la autenticidad, la pertinencia y se clasifica el incidente. Por ende se identifica si el incidente es verídico para no realizar acciones indebidas las cuales pueden afectar a la organización, es decir, este aviso de incidente debe venir del grupo de clientes atendidos por el CSIRT o si este incidente afecta a los sistemas de TI del grupo atendido aquí se determina la pertinencia y por último se le clasifica por medio de un triage el cual clasifica al incidente según su gravedad, se puede utilizar herramientas que el CSIRT mismo brinda para clasificar el incidente.

**Que es el triage**

Es un elemento esencial para gestionar los incidentes dentro de un CSIRT, con el triage se puede entender mejor que es lo que la organización está comunicando. Por este canal llega la información a un único lugar donde se pueda relacionar los

distintos canales por donde está siendo vulnerable la institución, también ayuda a realizar una evaluación inicial del informe que entra y lo registra a la espera de que le dé un curso, también es un punto de partida porque se puede empezar a documentar y a archivar el incidente por los pasos que se sigue para su solución.

Con el triage se puede identificar problemas de seguridad potenciales y a establecer prioridades de trabajo, para dar una solución oprima teniendo en cuenta cual es el canal vulnerable y aplicando parches informáticos hasta su solución adecuada para que ya no existan estos incidentes dentro de la institución, también generar estadísticas para los ejecutivos de alto nivel. Los encargados de manejar el triage son las personas capacitadas dentro del personal del DTIC, así mismo tiene la potestad de designar al personal que se va a encargar de dar solución al incidente.

- **Acciones**

Los incidentes que son sometidos a un triage se incluyen a la lista de peticiones de una herramienta de tratamiento de incidentes, en los cuales se debe dar los siguientes pasos: resguardo de incidentes, ciclo de vida del incidente, informe de tratamiento de incidente y archivarlo.

Dentro del resguardo del incidente se debe generar un número de incidente para poder reportarlo y si no es así, debe ser el primer paso para utilizarlo en comunicaciones posteriores sobre el incidente.

Dentro del ciclo de vida del incidente se sigue distintos pasos hasta que el incidente se resuelva y por fin las partes interesadas dispongan de toda la información necesaria. Dentro del ciclo de vida se debe tener en cuenta el análisis, es decir, la información del contacto, la asistencia técnica y la coordinación, este

ciclo termina cuando las partes interesadas han recibid la información y comunicación necesaria.

Es necesario contar con un informe o documento que sirva al personal para evitar errores en el tratamiento de incidentes en un futuro.

Al momento de archivar un incidente se debe tener en cuenta todos los procesos anteriores en especial las políticas de seguridad de la información.

### 5.4. Plan de respuesta o solución

El nivel de servicios debe estar bien constituido entre el CSIRT y el grupo de clientes atendidos, se debe tener en cuenta también los tiempos de respuesta porque con esto se puede prevenir una vulnerabilidad por ello siempre debe estar capacitado el personal del CSIRT sobre alguna vulnerabilidad que se suscitó debido a que es de un alto interés porque se vería afectada la reputación del equipo.

Para poner en marcha el plan de respuesta a una petición de incidente se debe seguir los siguientes pasos:

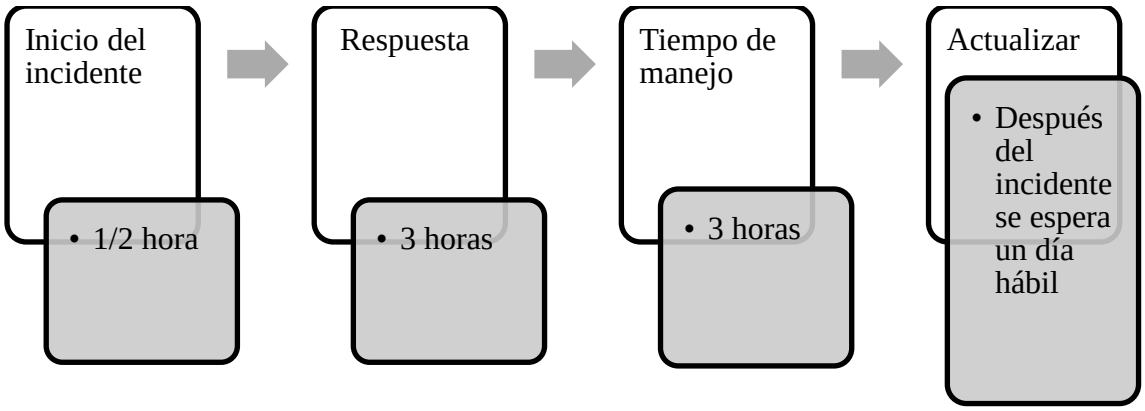



***Ilustración 21.*** *Plan de respuesta a una petición entrante*

Una buena práctica es informar al grupo de clientes atendidos sus tiempos de respuesta en especial cuando se trabaja con un CSIRT en una emergencia, es

importante ponerse en contacto con los CSIRT durante la fase temprana y apoyar si alguna persona tiene duda.

### 5.5. Herramientas disponibles para el CSIRT

Existen diferentes tipos de herramientas que son muy comunes para los CSIRT.

Dentro de los cuales se tiene software de encriptación de correos electrónicos y mensajes, herramientas de tratamiento de incidentes los cuales ayudan a administrar incidentes y darles un seguimiento adecuado con un rastreador de acciones, también herramientas de CRM es decir, el personal y técnicos del CSIRT deben estar registrados en una base de datos para que se mas fácil utilizar la información y quien va a estar a cargo del incidente y su resolución, además existen verificadores de la información los cuales ayudan a detectar actualizaciones y cambios en el sitio web, finalmente existen herramientas de búsqueda de información de contactos que ayudan a contactar al experto indicado para la comunicación de incidentes.

## 6. Formación del personal del CSIRT a nivel internacional

Las dos fuentes que se va a detallar a continuación son esenciales en la formación para el CSIRT.

### 6.1. TRANSITS

Es un proyecto de Europa, la cual tiene como objetivo la creación de los distintos centros de respuesta para la seguridad informática (CSIRT) en los distintos países y también contribuyen a mejorar los ya existentes con personal capacitado y cualificado con la capacitación respectiva en lo que es la organización, personal y políticas que se debe mejorar en la institución.

Tiene como objetivo desarrollar, actualizar y revisar el material de los módulos, organiza talleres de formación de material, capacita a los nuevos integrantes de

los CSIRT con la participación de distintos países y a distribuido el material de los cursos con bueno resultados.

### 6.2. CERT/CC

Al no contar con personal ni con prácticas de seguridad suficiente la infraestructura de red se vuelve vulnerable porque no se puede defender de los ataques para disminuir el daño que pueda ocasionar en la institución. Cuando una organización sufre un ataque debe ser rápida y eficaz al momento de responder a este echo debido que el incidente debe ser analizado para su posterior respuesta la cual nos permitirá defendernos de cualquier daño y que la organización no tenga pérdidas económicas, la mejor manera de protegernos de estos ataques es crear el CSIRT porque es una manera de contar con una rápida respuesta y ayudar a evitar incidentes informáticos. Esta organización brinda cursos de creación de CSIRT, también ayuda a mejorar la seguridad en las redes.

## 7. Conclusión

El principal objetivo de la creación de este documento es identificar los pasos que se debe seguir en la creación del CSIRT mediante la metodología ENISA, en la cual especifica claramente todo lo que debe tener una institución educativa, los requerimientos específicos en los laboratorios tanto físicos y lógicos para su buen funcionamiento, y si es posible la contratación del personal especializado lo cual debe estar implementado en el plan de financiamiento de la institución.

Dentro de la creación del CSIRT se pretende tener una visión general de los procesos, servicios, el personal atendido, las instituciones beneficiarias y como la comunidad universitaria en general se vería beneficiada, en especial el departamento de Tecnologías de la Información y Comunicación porque ellos son los más interesados en que todos los

servicios funcionen correctamente y que no exista ninguna vulnerabilidad al momento que se desee utilizar los servicios que brinda la institución.

**Anexo N.° 4**

**PROPUESTA DEL PLAN ESTARATEGICO PARA EL CSIRT DE LA UNACH**


# PLAN ESTRATEGICO

## 1. Introducción

Al momento de crear esta guía se pensó en la UNACH debido a que es una institución de educación superior y debe contar con un CSIRT, también se va a desarrollar un plan estratégico y operativo en el cual va a constar los distintos parámetros que debe tener el Departamento de Tecnologías de la Información y Comunicación (DTIC), para que no exista ningún inconveniente con la instituciones que van a ser colaboradoras para desarrollar esta propuesta la cual va a tener distintos servicios y sistemas que va a ofertar dentro del CSIRT. Esta guía está conformada por 5 etapas específicas que son: Estrategias, Diseño, Transición, Operación y mejora.

# FASE I: ESTRATEGIAS

### 1.1. Conformación del equipo inicial del proyecto

La persona encargada de poner en marcha este proyecto será el director del Departamento de Tecnologías de la Información y Comunicación (DTIC).

### 1.2. Definición del plan inicial de trabajo

Aquí se detalla las actividades preliminares que se debe llevar a cabo para desarrollar esta oferta en dicha institución.

Para realiazar un plan al momento que se quiere iniciar un trabajo de creación de un CSIRT en una institución beneficiaria se debe tener en cuenta los siguientes pasos:

- Estudiar la situación actual que tiene la UNACH tanto en infraestructura tanto física como lógica.
- Definir las instituciones que ayudaran a patrocinar este proyecto y la relación con otros CSIRT.

- Elaborar un plan estratégico de acuerdo con las características del CSIRT y de la UNACH
- Elaborar el plan operativo anual con el presupuesto adecuado que pueda contar la institución.
- Analizar los diferentes servicios que cuenta la UNACH y la elaboración del portafolio de los posibles servicios que pueda ofertar a la comunidad universitaria.
- Definir el modelo de la organización con el personal que se tiene y el personal que se debe contratar.
- Evaluar el estado físico del área en donde se va a posicionar el CSIRT con su respectivo personal y equipo para un buen funcionamiento.
- Elaborar planes de seguridad para proteger el estado físico y lógico de la UNACH con respecto a la seguridad de la información.
- Elaborar un presupuesto financiero tentativo para la adecuación de esta área dentro del DTIC.
- Elabora las actividades que se va a realizar cuando se vaya a implantar el proyecto.
- Definir los indicadores que se va a utilizar para la evaluación del proyecto.

### 1.3. Bitácora

La bitácora lleva el registro de todas las reuniones con sus respectivos responsables en el desarrollo del proyecto como se muestra a continuación.

CSIRT

dtic

**UNIVERSIDAD NACIONAL DE CHIMBORAZO**

**DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN**

**BITÁCORA DE REUNIONES CSIRT**

| Nro. | Fecha | Tema | Asistente | Firma | Observaciones |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

……..

