OFICINA DE POSGRADOS

Tema:

GUÍA PARA IMPLEMENTAR UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL

Proyecto de investigación previo a la obtención del título de Magíster en Ciberseguridad

Línea de Investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Luis Fernando Arias Batallas

Director:

Mg. Paúl Fernando Bernal Barzallo

Ambato – Ecuador

Octubre 2023

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

GUÍA PARA IMPLEMENTAR UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Luis Fernando Arias Batallas

Paul Fernando Bernal Barzallo, Mg. f. _____

CALIFICADOR

Verónica Maribel Pailiacho Mena, Mg. f. _____

CALIFICADOR

Jose Marcelo Balseca Manzano, Mg. f. _____

CALIFICADOR

Juan Carlos Acosta Teneda, PhD. f. _____

COORDINADOR DE LA OFICINA DE POSGRADOS

Hugo Rogelio Altamirano Villaroel, Dr f. _____

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Octubre – 2023

DECLARACIÓN DE AUTENTICAD Y RESPONSABILIDAD

Yo: **LUIS FERNANDO ARIAS BATALLAS**, con cédula de ciudadanía **0705466225,** autor del trabajo de graduación titulado: “GUÍA PARA IMPLEMENTAR UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL”, previo a la obtención del título profesional de **MAGÍSTER EN CIBERSEGURIDAD**, en la Oficina de **POSGRADOS.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.
2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de Universidad.

Ambato, octubre 2023

Luis Fernando Arias Batallas

CC. 0705466225

DEDICATORIA

A mi querida hija Valentina y mi amada esposa Charito, este logro no sería posible sin su amor incondicional y sacrificio. Han sido mi fuente de inspiración y motivación diaria en este largo camino de investigación y aprendizaje.

A ti, mi dulce Valentina, siempre has sido mi razón para superar cualquier obstáculo. Tus sonrisas radiantes y tu espíritu curioso me han recordado la importancia de perseguir mis sueños y nunca rendirme.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por permitirme continuar superándome académicamente.

Un agradecimiento especial a todas las personas que participaron de este proceso de investigación, aprendí de cada uno de Ustedes y espero que la información generada sirva de mucho para otras personas.

RESUMEN

Este estudio presenta una guía para la implementación de un centro de respuesta a incidentes informáticos (CSIRT por sus siglas en inglés) dirigidos a la sociedad civil. Se realizó una revisión exhaustiva de documentación existente sobre la creación de CSIRTs convencionales, analizando su contenido y recopilando información relevante. Además, se llevaron a cabo entrevistas con varias organizaciones latinoamericanas que brindan apoyo en seguridad digital a organizaciones de la sociedad civil. A partir de estas entrevistas, se documentaron las mejores prácticas de estas organizaciones, que cuentan con experiencia en el acompañamiento en seguridad digital durante varios años. La guía se desarrolló en colaboración con una organización de la sociedad civil que cuenta con una línea de ayuda, utilizando la metodología de investigación-acción participativa. Posteriormente, la guía fue evaluada por dos expertos en el tema. En definitiva, esta guía constituye un recurso valioso para las organizaciones de la sociedad civil que buscan establecer sus propios CSIRTs y mejorar sus capacidades de seguridad digital.

Palabras clave: incidentes informáticos, sociedad civil, ciberseguridad, informática.

ABSTRACT

This study presents a comprehensive guide for implementing Computer Security Incident Response Teams (CSIRTs) targeting civil society. A meticulous review of existing literature on conventional CSIRT establishment was conducted, entailing content analysis and compilation of pertinent information. Additionally, interviews were conducted with several Latin American organizations providing digital security support to civil society entities. These interviews facilitated the documentation of best practices from experienced organizations with a proven track record in digital security assistance. The guide was collaboratively developed in partnership with a civil society organization operating a helpline, utilizing a participatory action research methodology. Subsequently, the guide underwent evaluation by two subject matter experts. In conclusion, this guide serves as an invaluable resource for civil society organizations aiming to establish their own CSIRTs and enhance their digital security capabilities.

Keywords: computer incidents, civil society, cybersecurity, computing.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

ÍNDICE DE ANEXOS

INTRODUCCIÓN

Con la evolución tecnológica y la expansión del uso de servicios digitales, cada día se incrementan los usuarios en las diferentes plataformas de internet, si bien esto contribuye a realizar actividades cotidianas de forma más eficiente, también se incrementan los riesgos digitales para los usuarios (Fojón y Sanz, 2010).

Por lo tanto, se debe tener precaución en las comunicaciones y los datos personales para evitar incidentes que puedan comprometer la seguridad de las personas, es aquí donde nace el concepto de ciberseguridad, mismo que consiste en la aplicación de un proceso de análisis y gestión de los riesgos relacionados con el uso, procesamiento, almacenamiento y transmisión de información o datos y los sistemas y procesos usados basado en los estándares internacionalmente aceptados (Fojón y Sanz, 2010). La ciberseguridad se basa en tres pilares: la confidencialidad, la integridad y la disponibilidad (Unión Internacional de Telecomunicaciones, 2019):

- Asegurando la confidencialidad, mantiene la privacidad y protege la información contra el acceso no autorizado, por ejemplo, la divulgación de la información.
- Asegurando la integridad, protege la información contra modificaciones no autorizadas.
- Asegurando la disponibilidad, puesto que protege la información para que siempre permanezca accesible y sin interrupciones (p.89).

En los últimos meses, se ha observado que los ataques informáticos se han vuelto más comunes que antes, ahora cualquier persona puede ser víctima de uno de estos incidentes y las personas que no tienen una formación técnica, muy difícilmente conocen las formas de protegerse o mitigar un ataque de este tipo (Apolinario, 2022).

Fojón y Sanz (2010) en su estudio Ciberseguridad en España, una propuesta para su gestión afirma que para combatir las amenazas, los responsables de la

ciberseguridad deben disponer de recursos técnicos y humanos de última generación, fruto de la continua y acelerada evolución de las TIC, que ha derivado en ciberataques cada vez más sofisticados. amenazas y efectos potenciales.

Durante la emergencia sanitaria por COVID-19 una gran cantidad de las actividades cotidianas comenzaron a realizarse en línea, por lo que se debía esperar que se produzca un incremento en los ataques informáticos (Dias y Borges, 2018).

Según estadísticas de la Fiscalía General del Estado, en los meses de enero a junio de 2021 se han registrado 3762 denuncias de delitos informáticos, de los cuales 3190 son por apropiación fraudulenta por medios electrónicos, siendo este delito el que más casos registra a nivel nacional. Si se compara con las estadísticas del año 2020 se puede encontrar un total de 2744 casos de delitos informáticos, de los cuales apenas 1936 son por apropiación fraudulenta por medios electrónicos, esto demuestra que los delitos informáticos están en crecimiento (Flórez, 2021).

A pesar de ello, hay que tomar en cuenta que estas estadísticas solo muestran datos de los delitos informáticos denunciados, pero no se cuenta con datos en los casos en los que no se ha tenido denuncias.

Cuando las instituciones públicas o privadas son atacadas, deben buscar alguna alternativa para mitigar este inconveniente, normalmente las empresas cuentan con personal técnico en el área informática a quienes delegan la responsabilidad de administrar incidentes informáticos, instituciones con más recursos cuentan con equipos completos dedicados a este tema conocidos como Computer Emergency Response Team (CERTs). Según el sitio web csirt.ec creado por CEDIA, en Ecuador existen 19 Equipos de Respuesta ante Emergencias Informáticas (CSIRTs por sus siglas en inglés) orientados a las áreas de academia, nacional, militar, comercial y de infraestructura crítica (Ocampo, 2019).

Los miembros de la sociedad civil, por lo tanto, se encuentran más desprotegidos por el ejercicio de su ciudadanía digital a ataques informáticos, sin que exista una organización con la suficiente capacidad técnica para generar conciencia en la importancia del cuidado digital y le brinde soporte para resolver un incidente de carácter informático emergente, en los casos que así lo amerite; más aún un ciudadano no cuenta con un organismo de soporte para crear conciencia y prevenir incidentes (Ocampo, 2019).

Aquí nace la interrogante: ¿Cómo se podría atender los incidentes informáticos de la sociedad civil ecuatoriana?

Para responder esta interrogante se plantean las preguntas científicas de esta investigación:

- ¿Existen estudios para la implementación de centros de respuesta a incidentes informáticos para la sociedad civil?
- ¿Cuáles son los procedimientos más adecuados que debe implementar un centro de respuesta a incidentes informáticos para la sociedad civil ecuatoriana?
- ¿Con la aplicación de una guía para establecer un centro de respuesta a incidentes informáticos para la sociedad civil se mejora la prevención y atención de incidentes informáticos de un grupo de la sociedad civil ecuatoriana?

Por otra parte, el objetivo de este proyecto es aplicar la guía de implementación de un centro de respuesta a incidentes informáticos en una organización de la sociedad civil y para ello las tareas de investigación a desarrollar son:

- Fundamentación teórica del establecimiento de centros de respuesta a incidentes informáticos para la sociedad civil.
- Determinación de los procedimientos más adecuados para establecer centros de respuesta a incidentes informáticos para la sociedad civil.

- Elaboración de una guía para establecer centros de respuesta a incidentes informáticos para la sociedad civil.
- Implementación de la guía para establecer centros de respuesta a incidentes informáticos en una organización civil.
- Validación de la guía por parte de expertos.

En cuanto a la metodología de investigación, se desarrolla con un enfoque metodológico cualitativo y un diseño no experimental con corte transversal, mientras que para el desarrollo de la guía se utiliza la metodología de investigación acción – participativa.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

En el presente capítulo se analizan los conceptos más importantes en el establecimiento de un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT). En primer lugar, es importante el análisis de varios documentos relacionados con la creación de un centro de respuesta a incidentes informáticos tradicionales, pues no se logró encontrar ningún documento que oriente la creación de CSIRTS para la sociedad civil.

En el Manual básico de gestión de incidentes de seguridad informática del proyecto Amparo (2012) desarrollado por LACNIC, se presenta la información para el proceso organizacional y normativo para la integración de un CSIRT en una organización, los contenidos de este documento son:

- Descripción de la información básica que se debe conocer sobre esta en aplicaciones e infraestructura a tomar en cuenta, recomendaciones de posibles escenarios de inserción dentro de la organización y definiciones de las políticas de seguridad informática.
- Por otra parte, orienta a que el CSIRT defina los servicios que ofrece, los procedimientos para reportar incidentes, publicar sus políticas, procedimientos de operaciones, construcción de un documento base para comunicar información relevante a sus integrantes y un conjunto de temas y cuestiones que un CSIRT necesita elaborar para sus integrantes (p. 17).

En el documento de preguntas frecuentes del CSIRT (FAQ) construido por Carnegie Mellon University (2017) se plantean preguntas frecuentes que pueden venir a la mente en el momento de plantearse la creación de un CSIRT, algunas de ellas parte de conceptos esenciales como que es un CSIRT, los tipos, nombres más comunes, porque es necesario que una organización tenga un CSIRT, la estructura del mismo, los servicios que puede ofrecer, financiamiento, costos de creación de un CSIRT, entre otros (Carnegie Mellon University, 2017).

Este documento puede ser muy útil para responder a dudas puntuales antes y durante la creación de un CSIRT y podría ser el punto de partida para analizar documentación más extensa sobre el tema, tomando como consideración que las repuestas se describen de forma clara y pueden ser comprendidas por personas con poco conocimiento.

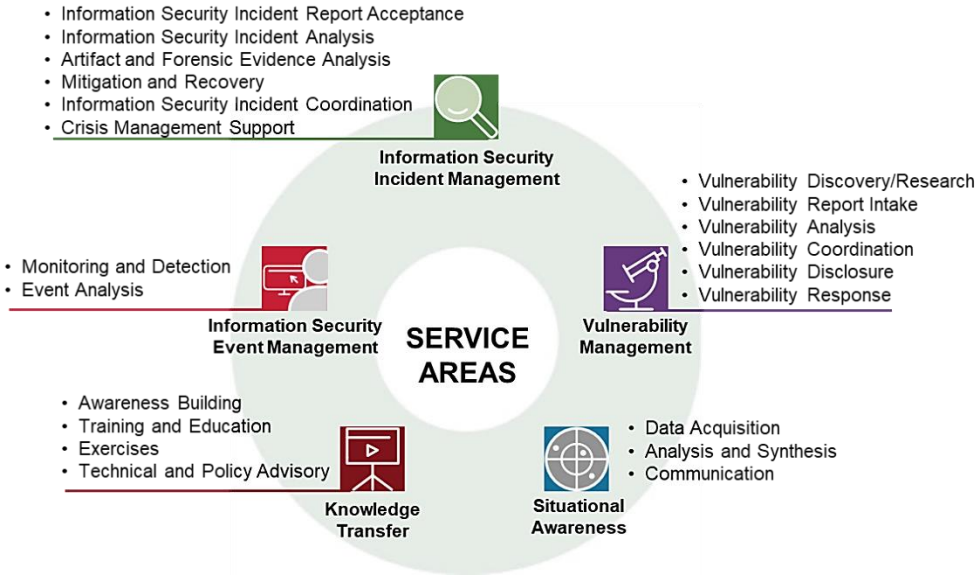
La guía a step-by-step approach on how to setup construido por ENISA (2006) es otra de las guías revisadas en esta investigación, la misma integra conceptos tales como: Estrategias generales para planificar y establecer un CSIRT, ¿Qué es un CSIRT?, el término Constituency, los beneficios de tenerla. Descripción de los diferentes tipos de entornos, posibles servicios que puede brindar.

Además, agrega una sección destinada a la construcción de un plan de negocios en el que brindan algunas alternativas para definir el modelo financiero, también se enfoca en determinar algunas características para el personal, los equipos de oficina, el desarrollo de las políticas de seguridad, ejemplos de procedimientos técnicos, manejo de incidentes, en general se podría decir que es una guía bastante completa (ENISA, 2006).

Dentro de las guías más interesantes se encuentra un CSIRT de Thai CERT traducido al español por CEDIA (2020), esta tiene algunos componentes que aparecen en los manuales anteriormente citados, pero se agregan elementos que son fundamentales como la gestión del ciclo de vida del equipo lo que permite medir y madurar la madurez de esta, además agrega algunos apéndices con material interesante para el proceso de implementación.

El último documento analizado proviene de FIRST (2019), el documento empieza centrado en una estructura de servicios basados en áreas:

Gráfico 1. CSIRT Services Framework Structure



Fuente*:* tomado a partir de Services Framework de FIRST (2019)

Continuando con el tema de gestión de incidentes de seguridad de la información, gestión de vulnerabilidades, conocimiento situacional y transferencia de conocimiento, al igual que el documento anterior, agrega algunos anexos que pueden ser útiles para el despliegue de un CSIRT.

En consecuencia, al revisar estas guías se observa que todas están orientadas a empresas, instituciones académicas o gobierno, pero no se encuentra ningún documento que guíe a una organización de la sociedad civil para la conformación de su propio CSIRT, por lo tanto, la importancia de este proyecto de desarrollo.

Partiendo de otro punto, la sociedad civil se define como un acuerdo de colaboración privada entre dos o más personas que quieren trabajar juntas para realizar una actividad con fines de lucro. Estos individuos tendrán la opción de elegir entre aportar mano de obra, lo que los califica como socios industriales, o bienes o dinero, lo que los califica como socios capitalistas (Torres y García, 2020).

Conviene mencionar un proyecto desarrollado por dentro del Ecuador por Chamorro et al. (2022) quien tuvo por objetivo conformar el CSIRT-UPEC, partiendo con la misión, visión y valores institucionales, aparte de establecer servicios, políticas, procesos para iniciar sus actividades. Actualmente, el Centro de Respuesta a Incidentes Informáticos de la Agencia de Regulación y Control de Telecomunicaciones EcuCERT de Arcotel y el grupo de centros de respuesta a incidentes informáticos CSIRT de Ecuador se encuentran trabajando en conjunto para gestionar la autorización, operación y funcionamiento del CSIRT-UPEC en la institución.

A nivel Latinoamérica, como menciona Barbosa (2021) el equipo de Respuesta a Emergencias Informáticas de México, también conocido como Mx-CERT (Equipo de Respuesta a Emergencias Informáticas de México), fue uno de los primeros CSIRT en América Latina. El "BA-Csirt", o "Instituto Tecnológico y de Estudios Superiores de Monterrey", es conocido actualmente como el primer "Csirt" de América Latina. Según el director del centro, Gustavo Lineares, el centro de ciberseguridad aborda desde los peligros más comunes en las redes sociales hasta el secuestro de información para informar a la población argentina.

1.1. Conceptos básicos sobre incidentes de ciberseguridad

Seguridad informática

Según Aguilera (2010) el campo de la seguridad informática se ocupa de crear las pautas, protocolos, procesos, métodos y técnicas necesarias para crear un sistema de información confiable y seguro. En los sistemas informáticos y las comunicaciones digitales las medidas de seguridad que se aplican no siempre son seguras al cien por ciento, tomando en cuenta que siempre una persona es quien utilizará los diferentes equipos o medios de comunicación.

Evento de ciberseguridad

Un evento de seguridad es una ocurrencia identificada de un sistema, servicio o red que indica una posible ruptura de la seguridad, de la política o una falla en los controles, o una situación desconocida previamente que pueda ser relevante para la seguridad (Fernández y Martínez, 2018).

Es importante distinguir entre un evento y un incidente debido a que los dos términos se utilizan a menudo como sinónimos, a pesar de que tienen diferentes significados. Un evento es cualquier cambio, error o interrupción dentro de una infraestructura de TI como un fallo del sistema, un error de disco o un usuario que olvide su contraseña (Bernal, 2021).

La Unión Internacional de Telecomunicaciones (2019) define un evento como cualquier situación observable en un sistema, la diferencia con el incidente es que este ocurre de manera espontánea y puede limitar el funcionamiento de cualquier equipo, en cambio, el evento que no es fortuito.

Incidentes de ciberseguridad

Un incidente se define como una serie de eventos no deseados o inesperados, que tienen una probabilidad importante de comprometer las operaciones de una organización y de amenazar la seguridad (Fernández y Martínez, 2018).

No todos los eventos de seguridad están clasificados como incidentes de seguridad, porque la ocurrencia de un evento de seguridad de la información no significa necesariamente que un intento haya sido exitoso o que haya cualquier implicación sobre la confidencialidad, integridad y/o disponibilidad (UIT, 2019).

Características de un incidente

Un incidente se caracteriza por presentar comportamientos o situaciones inusuales en sistemas y operaciones registradas como normales en una organización. El incidente se presenta cuando existen vulnerabilidades no descubiertas y por ende no son atendidas. De allí la recomendación de establecer los mecanismos de monitoreo y de detección que contribuyan a conocer mejor que sucede en red, y no impacte negativamente a la organización (Aguilar, 2019).

Basta con notar que algunos de los componentes de la tríada de seguridad de la información: Confidencialidad, Integridad y Disponibilidad se hayan afectado, para sospechar que se ha producido un incidente. Entre las características que pueden ayudar a reconocer un incidente, se tiene (Flórez, 2021):

- Anomalías en el tráfico de red interno y de salida: Pueden deberse a diversos factores, desde el uso de aplicaciones o servicios no reportados hasta la presencia de terminales comprometidos de usuarios que originan tráfico intencional o no hacia destinos sospechosos.
- Registro inusual de actividad de acceso a servicios: Esto puede indicar intentos de ingreso provenientes de usuarios no registrados para tal uso o una actividad maliciosa remota a través de algún terminal que haya sido infectado. Los intentos de acceso a servicios internos de la red, servidores y datos fuera de horario habitual de trabajo también deben ser considerados, así como los intentos de acceso inusuales a cuentas de usuario con privilegios.
- Información sospechosa adjunta en comunicaciones: La recepción de información adjunta en correos electrónicos de remitentes desconocidos no debería ser abierta, podría contener algún malware que actúa directamente o sirva para generar algún potencial ataque. Es importante desplegar una cultura de seguridad a través de programas de concientización acompañados de una evaluación constante que determine la efectividad de estos programas.

- Información modificada o no está disponible cuando es requerida: Puede deberse a que el canal de comunicación entre el usuario y la fuente de información haya sido interceptado, o el servidor de información este comprometido de tal forma que bloquea el servicio. Deben registrarse y monitorearse las conexiones remotas si se tratan de usuarios de la organización, así como establecer el seguimiento de aumento de uso de recursos computacionales en los servidores, de forma tal que se garantice la disponibilidad del servicio (p.33).

Gráfico 2. Componentes relacionados a la incidencia de ciberseguridad

Fuente: tomado a partir de Curso gestión de incidentes de ciberseguridad ITU Academy (2019)

De acuerdo con Ocampo (2019) un ejemplo simple para comprender la diferencia entre un evento y un incidente podría ser:

- **Evento:** Una persona está realizando un análisis de red utilizando nmap en la red interna, afortunadamente se ha podido detectar mediante un escaneo de red.
- **Incidente:** Una persona ha obtenido el acceso a la red interna y ha modificado las configuraciones de un dispositivo de red, en este caso al ser un incidente puede tener una connotación negativa en el ciclo de negocio de una empresa (p.88).

Tipos de incidentes

Los incidentes de ciberseguridad pueden ser involuntarios (error de configuración), o intencionales (ataque dirigido). Estos eventos también se pueden clasificar como técnicos o físicos. Los incidentes técnicos incluyen virus, malware, ataques de denegación de servicio (DoS) y fallos del sistema. Los incidentes físicos pueden incluir ingeniería social y la pérdida o robo de equipos de cómputo (Ríos, 2022).

Gráfico 3. Fases de la respuesta a incidentes

Fuente: tomado a partir de Curso gestión de incidentes de ciberseguridad ITU Academy (2019)

Vectores de ataque

Un vector de ataque es la técnica que emplea un atacante cuando intenta obtener acceso no autorizado a un sistema de TI y obtener datos confidenciales, con frecuencia aprovechando una debilidad en una red, sistema o aplicación. Los archivos adjuntos de correo electrónico, el malware, los troyanos o virus, las estafas de ingeniería social, el phishing, los ataques de fuerza bruta, las credenciales comprometidas obtenidas a través de una autenticación incorrecta, el robo de cuentas, la denegación de servicio distribuida y la explotación de API son algunos de los vectores de ataque más populares (Benavides et al., 2020).

Análisis de incidentes

Las actividades para el análisis de un incidente involucran una serie de componentes, por lo que es recomendable tener en cuenta lo siguiente (Cichonski et al., 2012):

- Tener conocimiento del estado normal del tráfico de red y operación de sistemas informáticos.
- Tener conocimiento total del comportamiento de la infraestructura tecnológica.
- Toda la información para el análisis de incidentes debe estar centralizada.
- Los productos de correlación de eventos estarán bien configurados.
- Se debe manejar una correcta base de conocimiento relacionada con incidentes de seguridad y nuevas vulnerabilidades.
- Documentar todos los incidentes ocurridos para los técnicos menos experimentados (p.31).

¿Qué es un CSIRT?

Un Centro de Respuesta a incidentes de Seguridad Informática es un equipo que ejecuta, coordina y asiste en la respuesta a incidentes de seguridad que involucren sistemas informáticos dentro de una comunidad predefinida (Tanczer et al., 2018).

Responder de forma apropiada e inmediata ante la ocurrencia de un incidente que pueda afectar a los recursos de los miembros de una comunidad determinada, resulta fundamental, puesto que permite desplegar y coordinar acciones con la finalidad de limitar o minimizar los efectos negativos de una determinada situación de riesgo, brindando una respuesta ante lo ocurrido (Tanczer et al., 2018).

Para lograr estos objetivos, un centro de respuesta también toma medidas preventivas, que buscan evitar o mitigar la ocurrencia de incidentes. Ejemplos de estas medidas son los programas de concientización y capacitación de usuarios, la implementación de controles de acceso robustos, etc. Sobre estos servicios se hará referencia más adelante (Bernal, 2021).

CSIRT debe cumplir diferentes propósitos. El primero de ellos consiste en controlar y minimizar cualquier tipo de daño a la organización y su información, junto con la preservación de evidencia sobre lo ocurrido y la documentación correspondiente. De esta forma, se conocerá el contexto del incidente, que permitirá determinar su origen y posibles consecuencias (Martínez, 2022).

También debe coordinar las actividades para una recuperación rápida y eficiente de las actividades que se han visto afectadas, en conjunto con los equipos de TI, de manera que la organización pueda operar con normalidad en el menor tiempo posible y con el menor impacto tolerable (Martínez, 2022).

Además, debe prevenir que eventos similares puedan ocurrir en el futuro, de tal forma que puedan erradicarse las causas raíz del incidente, junto con mantener una base de conocimientos que permita registrar las lecciones aprendidas de estos sucesos, con el objetivo de que no se repitan y si esto sucede, se pueda contar con un antecedente de la solución o soluciones posibles (Ocampo, 2019).

Nombre del centro de respuesta

Antes de empezar a operar, los centros de respuesta a incidentes deben adoptar una denominación que los identifique. La elección del nombre no obedece a parámetros preestablecidos, si bien los CERT que representan a países suelen incorporar las siglas que identifican al país como parte de su denominación (Ríos, 2022).

A lo largo del tiempo, la forma en que se nombran estos centros ha girado en torno a una serie de términos que se detallan a continuación (Mikly y Siegert, 2020).

- CERT, sigla de "*Computer Emergency Response Team*" CERT es una marca registrada en Estados Unidos del Centro de Coordinación del Software Engineering Institute (SEI) de la Universidad de Carnegie Mellon (CMU) en Estados Unidos, conocido como CERT/CC. Fue el primer grupo de respuesta a incidentes, creado en 1988 como respuesta al llamado Gusano de Morris, código malicioso que afectó a ARPANET, antecesora de Internet. Si bien hasta el año 2020, el SEI de CMU requería el cumplimiento de ciertos requisitos técnicos y legales para utilizar la denominación CERT, recientemente ha manifestado que solamente mantendrá el registro de la marca para los Estados Unidos de Norteamérica a partir del año 2020 según un correo electrónico enviado a los interesados en septiembre de 2020.
- CSIRT. Al ser un nombre genérico, no hay requerimientos previos para su uso. De hecho, SEI promueve el uso del acrónimo CSIRT para los centros de respuesta. En este documento se utilizará este nombre para hacer referencia a un centro de respuesta a incidentes.
- IRT, corresponde a "*Incident Response Team*" o Equipo de Respuesta a Incidentes. Es también otra forma de referirse a equipos de esta naturaleza, especialmente cuando actúan en el ámbito de una organización en particular.
- Los SOC, sigla que corresponde a "*Security Operations Center*" o Centro de Operaciones de Seguridad, constituyen áreas o departamentos que se ocupan de la parte operativa: realizar monitoreo en tiempo real del perímetro y las redes informáticas de una organización, para luego dar alertas ante la ocurrencia de un incidente y coordinar la respuesta (p.74).

Usualmente, los CSIRT más evolucionados o aquellos que deben proteger un número importante de recursos, integran una estructura en la que también opera un SOC, constituyendo éste una fuente de Información (Inostra et al., 2020).

Grupos e iniciativas existentes

Existen diversos grupos e iniciativas para el intercambio de información entre CSIRT a nivel mundial. Se brinda a continuación una breve reseña de los programas existentes para los equipos de la región a la fecha, con un breve detalle de las actividades que realizan y su ámbito de cobertura (LACNIC, 2012):

- **Lista de CSIRT de LACNIC:** Equipos de respuesta a incidentes de seguridad de la región Latinoamérica y del Caribe. Al seleccionar la opción de un determinado país de la 8 región, es posible desplegar el listado de CSIRT que han solicitado ser listados, con un detalle de contactos e información adicional.
- **Lista de Miembros de FIRST**: Es un listado de equipos de respuesta a incidentes de seguridad del mundo que son miembros de FIRST (Forum of Incident Response Teams). Se trata de una enumeración completa que provee información de contacto, organización y país al que pertenecen, comunidad objetiva, etc.
- **Lista de CERT Nacionales:** Es una convocatoria realizada por el SEI (Software 10 Engineering Institute) de la Universidad Carnegie Mellon para todos los equipos de respuesta a incidentes con representación nacional del país en el que se encuentran.
- **CSIRT de las Américas:** Se trata de una iniciativa de la OEA (Organización de los Estados Americanos) para equipos de gobierno de la región de América.
- **Listado de centros de respuesta acreditados ante Trusted-Introducer:** Se trata de una red de confianza implementada por una iniciativa europea, con el objetivo de incrementar la seguridad gracias a respuestas más

ágiles frente a ataques y nuevas amenazas. Ofrece servicios especializados y mantiene una base de datos de los equipos, proporcionando una visión general actualizada de su nivel de madurez y sus capacidades. Brinda un servicio de acreditación y certificación basado en buenas prácticas desarrolladas y probadas a lo largo de los años dentro de la propia comunidad (LACNIC, 2012).

CAPÍTULO II. DESARROLLO DE LA GUÍA PARA IMPLEMENTAR UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL

2.1. Metodología de la Investigación

Enfoque metodológico cualitativo

Según Salas et al. (2018) este método, también conocido como investigación naturalista, fenomenológica, interpretativa o etnográfica, es una especie de "paraguas" que agrupa una variedad de concepciones, visiones, técnicas y estudios no cuantitativos. Se seleccionó este enfoque para el proyecto de investigación tomando en cuenta que la guía permitirá implementar un CSIRT orientado a la sociedad civil y no se utilizarán elementos cuantificables.

Diseño no experimental con corte transversal

Es un procedimiento no experimental, transversal (ausencia de seguimiento) en el que una comunidad o una muestra representativa de esta son estudiadas en un momento dado. La valoración de las variables se hace en el mismo momento. Hay que cerciorarse de que la muestra elegida sea representativa de la población de estudio. En este caso el corte transversal se realizará cuando la guía esté lista y se procederá a la validación de esta por un equipo de expertos (Universidad de Jaén, 2018).

Método inductivo

Debido a que se utiliza un enfoque cualitativo, el método de investigación será inductivo, esto implica que partir de un fenómeno dado, se pueden encontrar similitudes en otro, permitiendo entender procesos, cambios y experiencias.

Técnica entrevista

Tomando en cuenta que este proyecto está orientado hacia la sociedad civil, parte del proyecto ha sido realizar un acercamiento a organizaciones internacionales que ya vienen brindando acompañamiento en seguridad digital para personas comunes y para ello la técnica de entrevista es la mejor opción (Dias y Borges, 2018).

Instrumento cuestionario

Para las entrevistas a las diferentes organizaciones se utiliza un cuestionario de 13 preguntas con el fin de obtener información relevante para la construcción de la guía, el cuestionario se puede encontrar en el anexo 1.

2.2. Metodología de desarrollo

En el presente proyecto se propone el desarrollo de una guía para implementar un centro de respuesta a incidentes informáticos para la sociedad civil, por tal motivo se ha visto conveniente utilizar una metodología para el desarrollo de la guía que permita involucrar a una organización que está brindando acompañamiento en seguridad digital a personas comunes, para ello la metodología utilizada es Investigación acción – participativa.