**Director del DTIC**

## 1.4. Situación actual de la Universidad Nacional de Chimborazo (UNACH)

Para conocer la información actual de la UNACH se debe indagar en la página institucional en la cual nos brinda toda la información desde la misión, visión y todos los aspectos que existen dentro de ella, por consiguiente, a continuación, se muestra la información de la UNACH.

En 2014, Riobamba fue declarada "Ciudad Universitaria", un reconocimiento al trabajo, influencia y desarrollo, generados por sus instituciones de educación superior. La UNACH, como parte de este proceso, promueve la internacionalización de la cultura, la producción científica y económica de su sede, que tiene características únicas para compartir con el mundo. La UNACH formó en 2018 la Red de Innovación y Emprendimiento junto a 7 universidades de la región (UNACH, 2018).

Con el paso del tiempo y la madurez alcanzada en 23 años de vida institucional, la Universidad Nacional de Chimborazo ha debatido sobre el concepto de internacionalización, tratando de responder a la pregunta ¿Qué modelo de internacionalización enmarcará nuestras acciones frente a los problemas de la globalización?

- Enfoque centrado en la creación de una cultura institucional
- Reformular los currículos para formar profesionales globales
- Movilidad docente y estudiantil para intercambiar culturas
- Internacionalizar las relaciones colaborativas de investigación

La UNACH oferta en 2018 treinta y un carreras, las cuales son parte de cuatro facultades, y cuentan además con el apoyo de dos centros

Una vez revisado el plan institucional se obtiene la siguiente información organizacional.

**Misión de la UNACH**

Formar profesionales emprendedores que se incorporen al desarrollo productivo y socio económico local, regional y nacional para impulsarlo a través de un ejercicio profesional eficiente.

**Visión de la UNACH**

Emprender el proceso de enseñanza, aprendizaje de calidad en una sólida formación y técnica de liderar procesos encaminados a la solución de los problemas de la sociedad.

**Valores institucionales**

- Libertad
- Justicia
- Humanismo
- Equidad
- Autonomía Responsable
- Igualdad de oportunidades
- Laicismo
- Compromiso social
- Pluralismo
- Solidaridad y reciprocidad
- Armonía con la naturaleza
- Inclusión
- Participación
- Interculturalidad
- Rendición de cuentas

## Organigrama de la institución

A continuación, se muestra la estructura organizacional de la UNACH en la cual también se describen los procesos que existen dentro de la institución.

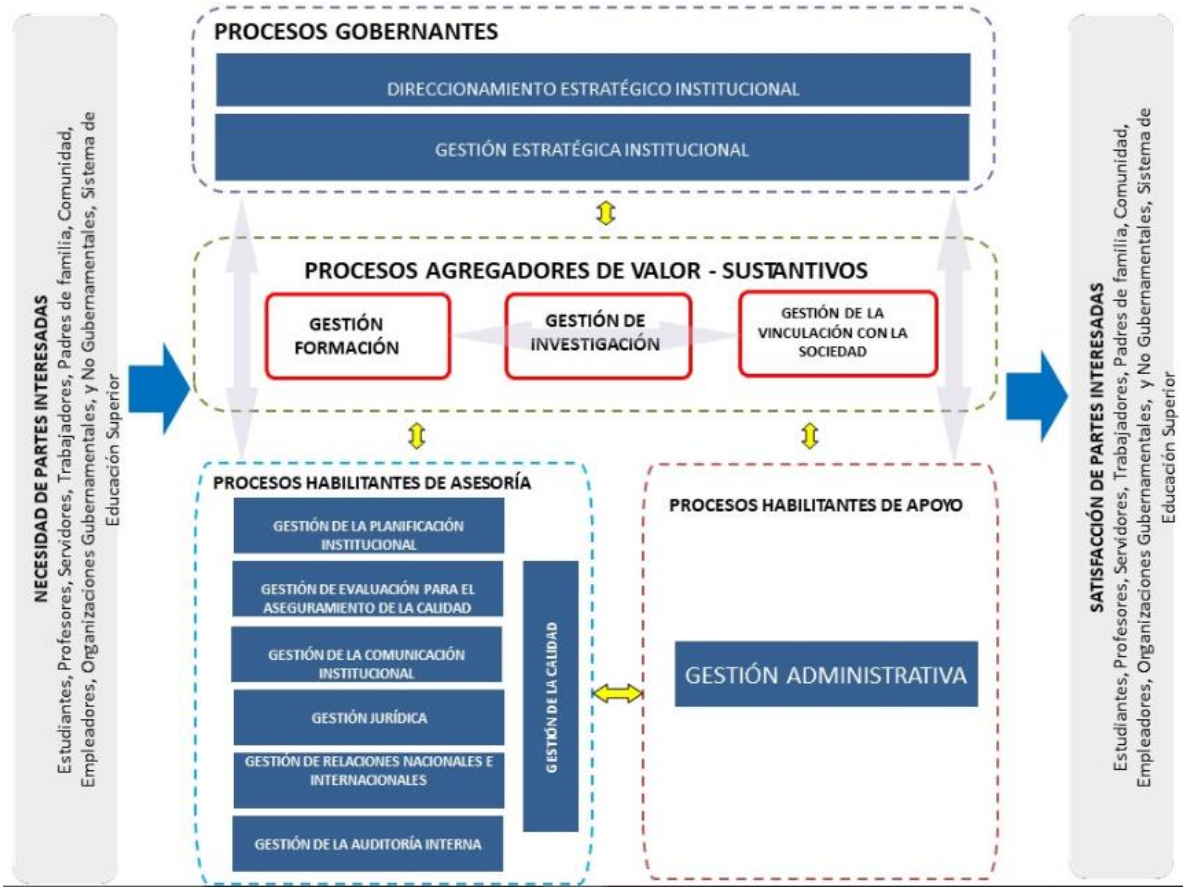



***Ilustración 22.*** *Estructura organizacional de la UNACH* (UNACH, 2019)

## Campos de la UNACH

La UNACH cuenta con tres campos que son esenciales para su desarrollo en el proceso académico de cada uno de ellos, los cuales se detalla a continuación.

### Campus Norte

Ubicado en la Av. Antonio José de Sucre, Km. 1 ½, vía Riobamba – Guano, es el campus más extenso de la Universidad Nacional de Chimborazo, en él funcionan tres de las cuatro facultades de la institución, además de las oficinas administrativas de

rectorado, Vicerrectorado Académico, Vicerrectorado Administrativo, direcciones y departamentos de apoyo a los procesos de gestión.

**Campus La Dolorosa**

Es el campus histórico de nuestra universidad, ubicado en la Av. Eloy Alfaro y 10 de agosto. Antiguamente fue un seminario de formación de religiosos, el cual se recibió en calidad de donación por Mons. Leonidas Proaño Villalba, obispo de Riobamba. Funciona en este campus la Facultad de Ciencias de la Educación, Humanas y Tecnologías, el Vicerrectorado de Posgrado e Investigación y sus direcciones.

**Campus Centro**

Es el campus más nuevo de la institución, ubicado en las calles Duchicela y Procesa Toa. En él funcionan las carreras de Arquitectura y Odontología, así como una oficina de atención de la Asamblea Nacional de Ecuador. Este campus tiene una de las edificaciones históricas más bellas de Riobamba, denominada "Casona Universitaria", un edificio de principios del siglo XX.

**Infraestructura de red**

En el siguiente diagrama se plasma la topología de red con la que conta en el campo principal de la UNACH y como están distribuidos en sus distintas áreas.

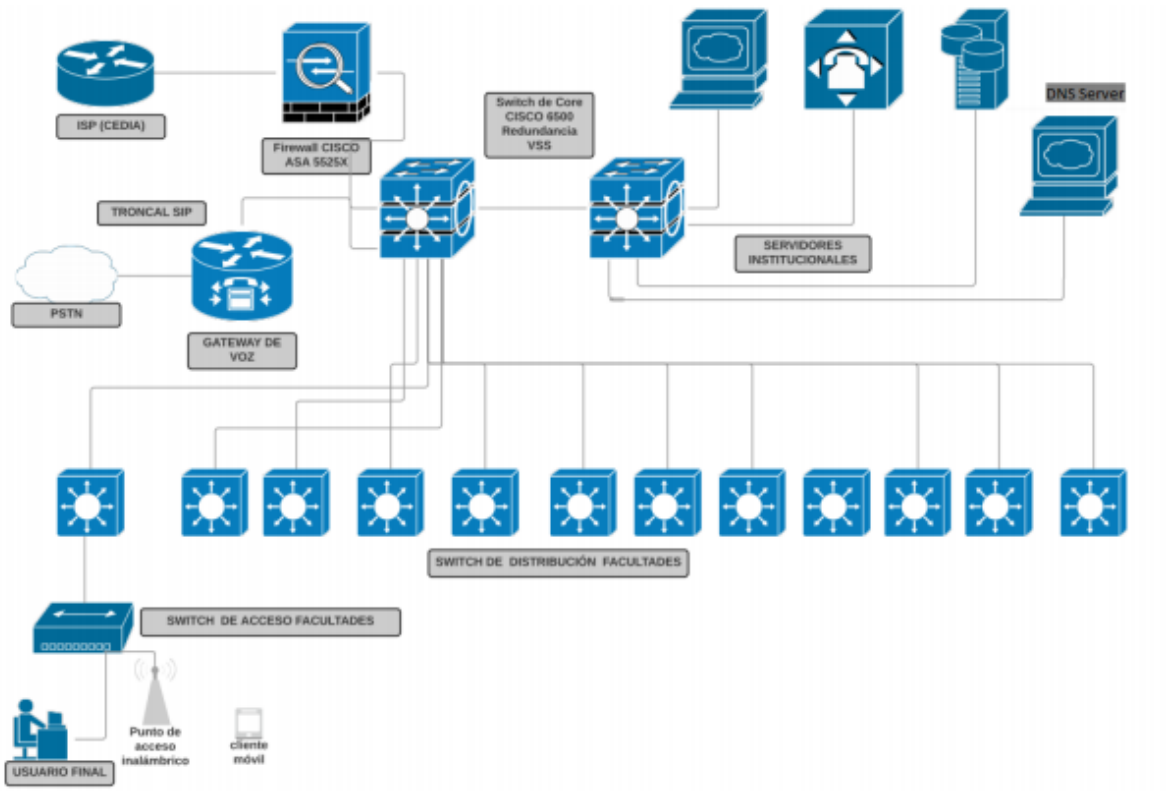



***Ilustración 23.*** *Topología de red de la UNACH (Bonifaz & Miranda , 2018)*

### 1.5. Definición de la entidad patrocinadora

La entidad patrocinadora seria CEDIA debido a que la UNACH pertenece a esta entidad la cual permite tener un beneficio sobre la administración, gestión y capacitación en temas de seguridad informática.