Según Espinoza (2020) la Investigación–Acción participativa hace referencia a un conjunto de corrientes y aproximaciones a la investigación que tienen en común tres pilares:

- **Investigación:** creencia en el valor y el poder del conocimiento y el respeto hacia sus distintas expresiones y maneras de producirlo; organizar la información.
- **Participación:** enfatizando los valores democráticos y el derecho a que las personas controlen sus propias situaciones y destacando la

importancia de una relación horizontal entre los investigadores y los miembros de una comunidad;

- **Acción:** como búsqueda de un cambio que mejore la situación de la comunidad involucrada (p.189).

En vista de esto se decidió utilizar esta metodología para lograr el mayor nivel de participación posible a lo largo de este proyecto de desarrollo, para lo cual se trabajó directamente con una organización en Ecuador que actualmente brinda acompañamiento en seguridad digital a periodistas, defensores de los derechos humanos, defensores de la tierra, etc.

Debido a la complejidad de su trabajo han solicitado que se mantenga la debida reserva del caso y que no se haga público su nombre, por lo que de ahora en adelante se denominara: La Organización.

En esta etapa se realizó revisión documental de manuales desarrollados por varias organizaciones dentro de los cuales se tiene:

Tabla 1. Manuales revisados

NOMBRE	ORGANIZACIÓN	INFORMACIÓN IMPORTANTE PARA LA GUÍA	AÑO
Manual básico de gestión de incidentes de seguridad informática	LACNIC	• Introducción a la gestión de incidentes de seguridad informática. • Definiciones clave y terminología utilizada en la gestión de incidentes. • Estructura y roles de un equipo de respuesta a incidentes de seguridad (CSIRT). • Tipos de incidentes de seguridad informática y clasificación de su gravedad. • Procesos de detección, notificación y registro de incidentes. • Evaluación y análisis de incidentes. • Escalamiento y coordinación de la respuesta a incidentes. • Mitigación y contención	2012

		de incidentes en curso. • Recopilación de evidencia y seguimiento forense. • Comunicación y coordinación con partes interesadas internas y externas. • Procedimientos de recuperación y restauración de servicios. • Análisis de lecciones aprendidas y mejora continua. • Consideraciones éticas y legales en la gestión de incidentes. • Recomendaciones de buenas prácticas y medidas de seguridad preventivas.	
CSIRT frequently asked questions (FAQ)	CERT	Se seleccionaron preguntas para ir dando forma a la estructura del marco de trabajo: • ¿Qué es un CSIRT y cuál es su función principal? • ¿Cuáles son los beneficios de establecer un CSIRT? • ¿Cuáles son los roles y responsabilidades típicos dentro de un CSIRT? • ¿Cuál es el proceso de notificación de incidentes al CSIRT? • ¿Cómo se clasifican y priorizan los incidentes dentro de un CSIRT? • ¿Cuáles son las fases típicas de respuesta a incidentes de seguridad? • ¿Cuáles son las mejores prácticas para la recopilación y preservación de evidencia? • ¿Cuáles son las medidas de seguridad recomendadas para prevenir incidentes? • ¿Cómo se coordina la respuesta a incidentes con otras organizaciones y	2017

		entidades? • ¿Cuál es el proceso de gestión de comunicaciones durante un incidente? • ¿Qué herramientas y tecnologías son útiles para un CSIRT? • ¿Cuáles son los desafíos comunes que enfrenta un CSIRT y cómo superarlos? • ¿Qué recursos y referencias adicionales están disponibles para obtener más información?	
A step-by-step approach on how to setup a CSIRT	ENISA	En el caso de la Guía de ENISA se toman en cuenta los siguientes elementos importantes para este trabajo de titulación: • Introducción a la creación de un CSIRT (Computer Security Incident Response Team). • Evaluación de la necesidad y justificación para establecer un CSIRT. • Definición de los objetivos y alcance del CSIRT. • Identificación de las partes interesadas y las responsabilidades involucradas. • Establecimiento de la estructura organizativa y los roles del CSIRT. • Selección de un modelo de operación adecuado (por ejemplo, modelo interno, externalización o colaboración). • Definición de los procesos de gestión de incidentes de seguridad. • Implementación de herramientas y tecnologías para el manejo de incidentes. • Creación de políticas y procedimientos internos del CSIRT. • Desarrollo de acuerdos de cooperación con	2006

		otros CSIRT y organizaciones relevantes. • Definición de un plan de comunicación interna y externa durante los incidentes. • Establecimiento de métricas y criterios de medición para evaluar la efectividad del CSIRT. • Implementación de mecanismos de retroalimentación y mejora continua.	
Estableciendo un CSIRT	ThaiCERT – Traducido por CEDIA	Algunos de los elementos destacados de esta guía coinciden con los de otra documentación, pero cuentan con elementos importantes a destacar: • Introducción al establecimiento de un CSIRT: objetivos y beneficios. • Evaluación de la necesidad y justificación para establecer un CSIRT en la organización. • Definición de la estructura organizativa y los roles del CSIRT. • Selección de un modelo operativo adecuado para el CSIRT (por ejemplo, interno, externo o híbrido). • Identificación de las responsabilidades y funciones clave dentro del CSIRT. • Establecimiento de políticas y procedimientos para la gestión de incidentes de seguridad. • Desarrollo de un plan de respuesta a incidentes que incluya actividades de preparación, detección, contención, mitigación y recuperación. • Definición de los flujos de comunicación interna y externa durante los	2020

		incidentes. • Implementación de herramientas y tecnologías adecuadas para la detección y respuesta a incidentes. • Establecimiento de un marco de colaboración con otras entidades, tanto a nivel nacional como internacional. • Creación de un programa de concienciación y capacitación en seguridad de la información para el personal. • Desarrollo de mecanismos de reporte de incidentes y gestión de solicitudes de ayuda. • Implementación de métricas y evaluación periódica del desempeño del CSIRT. • Establecimiento de un proceso de revisión y mejora continua de las actividades del CSIRT.	
Computer Security Incident Response Team (CSIRT) Services Framework Version 2.1.0	FIRST	El marco de servicios del Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) de la versión 2.1.0 proporciona orientación sobre los servicios que un CSIRT puede ofrecer. A continuación, se presentan algunos puntos importantes que se tomaron en cuenta en dicho marco: • Introducción al CSIRT Services Framework y su propósito. • Descripción de los servicios principales que un CSIRT puede ofrecer. • Servicio de gestión de incidentes: descripción de las actividades relacionadas con la detección, notificación, análisis, mitigación y resolución de incidentes de seguridad informática. • Servicio de respuesta a incidentes: explicación	2019

		detallada de cómo el CSIRT responde a los incidentes de seguridad de manera oportuna y eficiente. • Servicio de coordinación: información sobre la colaboración y coordinación con otros CSIRT, organizaciones gubernamentales y agencias de seguridad para mejorar la respuesta a incidentes a nivel nacional o internacional. • Servicio de inteligencia de amenazas: descripción de las actividades de recolección, análisis y divulgación de información sobre amenazas y ataques cibernéticos para mejorar la postura de seguridad de la organización. • Servicio de gestión de vulnerabilidades: explicación de las actividades relacionadas con la identificación, clasificación y mitigación de vulnerabilidades en los sistemas de la organización. • Servicio de gestión de crisis: orientación sobre cómo manejar situaciones de crisis y desastres relacionados con la seguridad informática, incluyendo la continuidad del negocio y la recuperación ante desastres. • Servicio de concienciación y capacitación: descripción de las actividades de educación y capacitación para concienciar a los usuarios y mejorar la seguridad informática en	

		la organización. • Servicio de análisis forense: información sobre las actividades de recolección, análisis y preservación de evidencia digital para investigar incidentes y apoyar en procesos legales. • Servicio de gestión de incidentes de terceros: orientación sobre cómo colaborar y brindar soporte a otros CSIRT y organizaciones externas en la gestión de incidentes. • Marco de gobernanza y gestión de calidad del CSIRT: descripción de las mejores prácticas para la gobernanza, gestión de riesgos y aseguramiento de la calidad en las operaciones del CSIRT. • Consideraciones legales y éticas: información sobre las implicaciones legales y éticas en la prestación de los servicios del CSIRT. • Recomendaciones para la implementación y mejora continua de los servicios del CSIRT	
National Computer Security Incident Response Teams (CSIRTs)	GFCE Global Good Practices	El documento "National Computer Security Incident Response Teams (CSIRTs)" de GFCE Global Good Practices proporciona orientación sobre las mejores prácticas para los equipos nacionales de respuesta a incidentes de seguridad informática (CSIRTs). A continuación, se presentan algunos puntos importantes que se tomaron en cuenta para este trabajo de investigación: • Introducción a los CSIRTs nacionales y su importancia en la gestión de incidentes de seguridad informática a nivel nacional. • Estructura y organización de un CSIRT nacional,	2017

		incluyendo roles y responsabilidades. • Establecimiento de políticas y marcos legales para respaldar las operaciones del CSIRT nacional. • Proceso de detección, notificación y gestión de incidentes de seguridad informática. • Establecimiento de mecanismos de coordinación y colaboración con otros CSIRTs, organizaciones internacionales y sectores relevantes. • Desarrollo de capacidades y habilidades técnicas para los miembros del CSIRT nacional. • Implementación de un sistema de alerta temprana para identificar y responder rápidamente a las amenazas emergentes. • Establecimiento de programas de concienciación y educación en seguridad informática a nivel nacional. • Colaboración con el sector privado, academia y sociedad civil para promover la seguridad informática en el país. • Desarrollo de un plan de continuidad del negocio y recuperación ante desastres para el CSIRT nacional. • Recopilación, análisis y compartición de información sobre amenazas y vulnerabilidades para mejorar la postura de seguridad nacional. • Implementación de medidas de seguridad proactivas para prevenir incidentes y fortalecer la resiliencia del país.	

		• Establecimiento de mecanismos de evaluación y mejora continua de las operaciones y capacidades del CSIRT nacional. • Consideraciones éticas y legales en la gestión de incidentes de seguridad informática a nivel nacional.	

Fuente: elaboración propia

Además, se entrevistó a varias organizaciones en el ámbito de Latinoamérica con el objetivo de conocer su manera de acompañamiento hacia la sociedad civil. El siguiente listado fue definido con base en parámetros como ubicación y años de experiencia dentro del campo, para ello se utilizó un cuestionario presentado en el Anexo 1. Se tomó la decisión de entrevistar a estas organizaciones debido a su experiencia y acompañamiento hacia la sociedad civil. Se aplicó durante los meses de enero y febrero de 2022 de manera virtual, en una sesión de 1 hora con cada organización.

Tabla 2. Listado de organizaciones entrevistadas

Organización	**Ubicación**
CiviCERT	Internacional varios países
Hiperderecho	Perú
Sursiendo	México
COLNODO	Colombia

Fuente: elaboración propia

Las entrevistas fueron realizadas por el autor del presente trabajo de investigación, se documentaron en formato de pódcast presentado para el programa Líderes 2.0 de LACNIC con el título: “Experiencias y retos del acompañamiento en seguridad digital a organizaciones sociales de Latinoamérica” y son accesibles desde el link: https://conexioneducativa.org/site/podcast/

Análisis de la entrevista

Durante la entrevista a las diferentes organizaciones se pudo destacar principalmente la importancia de definir un público objetivo para el CSIRT este público objetivo se define como Constituency, es importante tener claro hacia quien va dirigido el apoyo técnico, pues al ser un grupo tan amplio la sociedad civil se debe priorizar los grupos que tienen mayor riesgo, dentro de las organizaciones entrevistadas los grupos con mayor riesgo y necesidad de acompañamiento en seguridad digital son: Periodistas, Comunicadores, Activistas y Defensores de Derechos Humanos.

Además, se destaca la importancia de la formación de los profesionales encargados de la gestión de incidentes, pues se destaca que deberían tener una formación híbrida tanto técnica como social para poder abordar los requerimientos de la población, es indicar que dependiendo del país en el que se ubican los riesgos digitales pueden empeorar, pues existen países mucho más represivos en el que la utilización de algunas técnicas para mejorar la privacidad en internet pueden ser considerados delitos.

En cuanto a los temas más requeridos por la sociedad civil para la prevención de incidentes informáticos, todas las organizaciones entrevistadas coinciden en que son temas básicos como el manejo de un gestor de contraseñas para mejorar la creación de estas, activación de un segundo factor de autentificación, cifrado de correo electrónico, navegación segura y anónima.

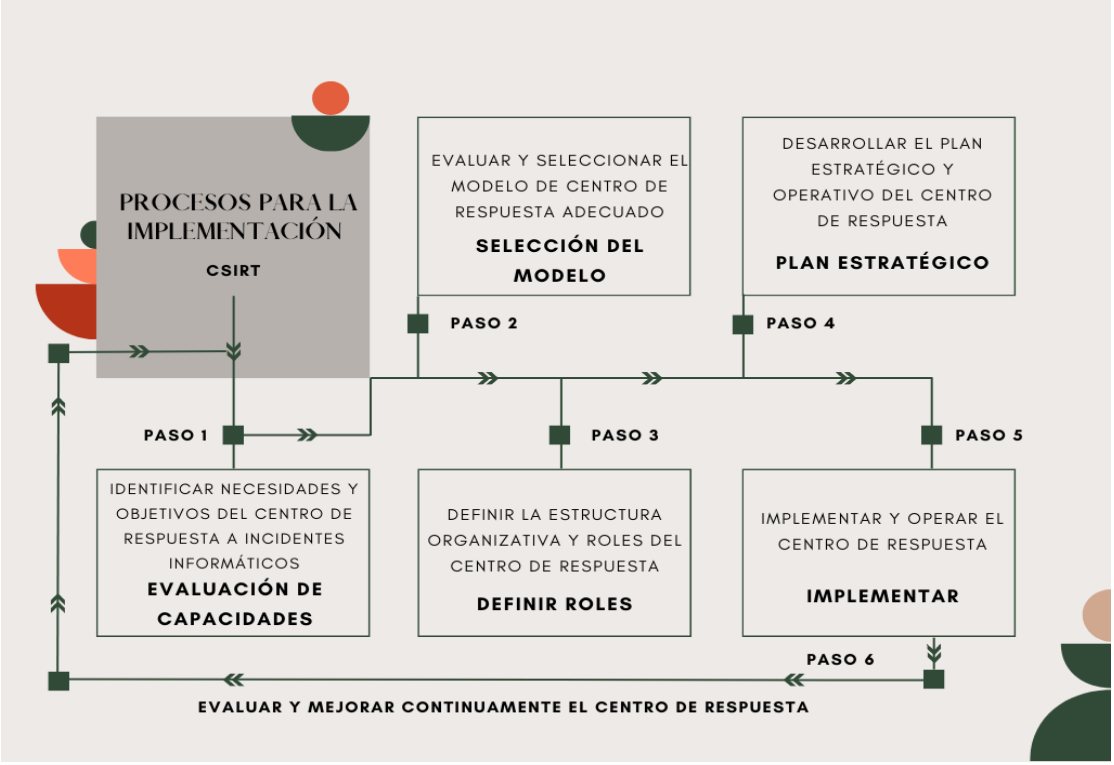
Con base en estas entrevistas se determinó algunos elementos importantes para la implementación de un CSIRT para la sociedad civil, específicamente relacionado con recursos, capacidades técnicas del personal y los protocolos de gestión de incidentes.

Fase de Participación

En la etapa de participación activa se solicitó el apoyo a un colectivo de la sociedad civil que brinda acompañamiento en seguridad digital, con el apoyo de los miembros de la organización se sistematizó algunos elementos fundamentales de los procesos que vienen desarrollando y se recabó información importante sobre su trabajo. El fin de solicitar apoyo a una sociedad civil se debe al respaldo que se tiene para ejecutar acciones concretas y porque bajo consideración de los autores, la sociedad necesita más apoyo, además de la experiencia que disponen en la materia, todos con el objetivo de brindar apoyo a la sociedad civil.