## FASE II: DISEÑO

### 3.1. Introducción

En los últimos años la evolución de la tecnología cada vez va en incremento porque salen al mercado cosas novedosas tanto en servicios y programas, los cuales a veces son utilizados para causar cualquier vulnerabilidad en especial en las organizaciones para robar, modificar la información por ende la UNACH no está exenta de sufrir cualquier ataque, por ello se debe estar a la vanguardia de los servicios digitales, es

decir ahora se cuenta con la información en de forma digital y ya no en documentos físicos. Esto da lugar a que toda la información sea almacenada dentro de repositorios o base de datos que se encuentran en la nube, así también podemos implementar seguridades informáticas las cuales nos permiten que la información no sea alterada o modificada.

Para no tener ningún inconveniente es necesario tener un CSIRT académico en la Universidad Nacional de Chimborazo UNACH, para así crear servicios de monitoreo y mitigación de las vulnerabilidades que puedan ocurrir y que puedan afectar a la información sensible de la organización.

**Análisis ambiental**

- **Fortalezas**
  - ✓ Equipamiento de los laboratorios para brindar servicios tecnológicos relacionados con la seguridad informática
  - ✓ Infraestructura física y lógica adecuados
  - ✓ Docentes y profesionales con conocimientos de seguridad informática
  - ✓ Capacitación del personal en seguridad informática
- **Oportunidades**
  - ✓ Relacionar las investigaciones de ataques informáticos y su mitigación
  - ✓ Relacionar la institución con otras instituciones externas que sepan del tema de seguridad informática
  - ✓ Buscar que la institución tenga convenios con entidades externas
  - ✓ Fomentar la disponibilidad del DTIC en el equipamiento moderno de los laboratorios
  - ✓ Iniciar capacitaciones del personal y miembros del grupo atendido en seguridad informática tanto en instituciones públicas y privadas

- **Debilidades**
    - ✓ No existe la capacitación adecuada en el ámbito de seguridad informática
    - ✓ Debería existir personal adecuado y especializado para encargarse de estas áreas porque deben estar a tiempo completo
    - ✓ Falta de acuerdos y convenios para trabajar conjuntamente entre universidades

**Principios**

- ✓ Todos los miembros de la UNACH deberían trabajar en conjunto
- ✓ La comunidad universitaria debe recibir un servicio de calidad el cual permita tener protegida la información
- ✓ La evolución de los servicios que brinda el CSIRT, está relacionada con su crecimiento y evolución
- ✓ El uso de las herramientas avanzadas va en paralelo con el desarrollo tecnológico de las amenazas, por ende, se debe tener en cuenta que el CSIRT ayuda a las instituciones a mitigar estas vulnerabilidades.
- ✓ Se debe trabajar con instituciones que estén relacionadas con el CSIRT porque puede ayudar con información sobre buenas prácticas para la solución de una vulnerabilidad.

**Valores que debe tener el grupo de clientes atendidos**

- ✓ Honestidad.
- ✓ Tenacidad.
- ✓ Solidaridad.
- ✓ Disciplina
- ✓ Lealtad.

**Misión del CSIRT**

El CSIRT del departamento de Tecnologías de la Información y Comunicación brindara servicios que permitan identificar y mitigar ataques a los sistemas de información, contribuir en la capacitación y formación del personal especializado en respuesta a incidentes de seguridad informática.

**Visión del CSIRT**

Consolidad al CSIRT como líder en equipos de respuesta a incidentes de seguridad informática a nivel académico dentro del país.

**Objetivos estratégicos, Indicadores y Estrategias**

**OE1-** Desarrollar los servicios que brinda el DTIC para responder ante los incidentes informáticos en la universidad

**Estrategias**

- Protegiendo los sistemas de información y optando por los procesos de seguridad
- Investigando sobre nuevos métodos de ataques informáticos y su solución
- Incremento de los servicios del CSIRT

**OE2 –** Brindar servicios para mitigar las vulnerabilidades con métodos, procesos y procedimientos internacionales.

**Estrategias**

- Estableciendo normas y estándares a nivel mundial para responder a los incidentes de seguridad informática
- Fortaleciendo las relaciones con otras instituciones que ya tengan estos proyectos
- Evaluando los procesos de manera eficiente y dar una solución adecuada para su desarrollo.

**OE3 –** Realizar un análisis con el DTIC sobre la situación actual acerca del financiamiento que se va a utilizar en la fase inicial de la creación del CSIRT.

**Estrategias**

- Participar con proyectos de investigación en el ámbito de seguridad informática
- Tratar de que los artículos científicos relacionados sobre los CSIRTs sean auspiciados.
- Gestionar el presupuesto del CSIRT tanto con la institución y las instituciones beneficiarias.

**OE4 –** Para el desarrollo de este proyecto se debe contar con el personal adecuado y capacitado para brindar un servicio de excelencia a la comunidad universitaria.

**Estrategias**

- Disponer del equipamiento tanto en software y hardware especializado.
- Capacitar al personal del CSIRT con otras instituciones relacionadas.
- Disponer de laboratorios para el CSIRT y su correcto funcionamiento.

## 2.1 Plan Operativo Anual (POA)

### Introducción

Dentro del POA consta de las diferentes estrategias y directrices que se debe cumplir a corto plazo para que la institución tenga un proyecto viable, también al momento de la creación del CSIRT se debe tomar en cuenta este punto porque ahí se detalla los diferentes procesos servicios y la organización tanto de la institución como del CSIRT al cual va acoplado esta guía.

**Proyectos en base a los objetivos estratégicos:**

**OE1-** Desarrollar o transformar los servicios que brinda el DTIC para responder ante los incidentes informáticos en la universidad

- Analizar y generar procedimientos adecuados para mitigar los ataques.
- Plataforma de pruebas para contrarrestar la vulnerabilidad.
- El CSIRT debe tener su plan de monitoreo en el cual se debe ver los posibles huecos por donde se pueda crear una vulnerabilidad y contrarrestarla de manera inmediata.

**OE2 –** Brindar servicios para mitigar las vulnerabilidades con métodos, procesos y procedimientos internacionales.

- Implantar los estándares mundialmente para los procesos del CSIRT.
- Realizar charlas para compartir información entre equipos de respuesta.
- Plan de monitoreo constante de los procesos para prevenir y mitigar las vulnerabilidades que puedan ocurrir.

**OE3 –** Realizar un análisis con el DTIC sobre la situación actual acerca del financiamiento que se va a utilizar en la fase inicial de la creación del CSIRT.

- Concursar y participar con proyectos de investigación a nivel mundial.
- Gestionar el auspicio de las publicaciones de artículos científicos relacionados al trabajo de los CSIRT.
- Gestionar el presupuesto del CSIRT con el presupuesto que la institución cuenta.

**OE4 –** Para el desarrollo de este proyecto se debe contar con el personal adecuado y capacitado para brindar un servicio de excelencia a la comunidad universitaria.

- Actualización contante de software y hardware para brindar servicios óptimos.
- Cada trimestre realizar capacitaciones internacionales con respecto al manejo

y administración de procesos de mitigación de ataques.

- Gestionar el espacio físico del CSIRT en el departamento de Tecnologías de la información y comunicación (DTIC) en la UNACH.

**2.2 Analizar y gestionar la demanda de la UNACH**

Con el avance de la tecnología las amenazas cada vez van incrementado por ende existen centro de respuesta a incidentes informáticos los cuales ayudan a prevenir estos ataques, debido a que la institución debe tener siempre disponible toda la información al momento que la comunidad universitaria la necesite, por lo que la UNACH debe contar con este centro y buscar una entidad patrocinadora que ayude en el análisis, diseño, creación, desarrollo, implantación y su posterior evaluación.

Dentro de este centro se va a tener toda la información monitoreada que no sufra ningún daño la cual puede perjudicar irremediablemente a la institución y a todo el personal que trabaja en dicha institución y si sufre alguna vulnerabilidad debe ser analizada, evaluada y solucionada adecuadamente sin que la comunidad universitaria se vea afectad.

Para no sufrir ningún daño el personal también debe esá capacitado para actuar si se produce cualquier inconveniente relacionado con las vulnerabilidades o ataques que puede ocurrir dentro de la institución.

**2.3 Portafolio de servicios que brindará el CSIRT**

La institución debe tener en claro los servicios con los que cuenta y los que se puede implementar trabajando en conjunto con el DTIC de la institución, porque ellos son los encargados de ver si soportara con los equipos que se tiene disponibles o si hará falta comprar unos nuevos o si hace falta más servicios con los cuales de debe configurar de

una manera correcta el CSIRT para que la organización se conforme de una mejor manera y las instituciones relacionadas tampoco se vean afectadas.

Tomando en cuenta los diferentes criterios proporcionados en las normativas y guías prácticas para la creación del CSIRT académico, los mismos que están expuestos en la guía práctica de ENISA (enisa, 2016), a continuación, se detalla los servicios que podría brindar el CSIRT aunque en su mayoría no brinda todos pero los más importantes y los que necesita la institución están listados.

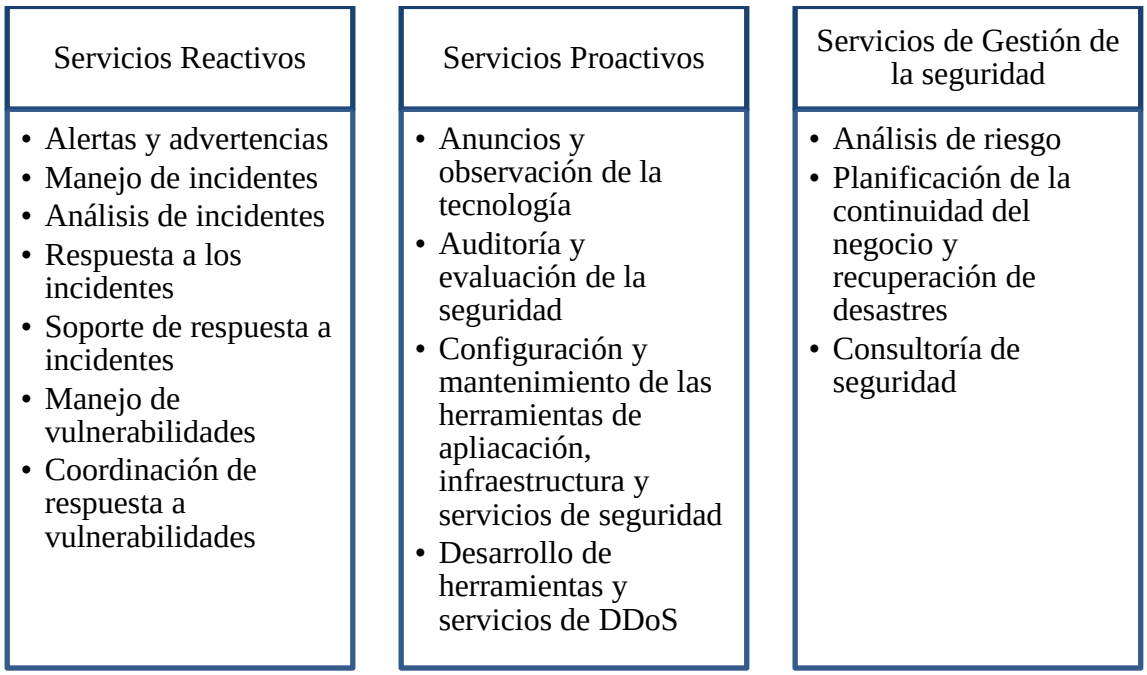



***Ilustración 24.*** *Propuesta Servicios Iniciales del CSIRT*

Estos son los servicios que tiene un CSIRT dentro de la institución al momento en que desee incrementar sus servicios debe estar acorde a la necesidad del DTIC y de la comunidad universitaria.

**2.4 Relación con otros equipos**

La Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA), es una de las instituciones patrocinadoras para la creación de estos centros debido a que ayuda a prevenir y mitigar las vulnerabilidades que puedan existir en una

institución. La UNACH al ser una institución de educación superior y pertenece a CEDIA puede ser beneficiaria de la creación de este centro para mantener la información protegida ante cualquier vulnerabilidad para así poder llegar a per tener al FIRST.

Para tener una mayor acogida al momento de la creación, desarrollo e implementación del CSIRT se debe estar en constante contacto con las otras entidades que están relacionadas compartiendo información adecuada acerca de todos los tipos de incidentes que puedan dañar la institución y así poder estar a la vanguardia y proteger de cualquier ataque.

## 2.5 Políticas y procedimientos del CSIRT

Dentro del DTIC de la UNACH debe existir políticas y procedimientos que se debe seguir cunado existe una vulnerabilidad, lo mismo pasa con el CSIRT por ello, se debe implementar estas políticas que se listan a continuación, pero si la institución ya cuenta debe ser mejorada para que no exista ningún inconveniente.

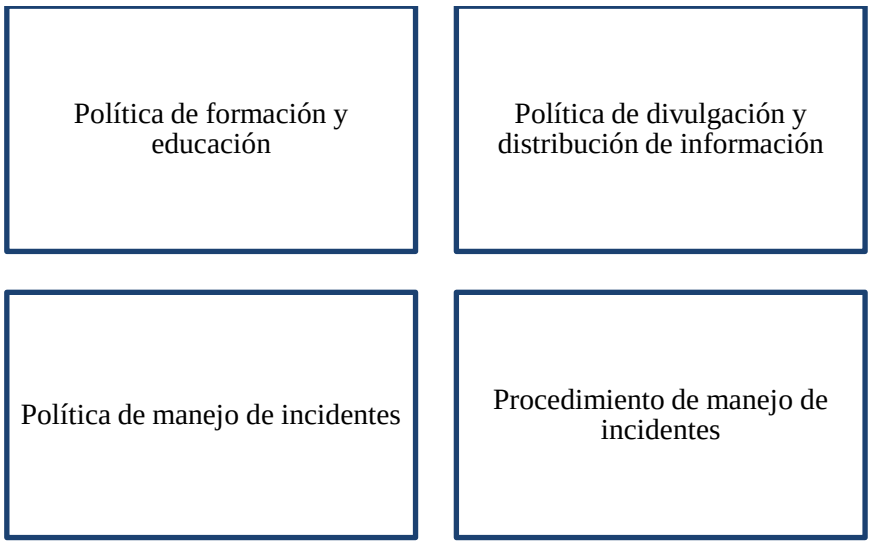



***Ilustración 25.*** *Políticas y procedimientos del CSIRT*

## 2.6 Estructura organizacional del CSIRT

### Descripción del modelo organizacional

Este modelo es solo de la institución debido a los servicios que está ofertando a la comunidad universitaria con la ayuda del Departamento de Tecnologías de la

Información y Comunicación desde su campo principal a sus extensiones. Es decir, el CSIRT y sus recursos se van a ubicar en un área específica del DTIC, el personal que ayuda en este modelo es parte de la institución ellos son encargados de publicar informes de las vulnerabilidades que han ocurrido en la institución, porque ellos son los expertos capacitados que ayudan a las soluciones de estos ataques los cuales pueden perjudicar a la institución y a las instituciones relacionadas.

**Organización de acuerdo con los procesos de la UNACH**

Dentro del organigrama de la UNACH existe procesos los cuales están encargados de ayudar al desarrollo de la institución.

**a) Procesos gobernantes**

**Descripción:** Direccionamiento y gestión estratégica para la creación del CSIRT.

**Responsable:** Miembros del Departamento de Tecnologías de la Información y Comunicación (DTIC) y las autoridades que dirigen la UNACH.

**Descripción:** Determinar el estado físico y lógico del área en el cual se va a implementar este proyecto teniendo en cuenta la calidad de seguridad que brindará el CSIRT a la comunidad universitaria.

**Responsable:** director del Departamento de Tecnologías de la Información y Comunicación (DTIC).

b) **Procesos agregados de valor - sustantivo**

**Descripción:** Análisis del financiamiento necesario para la implementación de este centro en la institución y así tener servicios adecuados para la comunidad universitaria.

**Responsable:** Gestión de evaluación para el aseguramiento de la calidad y el DTIC.

**Descripción:** Analizar, proponer, buscar ayuda de entidades relacionadas con el CSIRT y añadir al presupuesto institucional este valor agregado de financiación.

**Responsable:** Analista de Servicios financieros.

**Descripción:** Indagar, buscar, seleccionar y aplicar la metodología adecuada en la solución de las vulnerabilidades y la solución respectiva.

**Responsable:** El departamento de Tecnologías de la Información y Comunicación.

**Descripción:** Elaboración, realización de reuniones, seminarios, boletines, sitios web u otros servicios que sensibilicen el cumplimiento de buenas prácticas de seguridad.

**Responsable:** Analista de Servicios Especiales.

c) **Procesos habituales de apoyo**

**Descripción:** Planificación, organización y control de los incidentes que se puedan suscitar en la institución y la solución adecuada de la misma.

**Responsable:** Analista de Servicios Especiales.

**Jerarquía de la organización del CSIRT**

Al momento de crear el CSIRT pasaría a ser administrado por el director del departamento de Tecnologías de la Información y Comunicación de la institución debido a que dentro de este departamento se va a crear el área denominada CSIRT que va a estar distribuida y manejada por personal adecuado del CSIRT tanto de la institución como de las instituciones beneficiarias. Se presenta a continuación el área del CSIRT que debe ser implementado en el departamento DTIC.

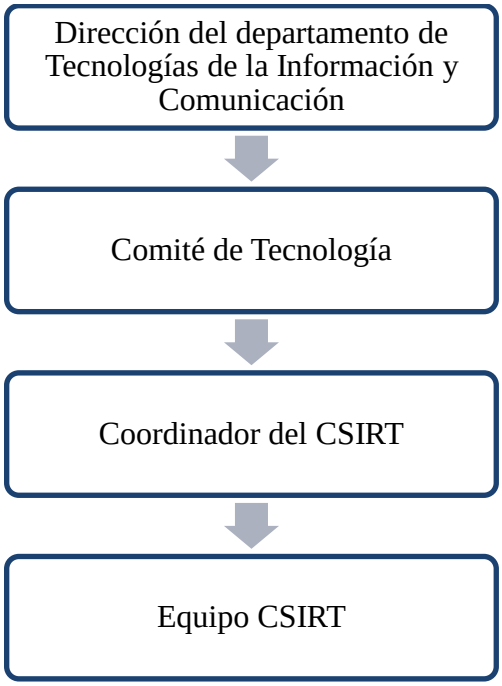



***Ilustración 26.*** *Propuesta Jerárquica Organizacional del CSIRT*

**Responsabilidades que debe tener el área del CSIRT**

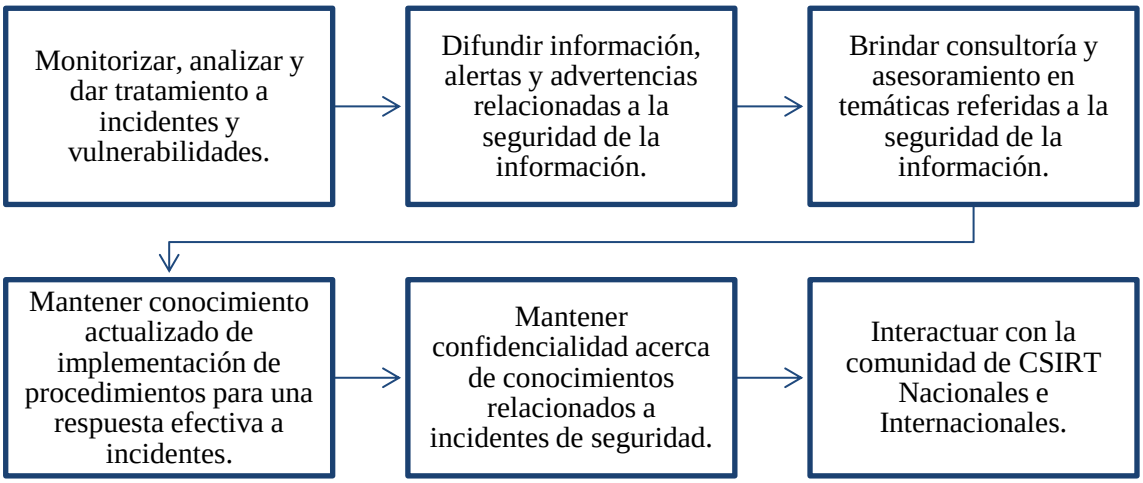



***Ilustración 27.*** *Responsabilidades del CSIRT*

## 2.7 Clasificación de puestos específicos dentro del CSIRT

El CSIRT al pasar a manos del DTIC de la institución debe tener en cuenta los distintos puestos que van a cumplir un papel fundamental en el desarrollo y transcurso de vida del CSIRT, por ello, se pone tentativamente la creación de estos puestos los cuales deberán ser analizados con el DTIC.