Para determinar el mejor procedimiento para implementar un centro de respuesta a incidentes informáticos para la sociedad civil se generó un flujograma de proceso en conjunto con la organización participante, el mismo que se define a continuación:

Gráfico 4. Procesos para la implementación de la guía



Fuente: elaboración en conjunto con la organización participante

Fase de Acción

Para el proceso de construcción de la guía se utilizó toda la información obtenida en las fases anteriores, en primera instancia se elaboró una lista de los contenidos que deberían constar en la misma, definiendo la estructura de la guía de la siguiente manera:

Tabla 3. Contenidos de la guía

Tabla de contenidos

1. Conceptos clave
- 1.1. ¿Qué es un centro de respuesta a incidentes informáticos para la sociedad civil?
- 1.2. ¿Cuáles son los elementos clave para la creación de un centro de respuesta a incidentes informáticos para la sociedad civil?
- 1.3. Los objetivos de un CSIRT para la sociedad civil

2. Planificación
- 2.1. Planificación del marco de trabajo
  - 1.1.1. Misión
  - 1.1.2. Grupo objetivo, o Constituency
  - 1.1.3. Equipo
  - 1.1.4. Disponibilidad
  - 1.1.5. Relaciones internas y externas
  - 1.1.6. Servicios
  - 1.1.7. Infraestructura y herramientas
- 1.2. Protocolo de atención de casos y verificación de identidad

2. Puesta en marcha del CSIRT
- 2.1. Implementación de herramientas tecnológicas
- 2.2. Comunicación de la existencia del CSIRT
- 2.3. Recursos para mejorar el acompañamiento en seguridad digital
- 2.4. Midiendo la madurez del CSIRT

Fuente: elaboración propia

El resultado final de la guía se puede consultar en el anexo 3.

Actividades realizadas para la implementación de la guía:

Identificar necesidades y objetivos del centro de respuesta a incidentes informáticos

Fecha: 22 de enero de 2022

Gráfico 5. Evidencia reunión virtual identificación de necesidades y evaluación

Fuente: elaboración propia

Como primera actividad se celebra una reunión virtual con los miembros de la organización para identificar necesidades y objetivos del centro de respuesta a incidentes informáticos, además de evaluar y seleccionar el modelo del centro con la participación de la organización, posteriormente se realiza la evaluación de preparación y capacidad del equipo mediante las preguntas presentadas en el Anexo 2 se clasifica esta evaluación en 4 áreas:

- Área 1: Estructura y organización del equipo
- Área 2: Recursos y capacidades técnicas
- Área 3: Capacidades de gestión de incidentes
- Área 4: Colaboración y coordinación

Los resultados se presentan a continuación:

Tabla 4. Evaluación del equipo del CSIRT – Área 1

Tabla de respuestas Evaluación del equipo de CSIRT - Área 1				
Existe un organigrama definido que muestra la estructura y roles del equipo de CSIRT	El equipo cuenta con un líder claramente designado y con autoridad para tomar decisiones	Hay un plan de sucesión para asegurar la continuidad del equipo en caso de cambios en el personal clave	Existe un proceso documentado para la gestión de incidentes, incluyendo la recepción, clasificación, investigación y resolución de los mismos	Se han definido las responsabilidades y los niveles de autoridad para cada miembro del equipo
NO	**SI**	**NO**	**NO**	**NO**

Fuente: elaboración propia

La tabla muestra las respuestas de una persona evaluada en el Área 1: Estructura y organización del equipo del CSIRT.

¿Existe un organigrama definido que muestre la estructura y roles del equipo de CSIRT?

Respuesta: NO

Interpretación: Según la evaluación de la persona, no existe un organigrama definido que muestre la estructura y los roles del equipo de CSIRT. Esto puede indicar una falta de claridad en cuanto a la organización y las responsabilidades dentro del equipo.

¿El equipo cuenta con un líder claramente designado y con autoridad para tomar decisiones?

Respuesta: SI

Interpretación: Según la evaluación de la persona, el equipo cuenta con un líder claramente designado y con autoridad para tomar decisiones. Esto indica que hay una figura de liderazgo establecida en el equipo, lo que puede facilitar la toma de decisiones y la dirección del CSIRT.

¿Hay un plan de sucesión para asegurar la continuidad del equipo en caso de cambios en el personal clave?

Respuesta: NO

Interpretación: Según la evaluación de la persona, no existe un plan de sucesión para asegurar la continuidad del equipo en caso de cambios en el personal clave. Esto puede representar un riesgo para la continuidad operativa del CSIRT, la salida de miembros clave podría generar vacíos en el equipo.

¿Existe un proceso documentado para la gestión de incidentes, incluyendo la recepción, clasificación, investigación y resolución de los mismos?

Respuesta: NO

Interpretación: Según la evaluación de la persona, no existe un proceso documentado para la gestión de incidentes. Esto puede indicar una falta de estructura y procedimientos claros para abordar y resolver los incidentes de seguridad de manera eficiente y efectiva.

¿Se han definido las responsabilidades y los niveles de autoridad para cada miembro del equipo?

Respuesta: NO

Interpretación: Según la evaluación de la persona, no se han definido las responsabilidades y los niveles de autoridad para cada miembro del equipo. Esto puede generar confusión y falta de claridad en cuanto a las tareas y roles específicos de cada integrante del CSIRT.

En general, esta evaluación sugiere que el Área 1: Estructura y organización del equipo del CSIRT presenta algunas debilidades, como la falta de un organigrama definido, la ausencia de un plan de sucesión, la falta de un proceso documentado

para la gestión de incidentes y la falta de definición de responsabilidades y niveles de autoridad. Estos aspectos pueden afectar la eficacia y la capacidad de respuesta del equipo frente a incidentes de seguridad.

Tabla 5. Evaluación del equipo del CSIRT – Área 2

Tabla de respuestas Evaluación del equipo de CSIRT - Área 2				
El equipo cuenta con los recursos técnicos necesarios, como hardware, software y herramientas de seguridad	Se mantiene actualizado un inventario de los recursos técnicos y se realizan regularmente las actualizaciones y mejoras necesarias	El equipo tiene acceso a la información y las fuentes de inteligencia de seguridad necesarias para detectar y responder a incidentes	Se lleva a cabo un monitoreo constante de los sistemas de información y se registran los eventos relevantes	Se realizan pruebas periódicas de los mecanismos de detección y respuesta para asegurar su eficacia
SI	**NO**	**NO**	**SI**	**SI**

Fuente: elaboración propia

La tabla muestra las respuestas de la evaluación en el área 2 de recursos y capacidades técnicas.

¿El equipo cuenta con los recursos técnicos necesarios, como hardware, software y herramientas de seguridad?

Respuesta: SI

Interpretación: Según la evaluación de la persona, el equipo cuenta con los recursos técnicos necesarios, como hardware, software y herramientas de seguridad. Esto indica que el equipo dispone de los elementos fundamentales para llevar a cabo sus funciones y tareas de seguridad informática.

¿Se mantiene actualizado un inventario de los recursos técnicos y se realizan regularmente las actualizaciones y mejoras necesarias?

Respuesta: NO

Interpretación: Según la evaluación de la persona, no se mantiene actualizado un inventario de los recursos técnicos, ni se realizan regularmente las actualizaciones y mejoras necesarias. Esto puede implicar un riesgo, la falta de seguimiento y actualización de los recursos técnicos puede generar vulnerabilidades y dificultar la eficacia del equipo.

¿El equipo tiene acceso a la información y las fuentes de inteligencia de seguridad necesarias para detectar y responder a incidentes?

Respuesta: NO

Interpretación: Según la evaluación de la persona, el equipo no tiene acceso a la información y fuentes de inteligencia de seguridad necesarias para detectar y responder a incidentes. Esto puede limitar la capacidad del equipo para anticiparse a amenazas y responder de manera efectiva a incidentes de seguridad.

¿Se lleva a cabo un monitoreo constante de los sistemas de información y se registran los eventos relevantes?

Respuesta: SI

Interpretación: Según la evaluación de la persona, se lleva a cabo un monitoreo constante de los sistemas de información y se registran los eventos relevantes. Esto indica que el equipo está activamente monitoreando los sistemas en busca de posibles incidencias y registrando los eventos que requieren atención y análisis posterior.

¿Se realizan pruebas periódicas de los mecanismos de detección y respuesta para asegurar su eficacia?

Respuesta: SI

Interpretación: Según la evaluación de la persona, se realizan pruebas periódicas de los mecanismos de detección y respuesta para asegurar su eficacia. Esto demuestra que el equipo reconoce la importancia de probar y validar regularmente sus sistemas y procesos de detección y respuesta para mantener su eficacia y capacidad de respuesta ante incidentes.

En general, esta evaluación del Área 2 indica que el equipo cuenta con los recursos técnicos necesarios, pero existen áreas de mejora en cuanto al mantenimiento y actualización de inventarios, acceso a información de seguridad y fuentes de inteligencia, así como en la realización de pruebas periódicas. Estas áreas pueden requerir atención para fortalecer la capacidad del equipo en materia de recursos y capacidades técnicas.

Tabla 6. Evaluación del equipo del CSIRT – Área 3

Tabla de respuestas

Evaluación del equipo de CSIRT - Área 3

Se ha establecido un plan de gestión de incidentes que incluya los procedimientos y protocolos a seguir en caso de incidentes de seguridad	El equipo ha participado en ejercicios y simulaciones de incidentes para practicar y mejorar sus capacidades de respuesta	Existe un proceso claro para la comunicación interna y externa durante la gestión de incidentes	Se lleva a cabo una revisión post-incidente después de cada incidente importante para identificar lecciones aprendidas y áreas de mejora	El equipo mantiene registros adecuados de los incidentes gestionados, incluyendo información relevante sobre la respuesta y las medidas tomadas
SI	**NO**	**SI**	**NO**	**SI**

Fuente: elaboración propia

En la tabla presentada se muestran las respuestas de la evaluación del área 3 correspondientes a capacidades de gestión de incidentes.

¿Se ha establecido un plan de gestión de incidentes que incluya los procedimientos y protocolos a seguir en caso de incidentes de seguridad?

Respuesta: SI

Interpretación: El equipo de CSIRT ha establecido un plan de gestión de incidentes que incluye los procedimientos y protocolos necesarios para abordar los incidentes de seguridad. Esto indica que el equipo está preparado y cuenta con una estructura clara para manejar las situaciones de seguridad.

¿El equipo ha participado en ejercicios y simulaciones de incidentes para practicar y mejorar sus capacidades de respuesta?

Respuesta: NO

Interpretación: El equipo de CSIRT no ha participado en ejercicios y simulaciones de incidentes para practicar y mejorar sus habilidades y capacidades de respuesta. Sería beneficioso que el equipo considere la realización de ejercicios y simulaciones para fortalecer sus habilidades y prepararse de manera más efectiva para responder a incidentes.

¿Existe un proceso claro para la comunicación interna y externa durante la gestión de incidentes?

Respuesta: SI

Interpretación: El equipo de CSIRT tiene establecido un proceso claro para la comunicación tanto interna como externa durante la gestión de incidentes. Esto asegura que la información se comparte de manera efectiva y se mantienen canales de comunicación abiertos durante la respuesta a incidentes.

¿Se lleva a cabo una revisión post incidente después de cada incidente importante para identificar lecciones aprendidas y áreas de mejora?

Respuesta: NO

Interpretación: El equipo de CSIRT no lleva a cabo revisiones post-incidente después de incidentes importantes para identificar lecciones aprendidas y áreas de mejora. Sería recomendable implementar estas revisiones para aprovechar las oportunidades de aprendizaje y mejorar los procesos y prácticas del equipo.

¿El equipo mantiene registros adecuados de los incidentes gestionados, incluyendo información relevante sobre la respuesta y las medidas tomadas?

Respuesta: SI

Interpretación: El equipo de CSIRT mantiene registros adecuados de los incidentes gestionados, lo que implica que se registra información relevante sobre la respuesta y las medidas tomadas para resolver los incidentes. Esto es importante para el seguimiento, análisis y aprendizaje continuo del equipo en la gestión de incidentes. Recuerda que estas interpretaciones se basan en las respuestas proporcionadas y es necesario considerar el contexto específico de cada situación para realizar una evaluación completa.

Tabla 7. Evaluación del equipo del CSIRT – Área 4

Tabla de respuestas

Evaluación del equipo de CSIRT - Área 4

El equipo tiene establecidos canales de comunicación y colaboración con otros equipos y entidades relevantes, tanto internas como externas	Se participa activamente en la comunidad de seguridad informática y se comparten experiencias y conocimientos con otros expertos	Se realizan actividades de capacitación y formación para mantener actualizadas las habilidades y conocimientos del equipo	El equipo realiza revisiones regulares de su desempeño y busca oportunidades para mejorar sus procesos y habilidades	Se promueve una cultura de aprendizaje y mejora continua dentro del equipo
SI	**SI**	**SI**	**SI**	**SI**

Fuente: elaboración propia

En la tabla anterior se presentan las respuestas de la evaluación del CSIRT en el área 4.

¿El equipo tiene establecidos canales de comunicación y colaboración con otros equipos y entidades relevantes, tanto internas como externas?

Respuesta: SI

Interpretación: El equipo tiene canales establecidos de comunicación y colaboración con otros equipos y entidades relevantes, tanto dentro como fuera de la organización. Esto facilita la interacción y el intercambio de información para abordar de manera efectiva los desafíos de seguridad.

¿Se participa activamente en la comunidad de seguridad informática y se comparten experiencias y conocimientos con otros expertos?

Respuesta: SI

Interpretación: El equipo se involucra de manera activa en la comunidad de seguridad informática, participando en actividades y compartiendo experiencias y conocimientos con otros expertos. Esto permite mantenerse actualizados sobre las últimas tendencias y prácticas en seguridad.

¿Se realizan actividades de capacitación y formación para mantener actualizadas las habilidades y conocimientos del equipo?

Respuesta: SI

Interpretación: El equipo se somete regularmente a actividades de capacitación y formación para actualizar sus habilidades y conocimientos en seguridad. Esto asegura que estén al tanto de las últimas tecnologías y técnicas, fortaleciendo así su capacidad para enfrentar los desafíos de seguridad.

¿El equipo realiza revisiones regulares de su desempeño y busca oportunidades para mejorar sus procesos y habilidades?

Respuesta: SI

Interpretación: El equipo lleva a cabo revisiones periódicas de su desempeño, buscando identificar áreas de mejora en sus procesos y habilidades. Esto demuestra un enfoque proactivo hacia la mejora continua y la excelencia en la gestión de la seguridad.

¿Se promueve una cultura de aprendizaje y mejora continua dentro del equipo?

Respuesta: SI

Interpretación: Dentro del equipo se fomenta una cultura de aprendizaje y mejora continua, donde se valora el aprendizaje constante, la adopción de mejores prácticas y la innovación en seguridad. Esto crea un ambiente propicio para el crecimiento y el desarrollo profesional del equipo.

Estas respuestas indican que el equipo de CSIRT demuestra un compromiso sólido con la colaboración, el aprendizaje y la mejora continua en el ámbito de la seguridad informática.

Evaluar y seleccionar el modelo de centro de respuesta adecuado

Fecha: 26 de marzo de 2022

Según la guía se propone 4 modelos para el CSIRT, la organización seleccionó uno de los modelos basado en 5 parámetros:

- Coordinación: Nivel de coordinación entre los equipos de respuesta a incidentes.