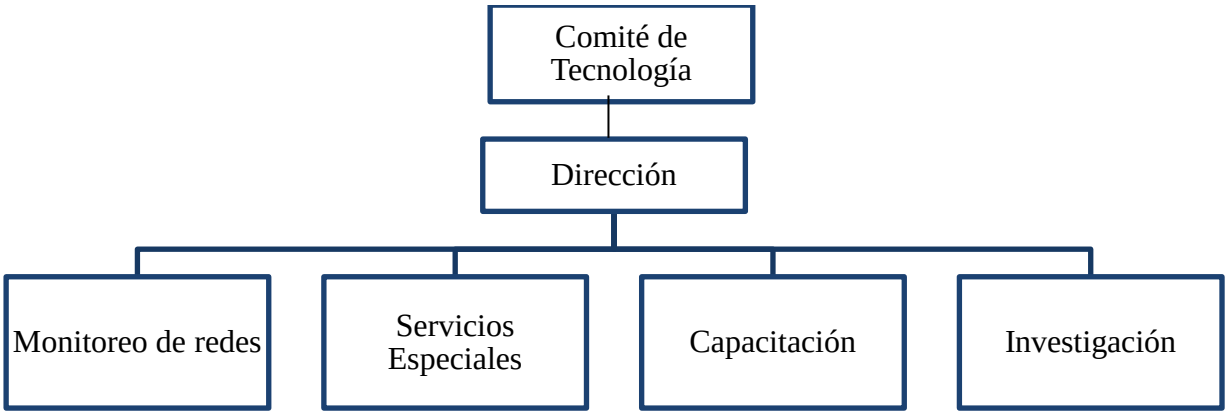



***Ilustración 28.*** *Propuesta de puestos para el CSIRT*

A continuación, se va a describir todos los puestos de trabajo que debe tener el CSIRT y las capacidades especiales que debe tener dicho personal para la resolución de los incidentes que se presenten en la institución y así poder defendernos ante cualquier vulnerabilidad para que la institución no se vea afectada

***Tabla 2.*** *Descripción del personal del comité de TIC*

| ***N.º*** | **1** |
|---|---|
| ***Denominación del Puesto*** | Personal del comité de tecnologías de la información y comunicación |
| ***Objetivo*** | Contribuir a la planificación, asesoramiento y coordinación en las distintas estrategias que debe aplicar el CSIRT en las vulnerabilidades para su solución. |
| ***Responsabilidades*** | - Colaborar al CSRIT en su planificación.<br>- Analizar y recomendar al CSIRT en temas de política y lineamientos de directrices.<br>- Evaluar los reportes de riegos.<br>- Analizar, asesorar y aprobar los planes correctivos y preventivos.<br>- Ayudar a priorizar actividades para el CSIRT en el DTIC de la institución.<br>- Monitoreo constante de la seguridad informática. |
| ***Características del puesto*** | Desarrollar, planificar y solucionar los inconvenientes del CSIRT. |
| ***Competencias técnicas / actitudinales*** | - El personal encargado debe estar disponible a tiempo completo.<br>- Debe ser magister en Informática.<br>- Capacidad de actuar en el momento que lo requieran.<br>- Tener iniciativas de aportar a las soluciones.<br>- Capacidad de relación interpersonal y comunicación efectiva.<br>- Capacidad de razonar y diseñar soluciones de problemas<br>- Tener conocimientos y comprensión del CSIRT. |
| ***Autoridad y acceso*** | Permite ayudar y asesorar al CSIRT. |

***Tabla 3.*** *Descripción del coordinador del CSIRT*

| **N.º** | **2** |
|---|---|
| **Denominación del Puesto** | Coordinador del CSIRT |
| **Objetivo** | Controlar y organizar las actividades en los laboratorios del CSIRT. |
| **Responsabilidades** | - Planifica y organiza al grupo.<br>- Aprueba las diferentes acciones del CSIRT.<br>- Controlar el avance del equipo.<br>- Verifica el cumplimiento de las actividades.<br>- Valora los informes y reportes periódicos.<br>- Aplica estrategias con las autoridades superiores. |
| **Características del puesto** | Es la persona encargada de mantener adecuados los laboratorios del CSIRT. |
| **Competencias técnicas / actitudinales** | - Personal a tiempo completo.<br>- Debe ser magister en Informática.<br>- Capacidad de actuar en el momento que lo requieran.<br>- Tener iniciativas de aportar a las soluciones.<br>- Capacidad de relación interpersonal y comunicación efectiva.<br>- Capacidad de razonar y diseñar soluciones de problemas<br>- Tener conocimientos sobre temas de seguridad informática y CSIRT. |
| **Autoridad y acceso** | Debe tener información limitada. |

***Tabla 4.*** *Personal de redes*

| **N.º** | **3** |
|---|---|
| **Denominación del Puesto** | Personal de la manipulación de redes |
| **Objetivo** | Monitorear la infraestructura de red por medio de sistemas que permitan ayudar a encontrar alguna vulnerabilidad. |
| **Responsabilidades** | - Detección de vulnerabilidades siguiendo distintas tareas.<br>- Garantizar un monitoreo adecuado en la seguridad de la información de la institución.<br>- Seleccionar las mejores herramientas de monitoreo que nos permitirán detectar las vulnerabilidades.<br>- La información debe estar protegida al momento de la monitorización.<br>- Capacitar al personal sobre distintas amenazas que puedan ocurrir.<br>- Reportar y realizar informe de las tareas cumplidas.<br>- Elaborar informes y reportes. |
| **Características del puesto** | El personal es encargado de velar por la infraestructura tanto física como lógica de esta área. |
| **Competencias técnicas / actitudinales** | - Debe ser un profesional acorde al tema.<br>- Debe tener experiencia en seguridad de redes<br>- Tener capacidad de solucionar problemas.<br>- Capacidad de monitorear las redes.<br>- Actuar con ética profesional.<br>- Capacidad de trabajar en grupo.<br>- Poseer actividades de aprendizaje y tener motivación.<br>- Capacidad de analizar, razonar y resolución de problemas. |
| **Autoridad y acceso** | A todas las redes para monitorear. |

***Tabla 5.*** *Descripción del investigador*

| **N.º** | **4** |
|---|---|
| **Denominación del Puesto** | Investigador |
| **Objetivo** | Realiza investigación sobre vulnerabilidades ocasionadas en otras instituciones que pertenecen al CSIRT |
| **Responsabilidades** | - Fortalecer la investigación en temas de seguridad y diseñar proyectos relacionados con el CSIRT.<br>- Publicar los informes de los incidentes de la institución y la solución utilizada.<br>- Informar de las tareas realizadas.<br>- Participar con otras instituciones sobre temas del CSIRT.<br>- Cumplir con todas las actividades que le encomiendan. |
| **Características del puesto** | Es el encargado de investigar y proponer soluciones en seguridad de la información. |
| **Competencias técnicas / actitudinales** | - Personal a fines.<br>- Tener capacidad de solucionar problemas.<br>- Capacidad de investigación.<br>- Actuar con ética profesional.<br>- Capacidad de trabajar en grupo.<br>- Poseer actividades de aprendizaje y tener motivación.<br>- Capacidad de analizar, razonar y resolución de problemas. |
| **Autoridad y acceso** | A la información para la mejora de la seguridad informática. |

***Tabla 6.*** *Descripción del analista de servicios del CSIRT*

| **N.º** | **5** |
|---|---|
| **Denominación del Puesto** | Analista de servicios del CSIRT |
| **Objetivo** | Analiza las distintas formas que utilizan los atacantes para crear una vulnerabilidad en la institución |
| **Responsabilidades** | - Detectar las vulnerabilidades y solucionar.<br>- Tener adecuadamente tanto el hardware y software del área, dando un mantenimiento adecuado.<br>- Al momento de investigar también se realizan pruebas para tener una idea de la vulnerabilidad.<br>- Establecer prioridades al momento de que se presente una vulnerabilidad.<br>- Elabora informes de las actividades realizadas y los logros alcanzados. |
| **Características del puesto** | El personal está capacitado para brindar información sobre las distintas vulnerabilidades suscitadas en la institución. |
| **Competencias técnicas / actitudinales** | - Personal a fines.<br>- Tener capacidad de solucionar problemas.<br>- Capacidad de investigación.<br>- Actuar con ética profesional.<br>- Capacidad de trabajar en grupo. |
| **Autoridad y acceso** | A todos los incidentes u eventos que existan en la Universidad.<br>Al hardware y software para análisis técnico.<br>Ambientes de simulaciones y pruebas. |

***Tabla 7.*** *Descripción del capacitador*

| **N.º** | **6** |
|---|---|
| **Denominación del Puesto** | Capacitador |
| **Objetivo** | Suministra información de las actividades principales de la seguridad de la información. |
| **Responsabilidades** | - Brinda capacitación en seguridad informática.<br>- Ejecuta talleres, cursos y tutorías.<br>- Ejecuta pasos para contrarrestar vulnerabilidades.<br>- Los procesos de capacitación se deben ejecutar de una manera adecuada.<br>- Recopila información para prevenir amenazas que puedan ocasionar daños en la institución.<br>- Contener una bitácora de las capacitaciones.<br>- Elabora informes sobre las tareas realizadas. |
| **Características del puesto** | Es la persona encargada de brindar capacitaciones sobre la seguridad de la información con respecto a los CSIRT. |
| **Competencias técnicas / actitudinales** | - Personal a fines y con experiencia.<br>- Tener capacidad de solucionar problemas.<br>- Capacidad para brindar una capacitación adecuada.<br>- Actuar de acuerdo con sus valores.<br>- Capacidad de trabajar en grupo y poseer motivación al momento de la capacitación. |
| **Autoridad y acceso** | A toda la información sobre seguridad de la información y como brindar las capacitaciones adecuadas para poder contrarrestar estos incidentes. |

## 2.8 Infraestructura y equipamiento de la UNACH

### a) Infraestructura del departamento de Tecnologías de la Información y comunicación

La infraestructura de red que posee la UNACH tanto en almacenamiento y la distribución que tiene con el DTIC, se encuentra disponible para la implementación de este proyecto debido a que la infraestructura de red, virtualización de servidores, para procesamiento y almacenamiento de datos y el posterior respaldo de los datos están en excelentes condiciones y capacidades para el proyecto en mención.

**Componentes**

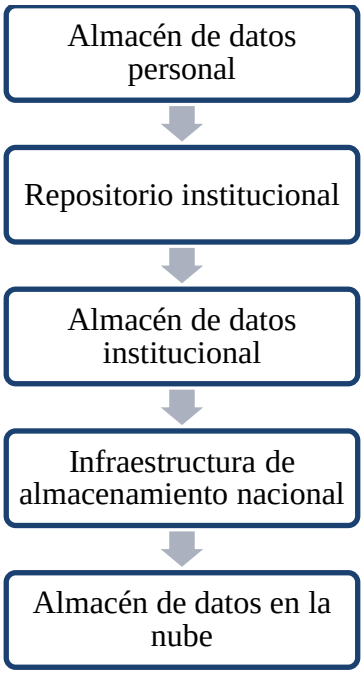



***Ilustración 29.*** *Componentes de la infraestructura de red*

### b) Infraestructura del laboratorio CSIRT

**Infraestructura inicial**

Para la infraestructura inicial del CSIRT y para el suministro de los servicios básicos es necesitaría la siguiente infraestructura de red la cual debe ser adecuada por el

departamento de Tecnologías de la Información y Comunicación de la UNACH que se muestra a continuación.