- Distribución de responsabilidades: Distribución de las responsabilidades de manejo de incidentes de seguridad.
- Comunicación: Nivel de comunicación entre los equipos y entidades relevantes.
- Políticas y procedimientos: Tipo de organización de las políticas y procedimientos.
- Recursos compartidos: Nivel de recursos compartidos entre los equipos de respuesta a incidentes.

Para determinar el mejor modelo, la organización asignó una puntuación del 1 al 5 a cada parámetro para de esta forma compararlos.

Tabla 8. Evaluación del equipo del CSIRT – Área 4

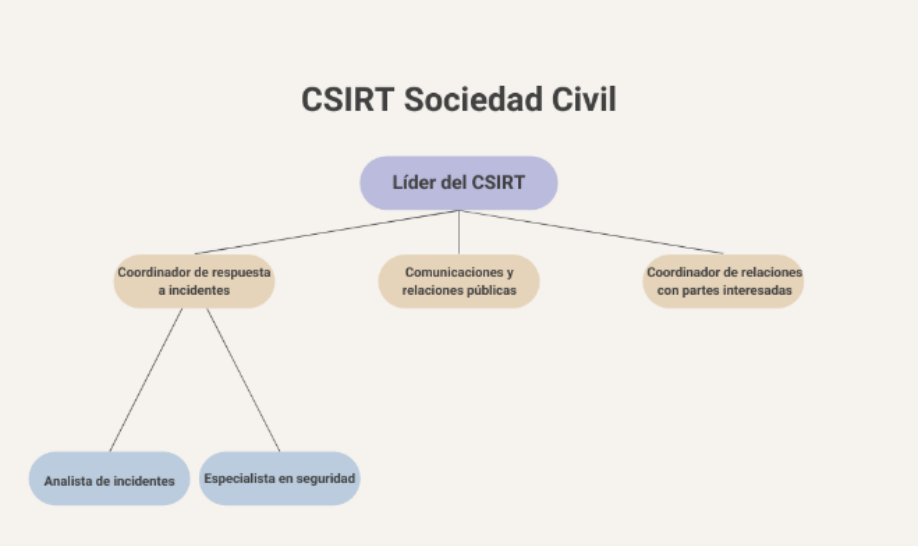
	Modelo	Parámetro.1	Parámetro.2	Parámetro.3	Parámetro.4	Parámetro.5	Puntuación_Total
3	Colaborativo	3	5	5	4	5	22
4	Híbrido	4	4	4	5	4	21
1	Centralizado	4	3	2	4	3	16
2	Descentralizado	2	4	3	3	4	16

Fuente: elaboración por parte de la organización participante

Definir la estructura organizativa y roles del centro de respuesta

Fecha: 26 de marzo de 2022

Gráfico 6. Organigrama interno del CSIRT



Fuente: elaboración de la organización participante

Se celebra una reunión virtual para la elaboración del organigrama interno del CSIRT. Esta es una actividad realizada en conjunto con la organización participante, donde se definen los roles de cada uno de los miembros y las funciones claves que tendrán dentro del equipo.

Desarrollar el plan estratégico y operativo del centro de respuesta

Fecha: 2 de abril de 2022

Gráfico 7. Evidencia reunión presencial construcción del plan estratégico y operativo del centro de respuesta

Fuente: elaboración propia

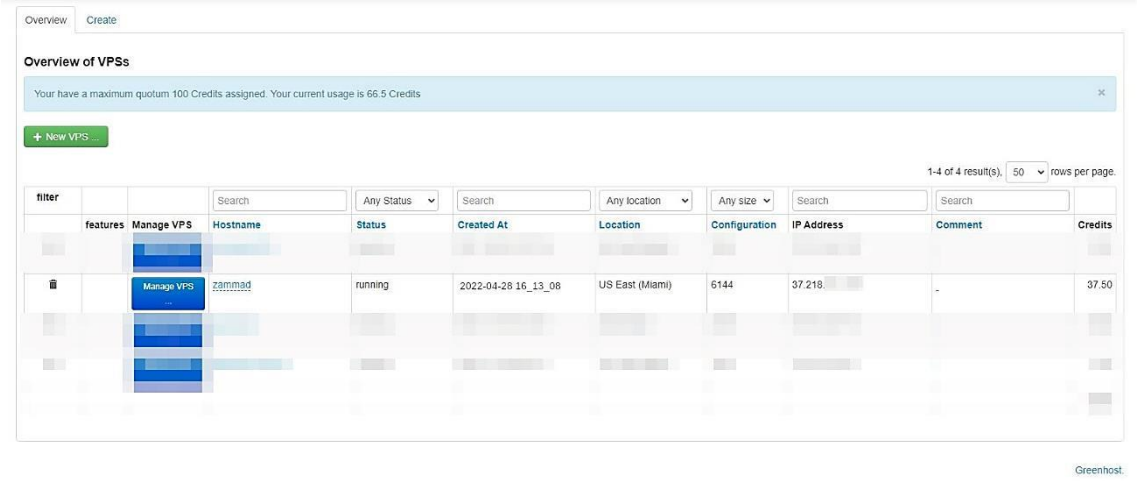
Durante dos días de forma presencial se realizó la construcción del plan estratégico y operativo del CSIRT, a su vez se definió el protocolo de atención de casos que se puede encontrar en el plan operativo, este documento ha sido anonimizado eliminando información de la organización participante, misma se encuentra como evidencia en el anexo 4.

Implementación de herramientas tecnológicas para el CSIRT.

Fecha: Febrero – Marzo 2022

Se gestiona un VPS para la organización con la empresa GreenHost, ellos proveen servicio gratuito mediante el proyecto Eclipse https://eclips.is/

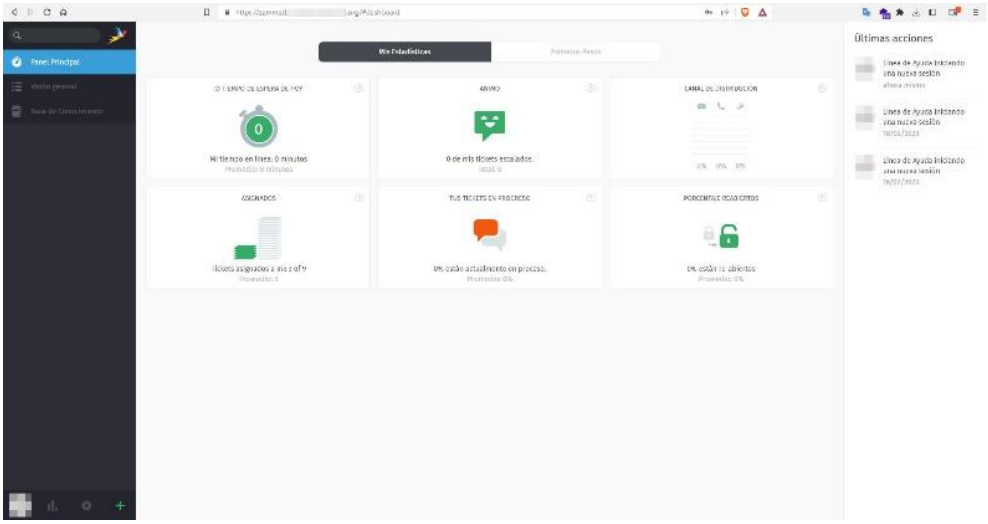
Gráfico 8. Plataforma eclips GreenHost VPS para gestión de tickets



Fuente: captura de pantalla plataforma Eclips organización participante

Se instala la herramienta de gestión de tickets Zammad en el VPS de GreenHost bajo la IP: 37.218.xxx.xxx y se configura los dns para apuntar al subdominio de la organización: https://zammad.xxxxxx.org

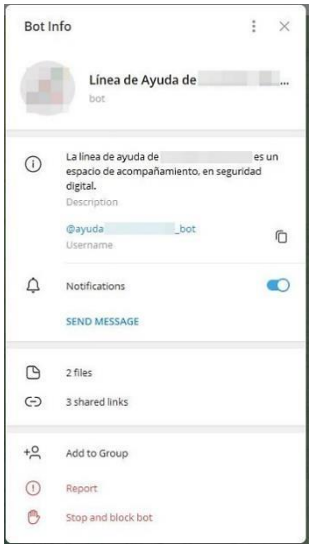
Gráfico 9. Bashboard plataforma Zammad intalada en el VPS



Fuente: captura de pantalla plataforma Zammad

Se configura un canal de recepción de casos mediante la creación de un bot de telegram que al momento se mantiene activo en: https://t.me/ayuda----------Ec_bot

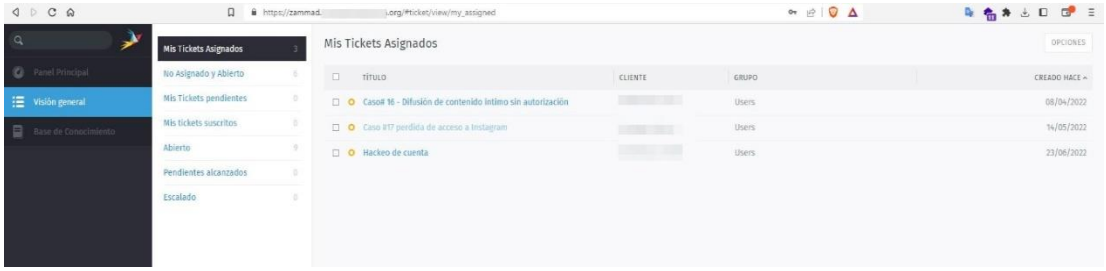
Gráfico 10. Evidencia reunión virtual identificación de necesidades y evaluación



Fuente: captura de pantalla bot Telegram

Hasta el 23 de junio de 2022 se atendieron 3 casos mediante el sistema de gestión de tickets

Gráfico 11. Evidencia atención de casos



Fuente: captura de pantalla zammad

Luego de realizadas todas estas actividades, se puede responder al objetivo específico acerca de la implementación de la guía, estableciendo centros de respuesta a incidentes informáticos en una organización civil, destacando el hecho que el centro de respuesta a incidentes informáticos de la organización donde se implementó aún es funcional y operativo para cualquier persona que quiera acceder a sus servicios.

Además, es importante destacar que la organización ya brindaba acompañamiento en seguridad digital para miembros de la sociedad civil como periodistas, defensores del territorio, ambientalistas y defensores de derechos humanos, pero el proceso realizado era bastante empírico y no tenía una estructura organizada de atención, tampoco contaban con un plan de operativo ni herramientas tecnológicas para gestionar la atención de los incidentes.

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

Al finalizar la construcción de la guía, que tuvo el fin de implementar un centro de respuesta a incidentes informáticos para la sociedad civil, se procede a la validación de esta con el fin de obtener los resultados de la investigación.

La guía contiene los elementos básicos a tomar en cuenta para implementar un CSIRT para la sociedad civil, además se presentan recomendaciones de varias herramientas para mejorar los procesos de atención de incidentes, documentación de auditorías y medir el nivel de madurez del equipo de respuesta.

3.1. Evaluación de la guía

La evaluación de la guía se realizó por parte de 2 expertos en seguridad digital que han brindado acompañamiento a organizaciones de la sociedad civil durante varios años. Para poder recopilar sus comentarios, sugerencias y valoración de esta se generó un cuestionario en línea utilizando la herramienta LimeSurvey.

Gráfico 12. Encuesta en línea Lime Survey

Fuente: elaboración propia

Perfil del experto 1:
Nombre: David Aragort
País: Venezuela

Entrenador en seguridad digital de periodistas, defensores de DDHH, activistas sociales y dirigentes políticos. Más de 4 años de experiencia en comunicaciones digitales.

Actualmente, trabaja como entrenador de seguridad digital y encargado de las comunicaciones en Redes Ayuda, una Organización No Gubernamental (ONG) que trabaja en pro de defender los derechos humanos en Venezuela.

El instrumento utilizado para la valoración por parte del experto fue un cuestionario compuesto por 16 preguntas, a continuación se detallan las respuestas obtenidas:

Gráfico 13. Datos básicos del experto

[P1] Nombre	David Aragort
[P2] Organización	RedesAyuda
[P3] Correo de contacto	david@aragort.com
[P4] Años de experiencia brindando acompañamiento en seguridad digital a la sociedad civil	3

Fuente: elaboración propia

Gráfico 14. Validación por expertos pregunta 5 a 9

[P5] Considera que los objetivos clave para un CSIRT orientado a la sociedad civil planteados en la guía son oportunos	Si [A1]
[P5_comment] Considera que los objetivos clave para un CSIRT orientado a la sociedad civil planteados en la guía son oportunos (Comentario)	Creo que la personalización de la atención es clave, pues si bien muchas veces las organizaciones de la sociedad civil (OSC) se enfrentan a problemas similares, existen muchos otros que dependen del contexto y también otros actores: gobiernos, empresas privadas, grupos delictivos, etc. Por otro lado, dentro de los objetivos también se aborda el factor preventivo que es clave, pues muchas veces los incidentes se pueden prevenir con formación y entendimiento de los fundamentos básicos de seguridad.
[P6] El capítulo 1 de la guía: Conceptos clave permiten al lector comprender los conceptos básicos de un CSIRT para la sociedad civil	Si [A1]
[P6_comment] El capítulo 1 de la guía: Conceptos clave permiten al lector comprender los conceptos básicos de un CSIRT para la sociedad civil (Comentario)	Sí, además al ser un capítulo introductorio, resume muy bien en 2 páginas los conceptos fundamentales para comenzar la lectura de la guía.
[P7] Se comprende cuales son los elementos clave para la creación de un CSIRT de la sociedad civil.	Si [A1]
[P7_comment] Se comprende cuales son los elementos clave para la creación de un CSIRT de la sociedad civil. (Comentario)	
[P8] ¿Utilizaría el Anexo para la construcción del marco de trabajo del CSIRT en su organización para documentar los elementos clave?	Si [A1]
[P8_comment] ¿Utilizaría el Anexo para la construcción del marco de trabajo del CSIRT en su organización para documentar los elementos clave? (Comentario)	
[P9] Dentro de su organización podría aplicar un protocolo de atención de casos parecido al sugerido en la guía	Si [A1]
[P9_comment] Dentro de su organización podría aplicar un protocolo de atención de casos parecido al sugerido en la guía (Comentario)	

Fuente: elaboración propia

Gráfico 15. Validación por expertos pregunta 10 a 15

[P10] Conocía las herramientas tecnológicas presentadas en la guía	Si [A1]
[P10_comment] Conocía las herramientas tecnológicas presentadas en la guía (Comentario)	Aunque también encontré algunos recursos, muy valiosos a mi parecer, que desconocía. Por ejemplo: la herramienta SIM3 Check
[P11] ¿Utilizaría la herramienta sugerida en la guía para la gestión de tickets de los casos atendidos?	Si [A1]
[P11_comment] ¿Utilizaría la herramienta sugerida en la guía para la gestión de tickets de los casos atendidos? (Comentario)	Sin embargo, el seguimiento de los casos que se deriven a otros equipos externos (por ejemplo, la línea de ayuda de Access Now) puede complicar un poco el seguimiento de los tickets ya que muchas veces en esos casos el usuario se entera de que la situación fue resuelta antes que la misma organización que lo derivó.
[P12] Utilizaría la herramienta rawrr para las auditorias	Si [A1]
[P12_comment] Utilizaría la herramienta rawrr para las auditorias (Comentario)	Creo que sería útil hacer mención a la metodología SAFETAG ya que sobre ella se fundamenta RAWRR.
[P13] ¿Considera que son útiles los recursos presentados en la guía para mejorar el acompañamiento en seguridad digital?	Si [A1]
[P13_comment] ¿Considera que son útiles los recursos presentados en la guía para mejorar el acompañamiento en seguridad digital? (Comentario)	
[P14] Le parece importante que la guía incluya un modelo para medir la madurez del CSIRT de la sociedad civil	Si [A1]
[P14_comment] Le parece importante que la guía incluya un modelo para medir la madurez del CSIRT de la sociedad civil (Comentario)	
[P15_SQ001] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Diseño)	3
[P15_SQ002] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Contenido)	4
[P15_SQ003] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Herramientas sugeridas)	5
[P15_SQ004] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Extensión)	5

Fuente: elaboración propia

Gráfico 16. Validación por expertos pregunta 16

[P16] Comentarios finales, sugerencias y recomendaciones.	Muy buen recurso, sería genial poder tener también una versión más condensada y en formato horizontal para presentar en formato de taller ante organizaciones que estén interesadas en crear un CSIRT para sus propias comunidades.

Fuente: elaboración propia

Perfil del experto 2:

Nombre: Carmen Aguilar

País: Ecuador

Entrenadora de seguridad digital, Magister en Tecnología Educativa, brinda acompañamiento a las organizaciones de la sociedad civil en temas de seguridad digital por medio de consultorías, su formación con énfasis en educación y tecnología le ha permitido realizar procesos eficientes de alfabetización digital.

El instrumento utilizado para la valoración por parte del experto fue un cuestionario compuesto por 16 preguntas, a continuación se detallan las respuestas obtenidas:

Gráfico 17. Datos básicos del experto

[P1] Nombre	CARMEN AGUILAR
[P2] Organización	Independiente
[P3] Correo de contacto	carmen2019aguilar@gmail.com
[P4] Años de experiencia brindando acompañamiento en seguridad digital a la sociedad civil	2

Fuente: elaboración propia

Gráfico 18. Validación por expertos pregunta 5 a 9

[P5] Considera que los objetivos clave para un CSIRT orientado a la sociedad civil planteados en la guía son oportunos	Si [A1]
[P5_comment] Considera que los objetivos clave para un CSIRT orientado a la sociedad civil planteados en la guía son oportunos (Comentario)	Los objetivos presentados están acorde a las actividades cotidianas de acompañamiento en seguridad digital.
[P6] El capítulo 1 de la guía: Conceptos clave permiten al lector comprender los conceptos básicos de un CSIRT para la sociedad civil	Si [A1]
[P6_comment] El capítulo 1 de la guía: Conceptos clave permiten al lector comprender los conceptos básicos de un CSIRT para la sociedad civil (Comentario)	Si pues para personas con poco conocimiento le dan un panorama inicial con información básica.
[P7] Se comprende cuales son los elementos clave para la creación de un CSIRT de la sociedad civil.	Si [A1]
[P7_comment] Se comprende cuales son los elementos clave para la creación de un CSIRT de la sociedad civil. (Comentario)	Los elementos son concisos y detallados
[P8] ¿Utilizaría el Anexo para la construcción del marco de trabajo del CSIRT en su organización para documentar los elementos clave?	Si [A1]
[P8_comment] ¿Utilizaría el Anexo para la construcción del marco de trabajo del CSIRT en su organización para documentar los elementos clave? (Comentario)	Claro porque es una ayuda para facilitar el proceso de creación del Marco de trabajo
[P9] Dentro de su organización podría aplicar un protocolo de atención de casos parecido al sugerido en la guía	Si [A1]
[P9_comment] Dentro de su organización podría aplicar un protocolo de atención de casos parecido al sugerido en la guía (Comentario)	Si aunque se debería adaptar a mi necesidad puntual pues brindo apoyo de forma independiente.

Fuente: elaboración propia

Gráfico 19. Validación por expertos pregunta 10 a 15

[P10_comment] Conocía las herramientas tecnológicas presentadas en la guía (Comentario)	No conocía las herramientas
[P11] ¿Utilizaría la herramienta sugerida en la guía para la gestión de tickets de los casos atendidos?	Si [A1]
[P11_comment] ¿Utilizaría la herramienta sugerida en la guía para la gestión de tickets de los casos atendidos? (Comentario)	Si porque me permitiría mejorar la atención brindada y posteriormente tener datos estadísticos para medir el impacto.
[P12] Utilizaría la herramienta rawrr para las auditorias	Si [A1]
[P12_comment] Utilizaría la herramienta rawrr para las auditorias (Comentario)	La he utilizado antes para documentar una auditoría.
[P13] ¿Considera que son útiles los recursos presentados en la guía para mejorar el acompañamiento en seguridad digital?	Si [A1]
[P13_comment] ¿Considera que son útiles los recursos presentados en la guía para mejorar el acompañamiento en seguridad digital? (Comentario)	Si son útiles
[P14] Le parece importante que la guía incluya un modelo para medir la madurez del CSIRT de la sociedad civil	Si [A1]
[P14_comment] Le parece importante que la guía incluya un modelo para medir la madurez del CSIRT de la sociedad civil (Comentario)	Si pues la evaluación de la madurez de un CSIRT es algo que en la mayoría de ocasiones se deja de lado.
[P15_SQ001] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Diseño)	4
[P15_SQ002] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Contenido)	5
[P15_SQ003] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Herramientas sugeridas)	5
[P15_SQ004] Como valoraría en forma general la guía, tomando en cuenta que 1 es la calificación mas baja y 5 la más alta. (Extensión)	5

Fuente: elaboración propia

Gráfico 20. Validación por expertos pregunta 16

[P16] Comentarios finales, sugerencias y recomendaciones.	Fomentar este tipo actividades a nivel nacional, difundir la guía cuando esté lista.

Fuente: elaboración propia

3.2. Análisis de la valoración del experto

Luego de revisar la valoración realizada por los expertos a la guía se puede observar que en general le asigna una calificación promedio de 4.25/5 en el caso del primer experto y un promedio de 4,75/5 el segundo experto, también muestra concordancia entre los contenidos y la aplicación de la guía en un ambiente real.

Algo muy importante a destacar son los comentarios finales donde los expertos indican que es un muy buen recurso y que aplicaría varias de las herramientas y recomendaciones dadas por el autor en las organizaciones donde trabajan, además el tema de la difusión de la guía y conocer herramientas nuevas para mejorar su trabajo es bien valorado.

3.3. Resultados de la investigación

Luego de desarrollar el proyecto de investigación en el cual se construyó la guía basada en la metodología de investigación y acción participativa en colaboración con una organización de la sociedad civil y validar la guía con un experto, se puede dar respuesta a las preguntas de investigación planteadas en la fase de planificación.

Pregunta de investigación 1: ¿Existen estudios para la implementación de centros de respuesta a incidentes informáticos para la sociedad civil?

Luego de realizar una revisión bibliográfica se constata que **NO** existen estudios para implementar centros de respuesta a incidentes informáticos para la sociedad civil, pues toda la documentación para implementar un CSIRT está orientada al trabajo en empresas, organizaciones, gobiernos, etc.

Lo más cercado que se pudo encontrar fue una guía construida por el colectivo “La Libre de Ecuador denominado Defensa Digital para Organizaciones Sociales”, esta guía documenta consejos y buenas prácticas para que las organizaciones sociales puedan realizar sus actividades con mayor seguridad en internet, pero no está orientada específicamente a la creación de un CSIRT.

Pregunta de investigación 2: ¿Cuáles son los procedimientos más adecuados que debe implementar un centro de respuesta a incidentes informáticos para la sociedad civil ecuatoriana?

En primera instancia, para la implementación de un CSIRT para la sociedad civil es fundamental identificar cuál será el público objetivo al que se brindará los servicios del CSIRT, pues al ser el sector de la sociedad civil tan amplio es fundamental definir un grupo más pequeño de beneficiarios.

Posteriormente, se centra en el equipo de profesionales que brindarán los servicios en el CSIRT, estas personas deberán tener conocimientos en seguridad digital para responder a los incidentes reportados, pero además deberán trabajar bastante en el tema preventivo.

Por último, es importante documentar los procesos y evaluar constantemente la madurez del CSIRT para mejorar los procesos poco a poco.

Pregunta de investigación 3: ¿Con la aplicación de una guía para establecer un centro de respuesta a incidentes informáticos para la sociedad civil se mejora la prevención y atención de incidentes informáticos de un grupo de la sociedad civil ecuatoriana?

Luego de haber construido la guía y haberla probado en una organización de la sociedad civil, se puede observar que varios de los procesos de prevención y atención de incidentes informáticos mejoraron, pues se organizaron algunos métodos que anteriormente no estaban claros, también se implementó una herramienta digital para la gestión de tickets lo que ayudó considerablemente en los procesos de atención de casos, optimizando los tiempos de respuesta y el seguimiento de cada caso reportado, también se mejoraron los procesos de escalamiento a organizaciones externas, pues se definió un protocolo de atención de casos más claro.

CONCLUSIONES

- La revisión de información realizada en el estado del arte permitió evidenciar los conceptos fundamentales del manejo y respuesta a incidentes de ciberseguridad, tomando en cuenta las particularidades de la sociedad civil y la ayuda que se puede brindar, tal y como constan en los objetivos posteriores.

- Las entrevistas a diferentes organizaciones de Latinoamérica permitieron obtener información de contexto sobre el trabajo realizado y la importancia de la defensa de los derechos digitales y el acompañamiento en la gestión de incidentes para la sociedad civil.

- El proceso de construcción de la guía fue bastante práctico, involucrando una organización de la sociedad civil que ya ha venido trabajando en acompañar a esta en temas relacionados con su seguridad digital, logrando su concientización y permitiendo que la guía sea funcional. Cabe recalcar el hecho que cualquier persona pueda acceder a ella.

- Los procesos aplicados a la creación de un CSIRT tradicional pueden ser replicados para organizaciones de la sociedad civil, tomando en cuenta los elementos particulares de cada organización y el público objetivo al que se brindará acompañamiento en seguridad digital.

RECOMENDACIONES

- Analizar detenidamente las necesidades de atención de incidentes informáticos del público objetivo al que se brindará servicios con un CSIRT de la sociedad civil permitirá brindar servicios diferenciados.

- Se recomienda implementar un sistema de gestión de tickets para poder organizar los casos remitidos, logrando optimizar el manejo y respuesta de incidentes de ciberseguridad y el escalado de casos a organizaciones externas.

- Es importante vincularse con comunidades de seguridad digital locales y regionales para poder recibir retroalimentación sobre el trabajo que está realizando el CSIRT de la sociedad civil y además al formar parte de una comunidad de confianza se puede obtener información importante sobre amenazas digitales de primera mano.

- Utilizar la guía para implementar un CSIRT para la sociedad civil como una base que le permita generar sus propios procesos con base en los recursos existentes en cada organización.

BIBLIOGRAFÍA

Access Now guia línea de ayuda. (2019). Recuperado el 15 de 04 de 2022, de https://guides.accessnow.org/self-doxing.html

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 24-40.

Apolinario, J. (2022). Propuesta de creación de Centros de respuesta a incidentes de Seguridad informática como estrategia de Cyberseguridad para medios de pagos digitales (Master's thesis, Universidad de Guayaquil-Facultad de Ciencias Matemáticas y Físicas-Carrera de Ingenierí.

Benavides, E., Fuertes, W., Sanchez, S., & Nuñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología, 13*(1), 97-104.

Bernal, P. (2021). Introducción a la Creación de CSIRT. *Cursos del Grupo Técnico de Seguridad 2021.*

Carnegie Mellon University. (2017). *CSIRT Frequently Asked Questions*. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485652

Chamorro, A., Pupiales, S. & Hidalgo, J. (Enero - Junio de 2022). Equipo de respuesta ante incidentes informáticos para la seguridad de la información (CSIRT-UPEC). Sathiri (18)1, 220-229. https://doi.org/10.32645/13906925.1200

CEDIA. (2020). *Estableciendo un CSIRT - Traducido al español*. https://csirt.cedia.edu.ec/proyectos-csirt/manual-estableciendo-un-csirt-de-thaicert-traducido-al-espanol/

CiviCERT. (2020). *Digital First Aid Kit*. Recuperado el 15 de 03 de 2022, de https://digitalfirstaid.org/es/about/

Dias, R., & Borges, F. (2018). Entrevista. *Polifonia*, 160-170.

ENISA. (2006). *A STEP-BY-STEP APPROACH ON HOW TO SETUP A CSIRT*. https://www.enisa.europa.eu/publications/csirt-setting-up-guide/at_download/fullReport

Espinoza, E. (2020). Reflexiones sobre las estrategias de investigación acción participativa. *Conrado*, 342-349.

Fernández, D., & Martínez, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia.* Thomson Reuters Aranzadi.

FIRST. (2019). *Computer Security Incident Response Team (CSIRT) Services Framework*. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Flórez, j. (2021). Diseño administrativo de un centro de respuesta a incidentes cibernéticos para la empresa Cibersecurity de Colombia LTDA.

Fojón, E., & Sanz, A. (18 de Junio de 2010). *Real Instituto Alcano*. Recuperado el 21 de Noviembre de 2021, de http://biblioteca.ribei.org/id/eprint/1879/1/ARI-102-2010.pdf

Inostra, C., Lara, A., Bernal, P., Pérez, E., Alexandro, Y., Lima, E., & anchez, R. (2020). Experiencias, oportunidades y retos de los CSIRT en los nuevos entornos digitales de las Redes Académicas. *Días Virtuales del grupo técnico de Seguridad*.

LACNIC. (2012). *LACNIC.* Recuperado el 10 de 12 de 2021, de https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

Martínez, G. (2022). LACNIC Implementación de SIM3 para los CSIRT Institucionales.

Mikly Melo, J. C., & Siegert Cerezo, E. (2020). Diseño del CSIRT para la Dirección Nacional de Inteligencia DNI.

Ocampo, H. (2019). Diseño documental de un centro de respuestas e incidentes informáticos-CSIRT. Obtenido de https://repository.unad.edu.co/handle/10596/51484

Ríos, E. (2022). Desarrollo de un sistema web prototipo para generar y gestionar documentos necesarios en el proceso de creación de CSIRT académicos.

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRT s and global cybersecurity: How technical experts support science diplomacy. *Global policy, 9*, 60-66. doi:https://doi.org/10.1111/1758-5899.12625

Torres, A., & García, A. (2020). Organizaciones Culturales de la Sociedad Civil: Modelos de gestión cultural y administrativa. *Estudios sobre las culturas contemporáneas*(50), 49-74.

Totem Project. (2022). *Totem Project*. Recuperado el 15 de 04 de 2022, de https://totem-project.org/

Unión Internacional de Telecomunicaciones. (2019). *UIT Academy.* Recuperado el 21 de Noviembre de 2021, de https://academy.itu.int/training-courses/full-catalogue/manejo-y-respuesta-incidentes-de-ciberseguridad

Universidad de Jaen. (2018). *Estudios transversales o de corte*. http://www.ujaen.es/investiga/tics_tfg/estu_transversales.html

ANEXOS

Anexo 1. Cuestionario para entrevistas a organizaciones

Introducción: El presente cuestionario tiene como fin conocer la manera en que su organización brindar un acompañamiento a la sociedad civil. Los resultados obtenidos dentro de este cuestionario serán confidenciales puesto que tendrán fines educativos.

Agradecemos su contestación a las preguntas puesto que aportaran significativamente a este trabajo de graduación.

Objetivo: Conocer las mejores prácticas para brindar acompañamiento en seguridad digital a la sociedad civil.

Instrucciones: Por favor responder las siguientes preguntas planteadas de acuerdo a su criterio.

Fecha:_____

Organización:_____

- ¿Cómo nace la organización?
- ¿Cuál es su misión?
- ¿Qué tipo de acciones han desarrollado en este último año durante la pandemia?
- Creen que los activistas y organizaciones de la sociedad civil necesitan acompañamiento en seguridad digital
- Como receptan los casos para brindar apoyo, en caso de que lo hagan.
- ¿Qué formación tiene el equipo que brinda acompañamiento?