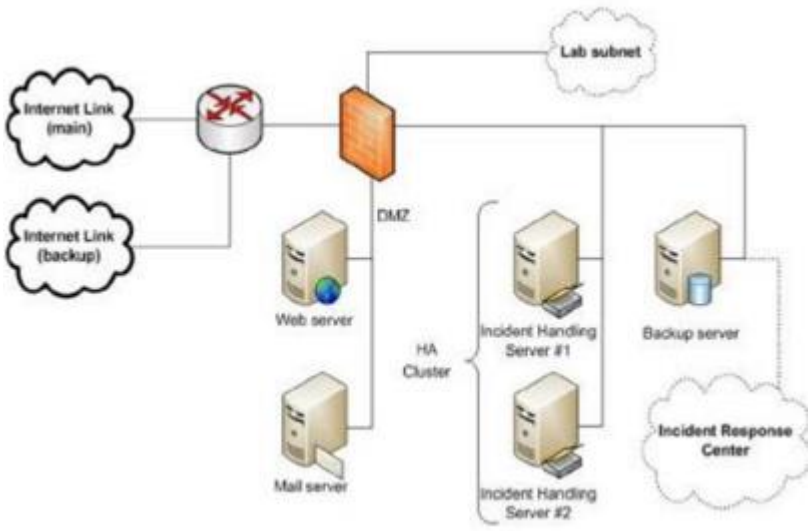



***Ilustración 30.*** *Infraestructura inicial* (ENISA, 2016)

**Etapa de creciente y desarrollo en la infraestructura del CSIRT**

Al momento en que se desea ampliar los servicios del CSIRT se debe tener en consideración también la infraestructura de red, es decir debe incrementar sus recursos, servicios y personal. Debido a este crecimiento se debe implementar virtualización de tecnología como se muestra a continuación.

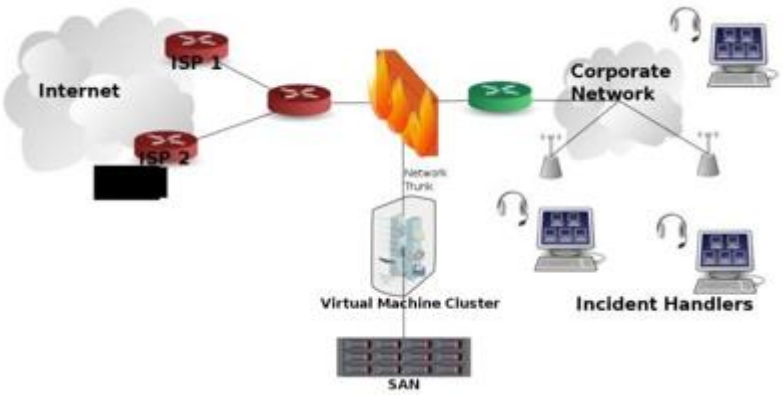



***Ilustración 31.*** *Infraestructura futura* (ENISA, 2016)

**Hardware**

Dentro de los servicios de hardware se debe tener todos los sistemas, servicios y tecnología que a continuación se lista:

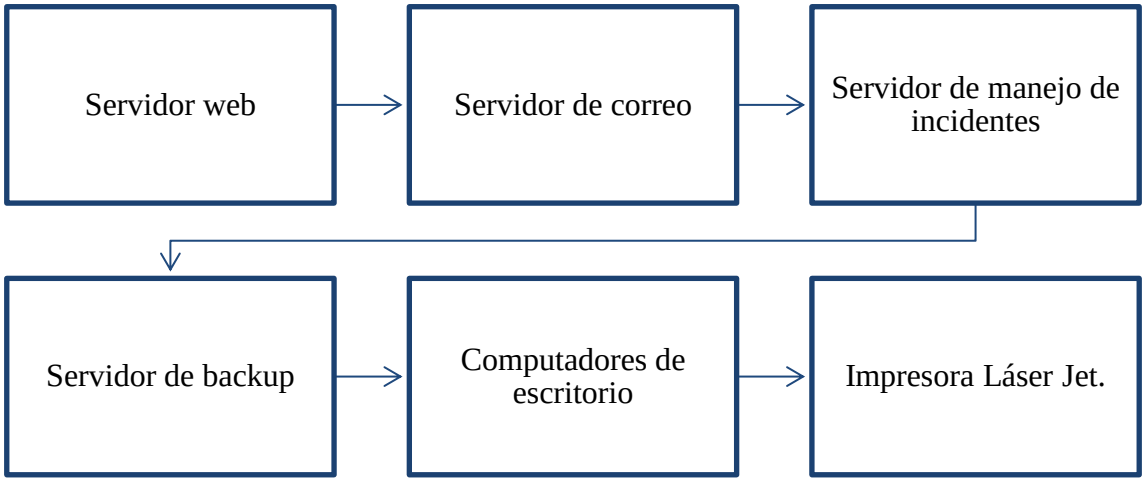



***Ilustración 32.*** *Hardware en su etapa futura*

**Software**

Las herramientas seleccionadas para la propuesta del CSIRT en su etapa de crecimiento deben ser de software de código abierto para evitar costos de adquisición y tratar mejor las vulnerabilidades que puedan existir en un futuro dentro de la institución, por ende, a continuación, se muestra el software que deben adquirir.

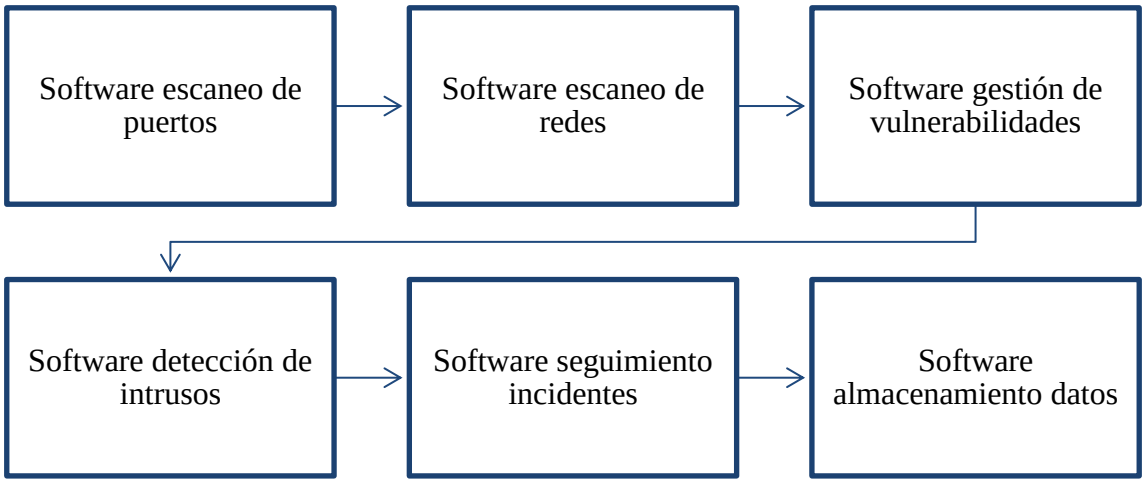



***Ilustración 33.*** *Software en su etapa futura*

**Propuesta para la adecuación física del CSIRT**

El área en el que se alojará el CSIRT en su etapa de inicio estará ubicado en el DTIC debido a que ahí cuenta con un espacio seguro y protegido ante desastres naturales, este lugar también cuenta con cámaras de seguridad, acceso a las redes telefónicas y datos y lo más importante es que cuenta con un espacio para el personal y equipos del CSIRT.

## 2.9 Procedimientos que se debe ejecutar en la seguridad, recuperación de desastres y la continuidad de los servicios del CSIRT

### 2.9.1 Plan de seguridad

Hoy en día los riesgos se presentan en todo lo que está relacionado con los sistemas y la red informática que tiene la institución la cual esta vulnerable al momento de recibir cualquier notificación de extraños, debido a que la información que contiene es de suma importancia, la cual no debería sufrir ninguna alteración, perdida o uso inadecuado de sus datos por lo que esto pondría en vulnerabilidad a la institución.

Este plan de seguridad es aplicable a la organización debido a que las áreas que protege la organización están expuestas a sufrir cualquier tipo de vulnerabilidades, en lo que se refiere al manejo de la información, por lo que debe cumplir con todas las normas de seguridad y políticas que rigen dentro de la institución.

### 2.9.2 Plan de recuperación de desastres

Los sistemas de información no están exentos de sufrir cualquier tipo de daño causado por los desastres naturales, o cualquier tipo de desastre ocasionado por personal dentro o fuera de la institución, el cual llega a tener muchas consecuencias entre ellas está la perdida de datos, fallo en los sistemas de información y hasta la perdida de la infraestructura tanto física y lógica.

El plan de recuperación de desastres se centra en los procesos que debe cumplir la organización hasta que se recupere del desastre, al momento que pone en marcha el plan de continuidad que debe tener el DTIC y así lograr obtener la recuperación de procesos sin que la organización vea afectada su información, sistemas e infraestructura. Se debe tomar en cuenta que la institución que está afectada contiene datos importantes, para ello se debe aplicar una correcta planificación para recuperarse del desastre porque si no se sigue los pasos adecuados no se podrá recuperar de dicho desastre, ni tampoco se recuperará el manejo de los sistemas.

### 2.9.3 Plan de continuidad de servicios

Muchas de las organizaciones no tienen los recursos e infraestructura para implementar un proceso de seguridad adecuada a la información, la cual debe estar respaldad, cuidada y no va a ser usada de una manera que afecte en el funcionamiento de la organización.

El CSIRT al brindar los servicios de protección, mitigación ante ataques informáticos está comprometido con la sociedad para mantener activos sus servicios sin que se vean afectados sus activos dando así una alta disponibilidad, eficiencia y eficacia de los mismo. Dando así la tranquilidad a las organizaciones que dependen de estos servicios permitiendo que ellos confíen que la información porque está protegida y segura al momento en que lo necesiten.

Por tal motivo el plan de continuidad de servicios expone diferentes estrategias para usar y solventar alguna caída del servicio, la cual debe recuperase en una cantidad de tiempo mínima, para que los usuarios no se den cuenta que no tienen servicios, es decir, deben tener un servicio de backup para que se ejecute de forma paralela y así no pierda el acceso a este servicio y no haya molestias en los usuarios.

### 2.9.4 Presupuesto del CSIRT en coordinación con El DTIC

El DTIC debe tener en cuenta que se va a iniciar con este proyecto en su etapa temprana en la cual se va a realizar la adecuación delos laboratorios de dicha área, con el hardware, software que se cuenta al momento en la institución con la infraestructura de red de la organización y almacenamiento de alto rendimiento del mismo departamento, con el uso de herramientas de código abierto el mismo que no tiene ningún costo, a partir de esto se tomó en cuenta un presupuesto referencial para la implementación del CSIRT en su etapa inicial los cuales se presentan en las siguientes tablas.