- Cuando brindan talleres de seguridad digital ¿cuáles son los temas más demandados?
- ¿Qué tipo de ataques informáticos son los más comunes?
- ¿Considera necesario que existan más organizaciones que brindan acompañamiento en seguridad digital?
- ¿Cuáles han sido los retos más grandes durante la ejecución de sus actividades?
- ¿Qué tipo de activistas u organizaciones son las que necesitan más apoyo o reciben más ataques informáticos?
- ¿Qué tipo de servicios brindan con su organización?, ¿Estos servicios tienen algún costo?
- ¿Cuáles son sus principales fuentes de financiamiento?

Gracias por su participación

Anexo 2. Cuestionario para evaluar el nivel de preparación y capacidad del equipo participante en la implementación de la guía.

Introducción: El presente cuestionario tiene como fin identificar las capacidades del equipo previo a la implementación de la guía, las preguntas se realizan de forma virtual en un conversatorio con la organización y se clasifican en 4 áreas.

Objetivo: Conocer los procesos y recursos clave utilizados por el equipo de respuesta a incidentes, además de sus capacidades técnicas.

Área 1: Estructura y organización del equipo

1. ¿Existe un organigrama definido que muestre la estructura y roles del equipo de CSIRT?
2. ¿El equipo cuenta con un líder claramente designado y con autoridad para tomar decisiones?
3. ¿Hay un plan de sucesión para asegurar la continuidad del equipo en caso de cambios en el personal clave?
4. ¿Existe un proceso documentado para la gestión de incidentes, incluyendo la recepción, clasificación, investigación y resolución de los mismos?
5. ¿Se han definido las responsabilidades y los niveles de autoridad para cada miembro del equipo?

Área 2: Recursos y capacidades técnicas

1. ¿El equipo cuenta con los recursos técnicos necesarios, como hardware, software y herramientas de seguridad?
2. ¿Se mantiene actualizado un inventario de los recursos técnicos y se realizan regularmente las actualizaciones y mejoras necesarias?
3. ¿El equipo tiene acceso a la información y las fuentes de inteligencia de seguridad necesarias para detectar y responder a incidentes?
4. ¿Se lleva a cabo un monitoreo constante de los sistemas de información y se registran los eventos relevantes?
5. ¿Se realizan pruebas periódicas de los mecanismos de detección y respuesta para asegurar su eficacia?

Área 3: Capacidades de gestión de incidentes

1. ¿Se ha establecido un plan de gestión de incidentes que incluya los procedimientos y protocolos a seguir en caso de incidentes de seguridad?
2. ¿El equipo ha participado en ejercicios y simulaciones de incidentes para practicar y mejorar sus capacidades de respuesta?
3. ¿Existe un proceso claro para la comunicación interna y externa durante la gestión de incidentes?
4. ¿Se lleva a cabo una revisión post-incidente después de cada incidente importante para identificar lecciones aprendidas y áreas de mejora?
5. ¿El equipo mantiene registros adecuados de los incidentes gestionados, incluyendo información relevante sobre la respuesta y las medidas tomadas?

Área 4: Colaboración y coordinación

1. ¿El equipo tiene establecidos canales de comunicación y colaboración con otros equipos y entidades relevantes, tanto internas como externas?
2. ¿Se participa activamente en la comunidad de seguridad informática y se comparten experiencias y conocimientos con otros expertos?
3. ¿Se realizan actividades de capacitación y formación para mantener actualizadas las habilidades y conocimientos del equipo?
4. ¿El equipo realiza revisiones regulares de su desempeño y busca oportunidades para mejorar sus procesos y habilidades?
5. ¿Se promueve una cultura de aprendizaje y mejora continua dentro del equipo?

Anexo 3. Plan estratégico y operativo desarrollado con la organización participante

PLAN ESTRATÉGICO DEL CSIRT ---------:

Visión:

La visión es ser reconocidos como líderes en la respuesta efectiva a incidentes informáticos orientados a la sociedad civil y garantizar la seguridad de la organización. Nos esforzamos por mantener un entorno digital seguro, protegiendo los activos y la información crítica de la organización, así como brindar confianza y tranquilidad a él usuarios internos y externos.

Nos fundamentamos en proteger los derechos digitales de las personas comunes con énfasis en periodistas, activistas, defensores de derechos humanos y personas en riesgo.

Objetivos estratégicos:

- Proteger los derechos digitales de los ciudadanos a través de la respuesta efectiva a incidentes de seguridad cibernética.
- Sensibilizar y educar a la sociedad civil sobre las mejores prácticas de seguridad digital.
- Colaborar con organizaciones y actores relevantes para fortalecer la seguridad cibernética en la sociedad civil

Análisis del entorno:

Aspectos	Descripción
Amenazas	- Aumento de ataques cibernéticos dirigidos a la sociedad civil.

	- Difusión de información falsa y desinformación en línea. - Exposición de datos personales y violación de la privacidad.
Riesgos	- Pérdida de confianza y reputación de las organizaciones de la sociedad civil debido a brechas de seguridad. - Impacto en la libertad de expresión y derechos digitales de los ciudadanos. - Potencial de censura y control del acceso a la información en línea.
Desafíos	- Falta de conciencia y capacitación en seguridad cibernética en la sociedad civil. - Escasez de recursos y financiamiento para implementar medidas de seguridad adecuadas. - Necesidad de establecer colaboraciones y alianzas para fortalecer la respuesta a incidentes cibernéticos.
Regulaciones	- Marco legal y normativo en desarrollo para la protección de datos personales y seguridad cibernética. - Necesidad de promover políticas y regulaciones que protejan los derechos digitales de la sociedad civil. - Coordinación entre diferentes entidades gubernamentales y organizaciones de la sociedad civil en materia de ciberseguridad.
Recursos	- Disponibilidad limitada de expertos en ciberseguridad especializados en la sociedad civil. - Necesidad de fortalecer la infraestructura tecnológica para garantizar la seguridad de las organizaciones y ciudadanos. - Acceso limitado a programas de capacitación y recursos para mejorar la seguridad cibernética.

Evaluación de recursos y capacidades:

La organización sin fines de lucro de la sociedad civil se encuentra en un entorno desafiante en términos de ciberseguridad. Con un equipo de 7 personas, de las cuales 3 son técnicos con conocimientos en ciberseguridad y los demás poseen perfiles en ciencias sociales, la organización se enfrenta a amenazas y riesgos constantes en el ámbito digital.

Entre las amenazas identificadas se encuentran el aumento de ataques cibernéticos dirigidos específicamente a organizaciones de la sociedad civil, la difusión de información falsa y desinformación en línea, así como la exposición de datos personales y violaciones de privacidad.

Estos riesgos pueden tener consecuencias significativas, como la pérdida de confianza y reputación de la organización, el impacto en la libertad de expresión y los derechos digitales de los ciudadanos, y la posibilidad de censura y control del acceso a la información en línea.

La falta de conciencia y capacitación en seguridad cibernética es uno de los desafíos principales que enfrenta la organización. Además, la escasez de recursos y financiamiento limita la capacidad de implementar medidas de seguridad adecuadas. En este contexto, es fundamental establecer colaboraciones y alianzas con otras organizaciones y entidades para fortalecer la respuesta a incidentes cibernéticos.

En términos de recursos, aunque la organización cuenta con computadoras portátiles, escritorios y servidores para implementar herramientas, se reconoce la necesidad de contar con expertos en ciberseguridad especializados y fortalecer la infraestructura tecnológica para garantizar la seguridad de las organizaciones y los ciudadanos. También se requiere acceso a programas de capacitación y recursos que permitan mejorar la seguridad cibernética de manera continua.

Estrategias y acciones:

- Crear un equipo dedicado exclusivamente a la gestión y respuesta de incidentes de seguridad informática dentro de la organización. Designar roles y responsabilidades claras para los miembros del equipo.

- Desarrollar y mejorar las políticas y procedimientos: Establecer políticas claras de seguridad de la información y procedimientos para la gestión de incidentes. Definir los pasos a seguir en caso de un incidente de seguridad y cómo se reportarán y documentarán los eventos.
- Implementar medidas de seguridad técnicas: Configurar y mantener soluciones de seguridad, como firewalls, sistemas de detección de intrusiones, sistemas de prevención de pérdida de datos y antivirus, para proteger la infraestructura tecnológica de la organización.
- Capacitación y concientización en ciberseguridad: Brindar formación y sesiones de concientización sobre las mejores prácticas de seguridad informática a todo el personal de la organización.
- Establecer colaboraciones y alianzas externas: Establecer relaciones de trabajo con otros CSIRT, organizaciones de la sociedad civil y entidades gubernamentales relacionadas con la seguridad informática.
- Realizar evaluaciones de riesgos regulares: Realizar evaluaciones periódicas de riesgos de seguridad informática para identificar posibles vulnerabilidades y amenazas.
- Mantenerse actualizado sobre las últimas amenazas y tendencias en ciberseguridad: Seguir de cerca los desarrollos en el campo de la seguridad informática, participar en comunidades y foros especializados, y mantenerse actualizado sobre las últimas amenazas y tendencias en ciberseguridad.

Medición y seguimiento:

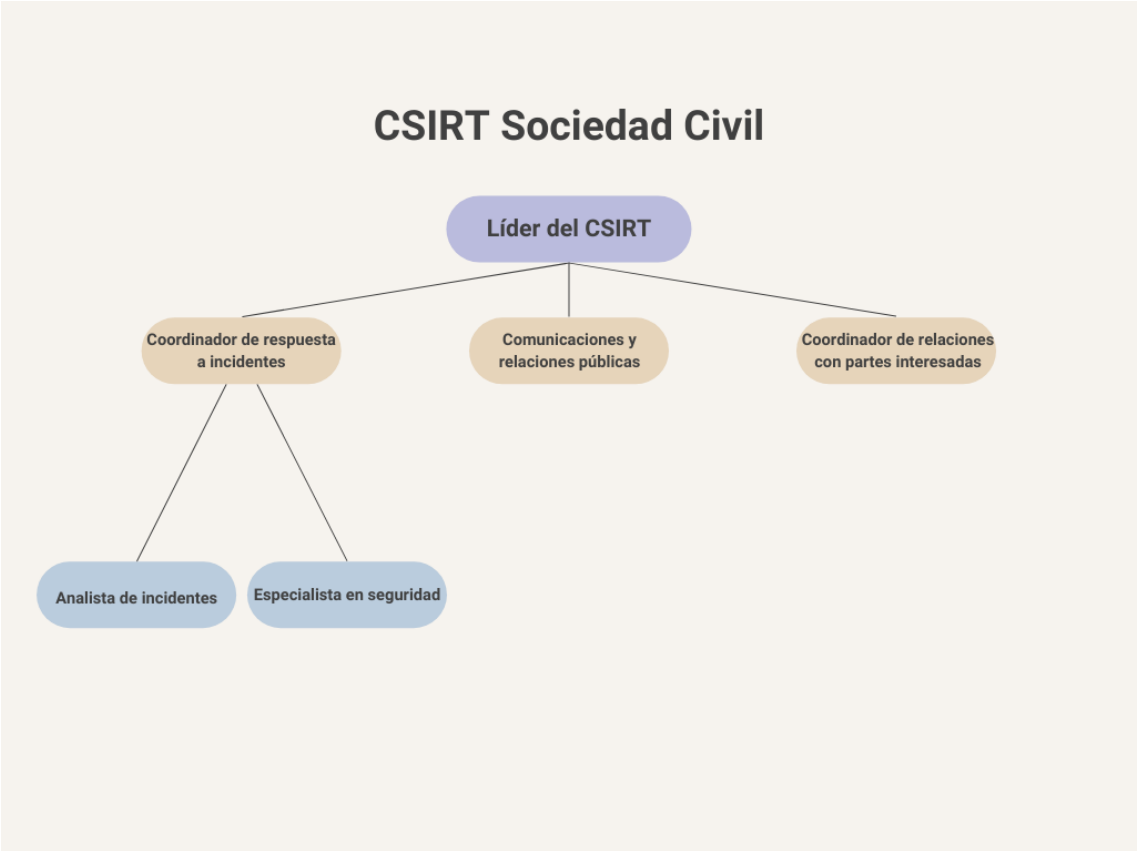
Métricas del CSIRT

- Tiempo promedio de respuesta
- Número de incidentes resueltos
- Porcentaje de satisfacción del cliente
- Tiempo promedio de resolución de incidentes
- Porcentaje de incidentes escalados correctamente

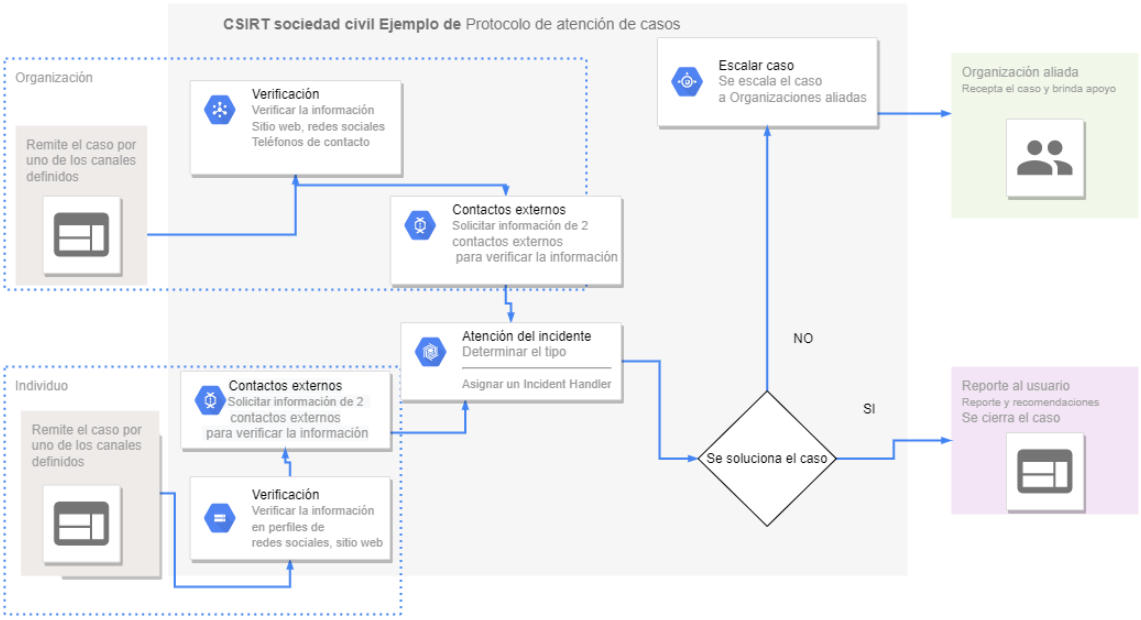
- ❖ Porcentaje de incidentes repetidos
- ❖ Porcentaje de pérdida de datos durante la respuesta
- ❖ Número de incidentes sin documentación
- ❖ Porcentaje de incidentes mal clasificados
- ❖ Tiempo promedio de comunicación con las partes interesadas

PLAN OPERATIVO DEL CSIRT:

Estructura organizativa y roles:



Procesos de gestión de incidentes:



Recopilación y análisis de información:

La recopilación y análisis de información son elementos fundamentales en el funcionamiento de un CSIRT (Equipo de Respuesta a Incidentes de Seguridad Informática) orientados a la sociedad civil. Esta actividad se centra en recabar y examinar datos relevantes relacionados con la seguridad informática, con el objetivo de detectar amenazas, identificar patrones y tomar decisiones informadas para proteger a la comunidad y responder eficazmente a los incidentes.