***Ilustración 34.*** *Presupuesto equipos de oficina*

| Equipos de oficina | Cantidad | Precio unitario | Sub total |
|---|---|---|---|
| Computadoras de escritorio | 10 | 298 | 2980 |
| Impresora multifuncional | 2 | 540 | 1080 |
| Sillas | 10 | 35 | 350 |
| Escritorio de trabajo | 10 | 120 | 1200 |
| Archivadores de pared | 5 | 70 | 350 |
| Armario | 4 | 250 | 1000 |
| Suministro de oficina | | | 1500 |
| **Total** | | | **8460** |

***Ilustración 35.*** *Presupuesto hardware*

| Hardware | Cantidad | Sub total |
|---|---|---|
| Servidores físicos para el data center | | 25000 |
| Sistemas de almacenamiento unifica | 1 | 10000 |
| Sistemas de respaldo | 1 | 9000 |
| **Total** | | **44000** |

***Ilustración 36.*** *Presupuesto servicios básicos*

| Servicios básicos | Meses | Precio mensual | Sub total |
|---|---|---|---|
| Luz | 12 | 150 | 1800 |
| Internet | 12 | 150 | 1800 |
| Agua | 12 | 150 | 1800 |
| **Total** | | | **5400** |

## 2.10 Bitácora de pasos para poner en marcha el CSIRT

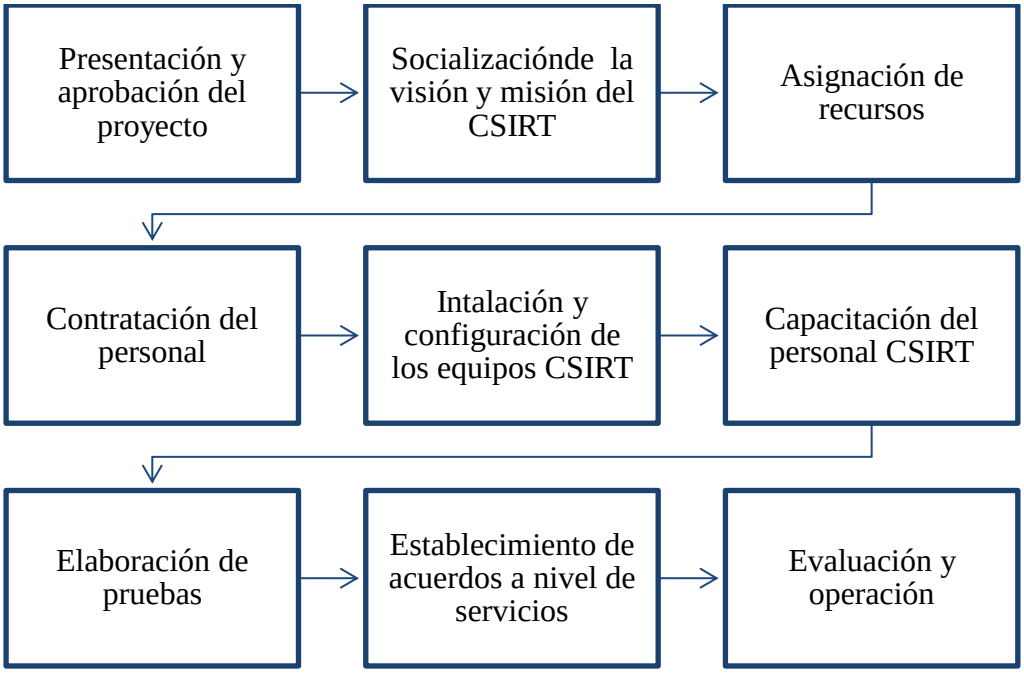



***Ilustración 37.*** *Cronograma de implantación del proyecto CSIRT*

## 2.11 Definición de indicadores de evaluación de la implantación del proyecto

Dentro del CSIRT se cuenta con indicadores de evaluación al momento en que se crea el CSIRT en la institución los cuales se debe seguir de una manera coordinada para su buen uso y funcionamiento.

**Metas**

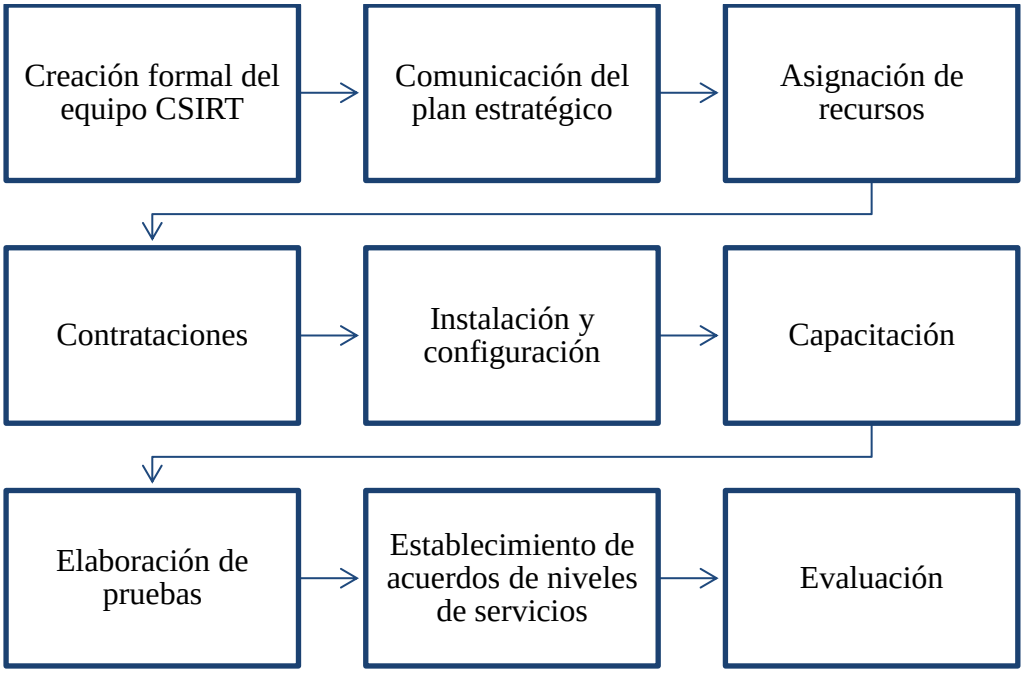



***Ilustración 38.*** *Indicador de evaluación para metas*

**Resultados**

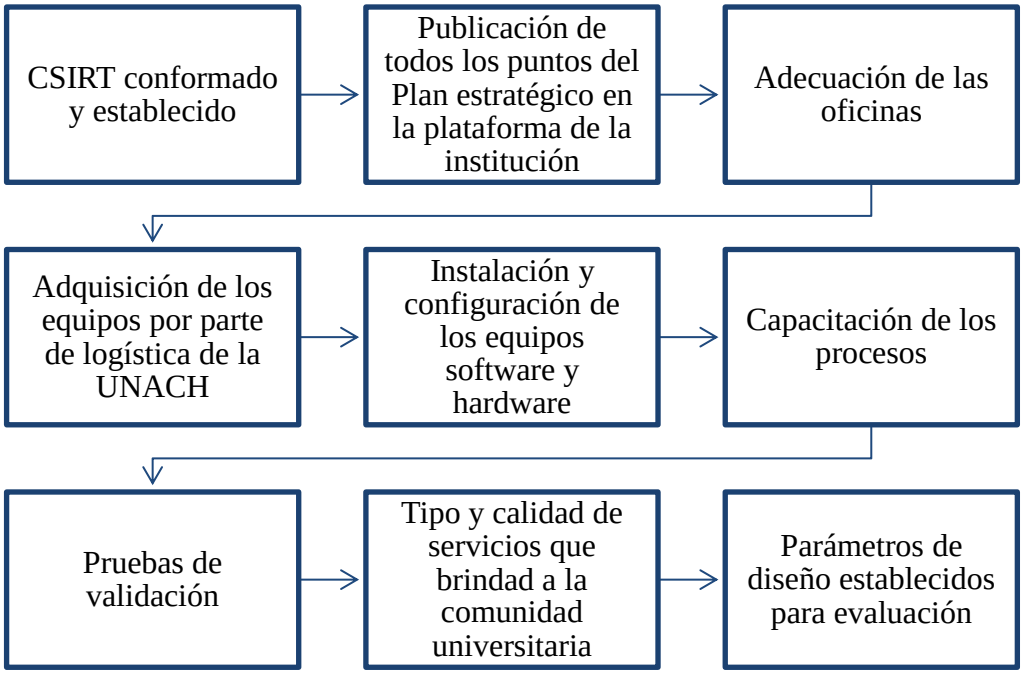



***Ilustración 39.*** *Indicador de evaluación resultados*

**Índice de medición**

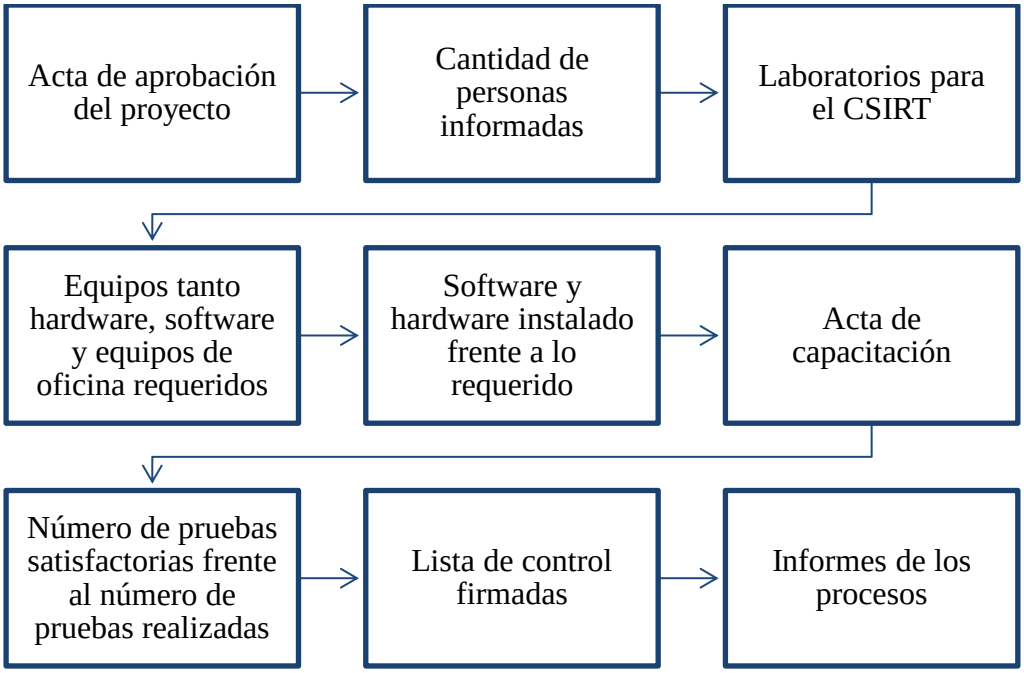



***Ilustración 40.*** *Indicador índice de medición*

## FASE III: TRANSICIÓN

### Gestión de alertas e incidentes

**4.1. Clasificación y priorización de incidentes.** La clasificación y priorización de los incidentes permite que la organización ponga en marcha un plan de respuesta apropiado para que el impacto no sea masivo y se pueda dar solución apropiada a la misma. La clasificación de los incidentes de seguridad se les clasifica dependiendo de la categoría y severidad de los incidentes de seguridad para que no puedan afectar a la institución.

Dentro de las categorías de incidentes informáticos tenemos los siguientes.

- Exponer los datos e información personal, es decir confidencial dentro de la institución
- Denegación de servicios
- Violación de derechos de propiedad intelectual

- Violación de las políticas
- Escaneo de puertos y vulnerabilidades
- Actividades de phishing
- Spam
- Acceso no autorizado
- Vulnerabilidad en sistemas, aplicaciones y servicios

Existen diferentes factores que se tienen en cuenta para determinar la severidad de un incidente, dentro de los principales se tiene:

- Alcance del impacto
- Situación actual del sistema o servicio
- Sensibilidad de la información
- Probabilidad de propagación

## FASE IV: OPERACIÓN

### Respuesta a incidentes y apoyo a la comunidad

**5.1. Manejo de incidentes.** Dentro del CSIRT se brinda el servicio de manejo a incidentes debido a que es uno de los más importantes porque se puede prevenir cualquier tipo de ataque o vulnerabilidad. El manejo de estos incidentes debe ser tratado por un especialista relacionado del tema, el principal objetivo es tener una metodología basada en la aplicación del mejor criterio para la resolución de este. Las organizaciones generalmente tienen criterios no adecuados los cuales les generan las siguientes consecuencias.

- Tiempo excesivo en la resolución del incidente
- Solución del problema temporalmente por medio de parches
- No tienen una bitácora de errores en caso de que se suscite de nuevo el

incidente

El manejo de incidentes generalmente contiene las siguientes etapas:

- Detección y análisis
- Manejo de incidentes (contención, erradicación y recuperación)
- Cierre del incidente (documentación, notificación y registro)

En la etapa de detección y análisis se recepta la información del incidente vía email, es decir requerimiento al help desk o logs de los recursos tecnológicos de la organización la cual está siendo atacada, esta información debe registrarse en un formulario. Esta información es recopilada y analizada en un proceso llamado triage, en el cual se clasifica el incidente y se priorizan los recursos tanto humanos y tecnológicos de acuerdo con el nivel de impacto, y finalmente se procede a la resolución y documentación del incidente.

También se muestra un modelo de formulario con el que se puede notificar el incidente dentro de la organización se lo puede hacer por medio de correo electrónico, fax o distintos medios de comunicación siempre y cuando tenga un número de incidente para luego poder documentar y archivar el incidente.

| | FORMULARIO DE COMUNICACIÓN DE UN INCIDENTE | | | | |
|---|---|---|---|---|---|
| | **Instrucciones:** | | | | |
| | Llenar este formulario y enviarlo por correo electrónico o por fax a: | | | | |
| | Las líneas con un (*) son obligatorias. | | | | |
| | | | | | |
| | **Nombre y organización** | | | | |
| **1** | **Nombre (*):** | | | | |
| **2** | **Nombre de la organización (*):** | | | | |
| **3** | **sector:** | | | | |
| **4** | **País (*):** | | | | |
| **5** | **Ciudad:** | | | | |
| **6** | **Dirección de correo electrónico (*):** | | | | |
| **7** | **Número de teléfono (*):** | | | | |
| **8** | **otros:** | | | | |
| | | | | | |
| | **Ordenador(es) afectado(s)** | | | | |
| **9** | **Número de ordenadores:** | | | | |
| **10** | **Nombre del ordenador e IP (*):** | | | | |
| **11** | **Función del ordenador (*):** | | | | |
| **12** | **Hardware:** | | | | |
| **13** | **Sistema operativo:** | | | | |
| **14** | **Software afectado:** | | | | |
| **15** | **Ficheros afectados:** | | | | |
| **16** | **Seguridad:** | | | | |
| **17** | **Protocolo/puerto:** | | | | |
| | | | | | |
| | **Incidente** | | | | |
| **18** | **Número de referencia:** | | | | |
| **19** | **Tipo de incidente:** | | | | |
| **20** | **Inicio del incidente:** | | | | |
| **21** | **El incidente aún no se a resuelto:** | **Si** | | No | |
| **22** | **Hora y método de descubrimiento:** | | | | |
| **23** | **Vulnerabilidades conocidas:** | | | | |
| **24** | **Ficheros sospechosos:** | | | | |
| **25** | **Medidas preventivas:** | | | | |
| **26** | **Descripción detallada (*):** | | | | |
| | | | | | |

***Ilustración 41.*** *Formulario de Comunicación de un incidente*

En la siguiente imagen se detalla las diferentes etapas, actividades y procesos que debe cumplir al momento de que se detecta alguna vulnerabilidad (Andrade , 2013).

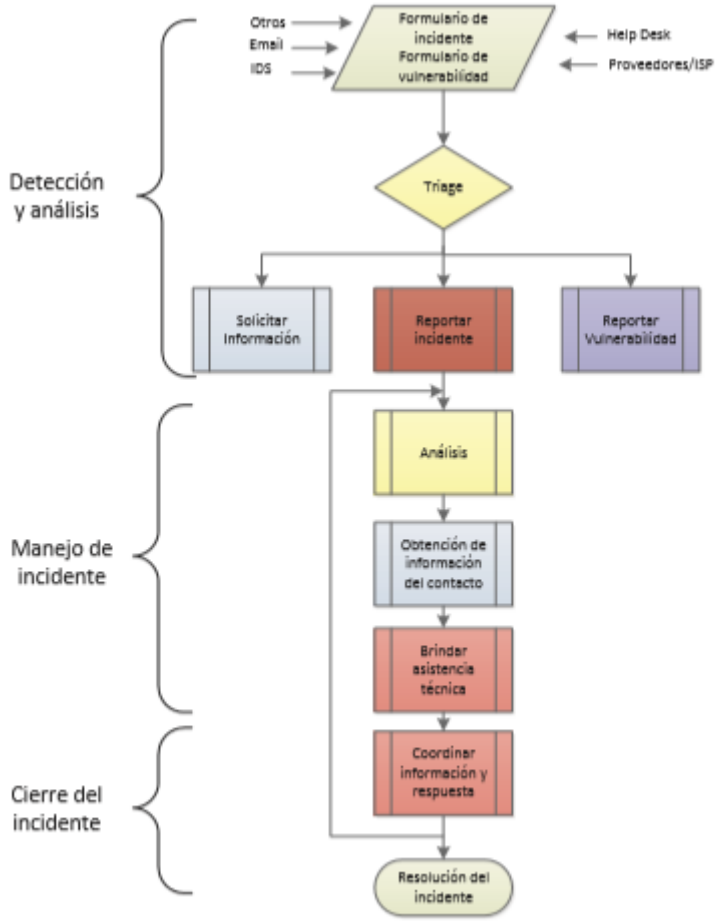



***Ilustración 42.*** *Proceso de manejo de incidentes de seguridad informática* (ENISA, 2016)

Dentro de las tres etapas en el manejo de incidentes se detallan características importantes a continuación.

***Ilustración 43.*** *Características importantes*

| | |
|---|---|
| Detección y análisis | - Priorización del manejo de incidentes basado en el impacto del negocio<br>- Identificar los servicios afectados<br>- Estimación actual del incidente<br>- Reporte del incidente al personal y organizaciones externas afectadas |
| Manejo de incidentes (contención, erradicación y recuperación) | - Adquirir, almacenar y documentar la evidencia<br>- Contención del incidente<br>- Identificar y mitigar la vulnerabilidad<br>- Implementar filtros si no ha sido contenido el ataque<br>- Redirigir el objetivo<br>- Erradicar el incidente y eliminar las vulnerabilidades |
| Cierre del incidente (documentación, notificación y registro) | - Restaurar los servicios afectados<br>- Implementar monitoreo<br>- Realizar actividades post incidentes<br>- Creación de reporte de seguimiento de incidente<br>- Documentar y almacenar los procesos utilizados |

## FASE V: MEJORA

### Operación, revisión y mejoramiento continuo

Durante el proceso de manejo de incidentes de seguridad informática está definido dentro de diferentes modelos de gestión de tecnología, el establecer un modelo de gestión de TI, permite establecer los procesos de gestión de incidentes.

Dentro de la gestión de tecnologías de la información se tiene distintos modelos que son: El modelo de medición, los criterios de certificación externos y los conceptos y prácticas. Dentro del grado de especificación existe la mejora, planeación, operación y la implementación se debe seguir adecuadamente dentro de la institución para su mejora continua.

Es importante establecer métricas que permita evaluar la eficiencia del CSIRT dentro de lo cual tenemos las siguientes métricas.

- Mantenimiento de la calidad del servicio
- Mantenimiento de la satisfacción de los miembros de la comunidad
- Resolución de incidentes de seguridad informática en un tiempo establecido

**Anexo N.° 5**

**Acta entrega recepción al Departamento de Tecnologías de la Información y Comunicación (DTIC) de la UNACH**

ACTA ENTREGA RECEPCIÓN DE UNA GUÍA DEL PROTOTIPO CSIRT PARA LA UNACH

En la ciudad de Riobamba a los 04 días del mes de diciembre de 2019, por un lado la Srta.: Mónica Chacha, en calidad de estudiante de la carrera de Ingeniería en Sistemas y Computación; y, por otro la Ing. Lorena Molina, en calidad de Tutora del Proyecto de Investigación titulado **"ANÁLISIS DE LAS METODOLOGÍAS ENISA Y APCERT PARA LA CREACIÓN DEL CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS (CSIRT). CASO PRÁCTICO: PROTOTIPO DE UN CSIRT EN LA UNIVERSIDAD NACIONAL DE CHIMBORAZO"**, con el fin de realizar la entrega – recepción de una guía del prototipo CSIRT para la UNACH al Director del Departamento de Tecnologías de la Información y Comunicación.

Para constancia de lo actuado, firman la presente acta:

Mónica Chacha
Estudiante

Ing. Lorena Molina
Tutora de Tesis

Ing. Javier Haro
Director del DTIC