El CSIRT de la sociedad civil implementará estrategias y acciones específicas para llevar a cabo la recopilación y análisis de información de manera efectiva. A continuación, se describen algunas de ellas:

- **Monitoreo de fuentes de información:** El CSIRT se mantendrá al tanto de las fuentes de información relevantes en el ámbito de la seguridad informática para recopilar datos actualizados sobre amenazas, vulnerabilidades y tendencias. Estas fuentes pueden incluir informes de

organizaciones de ciberseguridad, boletines de alerta, grupos de discusión y redes de intercambio de información.

- **Análisis de incidentes:** El CSIRT realizará un análisis exhaustivo de los incidentes de seguridad reportados o detectados. Esto implica recopilar información detallada sobre el incidente, como la naturaleza del ataque, los sistemas afectados y los posibles vectores de ataque. Mediante el análisis de incidentes, el CSIRT podrá identificar patrones comunes, técnicas de ataque y posibles medidas de mitigación.
- **Intercambio de información y colaboración:** El CSIRT buscará establecer alianzas y colaboraciones con otros CSIRT, organizaciones de la sociedad civil y entidades gubernamentales que compartan intereses comunes en materia de seguridad informática. El intercambio de información permitirá obtener conocimientos adicionales, compartir buenas prácticas y colaborar en la respuesta conjunta a incidentes de seguridad.
- **Análisis de tendencias y riesgos:** El CSIRT realizará análisis periódicos de tendencias y riesgos en el ámbito de la seguridad informática. Esto implica evaluar las amenazas emergentes, las vulnerabilidades conocidas y las prácticas recomendadas en la comunidad de la sociedad civil. Con base en este análisis, el CSIRT podrá anticipar posibles riesgos y desarrollar estrategias proactivas para mitigarlos.
- **Uso de herramientas de análisis:** El CSIRT empleará herramientas y tecnologías especializadas para facilitar el análisis de información. Esto incluye sistemas de gestión de incidentes, herramientas de correlación de eventos, soluciones de análisis de logs y software de inteligencia de amenazas. Estas herramientas permitirán procesar grandes volúmenes de datos y extraer información relevante para la toma de decisiones.
- La recopilación y análisis de información en el CSIRT de la sociedad civil fortalecerá su capacidad para proteger a la comunidad, identificar posibles amenazas y colaborar en la mejora continua de la seguridad informática en el ámbito civil.

Comunicación y coordinación:

Canales de comunicación	Información
Correo electrónico para reportar incidentes	ayuda@-------.org
Teléfono	098------50
Bot de telegram	https://t.me/ayuda------Ec_bot

Capacidad de respuesta y recuperación:

Lista de recursos externos para escalar casos:

- Línea de ayuda de Access Now: help@accessnow.org

ANEXO 4 GUÍA

GUÍA PARA IMPLEMENTAR UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL


VPN

TABLA DE CONTENIDOS

Agradecimientos

Esta guía fue escrita por Luis Fernando Arias, Facilitador de Tecnologías de la Información y Comunicación para el Desarrollo y Seguridad Digital de Ecuador.

La Guía fue probada en el Colectivo Conexión Educativa, un agradecimiento especial a todo el equipo de voluntarios.

Esta guía ha sido creada con base en la revisión bibliográfica de varios manuales para la implementación de CSIRTS y con entrevistas a diferentes organizaciones que brindan acompañamiento en seguridad digital a miembros de la sociedad civil.

Además, me gustaría extender un agradecimiento especial a Access Now organización que ha hecho posible la construcción de esta guía, gracias por la confianza y el apoyo durante todo este tiempo.

Las siguientes son algunas de las personas que se tomaron el tiempo para revisar la guía y brindar comentarios significativos, un agradecimiento especial:

- Mgs. Paul Bernal
- Carmen Aguilar (Ecuador)
- David Aragort (Venezuela)

Sobre esta guía

Esta guía está destinada a cualquier organización o colectivo/a que se interese por brindar respuesta a incidentes informáticos para la sociedad civil, con principal énfasis en personas que brindan acompañamiento en seguridad digital a activistas, defensores de derechos humanos, periodistas y organizaciones sociales de diferentes tipos.

Esta guía fue construida utilizando la metodología investigación acción participativa con profesionales que manejan incidentes informáticos de la sociedad civil con el objetivo de cambiar el enfoque pensado para los centros de respuesta comunes creados por empresas, gobiernos o academias.

Público objetivo:

Esta guía está diseñada para las organizaciones que les interesa conocer el funcionamiento de un centro de respuesta a incidentes informáticos para la sociedad civil e implementar uno propio.

1. CONCEPTOS CLAVE

1.1 ¿QUÉ ES UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL?

"¿Las personas comunes sufren incidentes informáticos?"

"¿Qué personas son más propensas a sufrir un ataque informático?"

"¿Podemos brindar apoyo si alguien pierde acceso a sus cuentas de redes sociales?"

"¿Cómo puedo comunicarme de forma segura con un centro de respuesta a incidentes informáticos para la sociedad civil?"

Estas son algunas de las preguntas que pueden plantearse al iniciar el proceso para crear un centro de respuesta a incidentes informáticos. Esta sección intenta responder a estas cuestiones y definir algunos conceptos clave para implementar centros de respuesta a incidentes informáticos para la sociedad civil. También permite al lector reflexionar sobre los conocimientos básicos sobre un centro de respuesta por medio de:

- Consideraciones importantes para la atención de incidentes a personas comunes
- Delimitación de objetivos prioritarios de un centro de respuesta a incidentes

1.2 ¿CUÁLES SON LOS ELEMENTOS CLAVE PARA LA CREACIÓN DE UN CENTRO DE RESPUESTA A INCIDENTES INFORMÁTICOS PARA LA SOCIEDAD CIVIL?

Un centro de respuesta a incidentes informáticos para la sociedad civil es un servicio que brinda acompañamiento en seguridad digital y que está al alcance de cualquier persona, con énfasis en personas que debido a sus actividades cotidianas están en riesgo, como pueden ser: defensores de derechos humanos, activistas, periodistas, miembros de organizaciones de base, etc.

Los servicios brindados por un CSIRT(por las siglas en inglés de Computer Security Incident Response Team) orientado a la sociedad civil son: Atención de incidentes informáticos brindando respuesta rápida, capacitación en seguridad digital, campañas de prevención, alertas, análisis de vulnerabilidades, auditoría forense, etc.

La filosofía fundamental de un CSIRT de la sociedad civil es brindar un acompañamiento oportuno hacia las personas que desconocen cómo protegerse en internet, debe tener un enfoque preventivo y además reactivo para poder brindar un acompañamiento integral.

Un CSIRT de la sociedad civil debería ser preferiblemente gratuito y estar accesible en cualquier momento, permitiendo así que las personas puedan pedir ayuda en cualquier emergencia, debería brindar la oportunidad de comunicarse con un profesional de la seguridad informática para recibir asistencia sobre un evento o incidente que le esté afectando.

Las personas podrían comunicarse con el centro de respuesta mediante mensajes de texto, redes sociales, correo electrónico o por medio de algún formulario web,

un equipo de profesionales y voluntarios deberá estar listo para asistir a las personas en sus requerimientos.

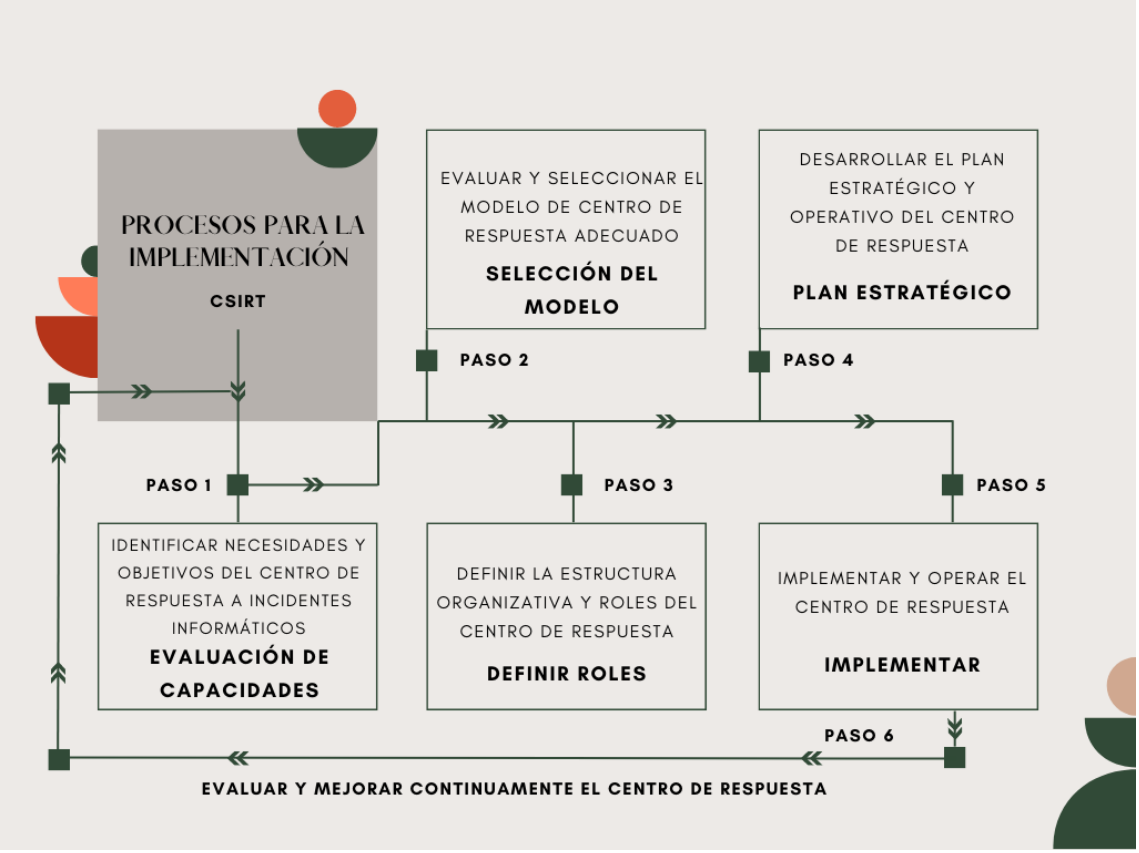
1.3 LOS OBJETIVOS DE UN CSIRT PARA LA SOCIEDAD CIVIL

Los objetivos clave de un CSIRT son:

- Brindar respuesta rápida a incidentes de seguridad digital
- Proveer recomendaciones personalizadas, instrucciones y seguimiento en temas relacionados con seguridad digital
- Realizar análisis de riesgos y creación de políticas de seguridad organizacional, individual y comunitaria.
- Creación de guías y contenidos educativos sobre buenas prácticas y herramientas de seguridad digital.
- Brindar soporte para la protección de infraestructura tecnológica.

1.4. Procesos para implementar un CSIRT

Un proceso claro de las actividades a realizar es fundamental para poder crear un CSIRT para la sociedad civil, estos son los pasos que se deben tomar en cuenta para iniciar:



1.5. Modelo del CSIRT

Existen 4 modelos que se describen en la siguiente tabla:

Modelo	Características
Centralizado	- Todas las funciones y responsabilidades del CSIRT se centralizan en un solo equipo. - El equipo centralizado es responsable de recibir, analizar y responder a los incidentes de seguridad de toda la organización.
Descentralizado	- Se establecen equipos de respuesta a incidentes en diferentes departamentos o unidades de la organización. - Cada equipo es responsable de manejar los incidentes de seguridad en su área específica.
Colaborativo	- Varios equipos de respuesta a incidentes trabajan de manera colaborativa para abordar los incidentes de seguridad. - Los equipos pueden pertenecer a diferentes organizaciones o entidades que comparten recursos y conocimientos para mejorar la respuesta a incidentes.
Híbrido	- Combina elementos de los modelos centralizado y descentralizado. - Puede haber un equipo centralizado que coordine y brinde apoyo a varios equipos descentralizados en diferentes ubicaciones o unidades de negocio.

La organización deberá seleccionar con el equipo el modelo más adecuado, para lo cual se propone utilizar los siguientes parámetros:

- Coordinación: Nivel de coordinación entre los equipos de respuesta a incidentes.

- Distribución de responsabilidades: Distribución de las responsabilidades de manejo de incidentes de seguridad.
- Comunicación: Nivel de comunicación entre los equipos y entidades relevantes.
- Políticas y procedimientos: Tipo de organización de las políticas y procedimientos.
- Recursos compartidos: Nivel de recursos compartidos entre los equipos de respuesta a incidentes.

Comparación de los modelos:

Modelo	Parámetro.1	Parámetro.2	Parámetro.3	Parámetro.4	Parámetro.5
Centralizado	Funciones centralizadas	Responsabilidad global	Comunicación interna	Políticas y procedimientos centralizados	Recursos compartidos
Descentralizado	Equipos por departamento	Responsabilidad específica	Comunicación interna	Políticas y procedimientos descentralizados	Recursos específicos por departamento
Colaborativo	Equipos colaborativos	Colaboración interorganizacional	Comunicación interorganizacional	Políticas y procedimientos colaborativos	Recursos compartidos y conocimientos
Híbrido	Combinación de centralizado y descentralizado	Coordinación y apoyo centralizado	Comunicación interna y descentralizada	Políticas y procedimientos coordinados	Recursos centralizados y descentralizados

2. PLANIFICACIÓN

2.1 PLAN ESTRATÉGICO Y OPERATIVO

La planificación es fundamental para la creación de un CSIRT a continuación se presentan los puntos clave a tomar en cuenta:

MODELO PLAN ESTRATÉGICO DEL CSIRT:

Visión:

Establecer una visión clara y de largo plazo para el CSIRT, en línea con los objetivos de seguridad de la organización.

Objetivos estratégicos:

Identificar los objetivos clave del CSIRT, como mejorar la capacidad de respuesta a incidentes, reducir el tiempo de resolución, fortalecer la postura de seguridad y fomentar la colaboración con otros equipos y organizaciones.

Análisis del entorno:

Evaluar el entorno de seguridad actual, incluyendo las amenazas emergentes, las regulaciones relevantes y las mejores prácticas en respuesta a incidentes.

Evaluación de recursos y capacidades:

Realizar un análisis exhaustivo de los recursos disponibles, incluyendo personal, herramientas, infraestructura y presupuesto.

Identificar las brechas y necesidades de recursos para alcanzar los objetivos estratégicos.

Estrategias y acciones:

Definir estrategias específicas para abordar los desafíos y aprovechar las oportunidades identificadas.

Establecer acciones concretas para mejorar la preparación y capacidad del CSIRT, como la adquisición de herramientas y tecnologías, la formación y capacitación del personal, la mejora de los procesos y la colaboración con otras entidades.

Medición y seguimiento:

Establecer indicadores clave de rendimiento (KPIs) para evaluar el progreso y el cumplimiento de los objetivos estratégicos.

Realizar revisiones periódicas para monitorear y ajustar la estrategia según sea necesario.

PLAN OPERATIVO DEL CSIRT:

Estructura organizativa y roles:

Definir la estructura organizativa del CSIRT, incluyendo los roles y responsabilidades de cada miembro del equipo.

Establecer mecanismos claros de comunicación y coordinación interna.

Procesos de gestión de incidentes:

Establecer un marco de gestión de incidentes que incluya la detección, notificación, análisis, respuesta y recuperación de incidentes de seguridad.

Definir los procedimientos y flujos de trabajo para cada etapa del proceso de gestión de incidentes.

Recopilación y análisis de información:

Establecer mecanismos para recopilar y analizar información sobre incidentes de seguridad, tendencias, patrones y nuevas amenazas.

Utilizar herramientas y técnicas de inteligencia de amenazas para mejorar la detección y respuesta.

Comunicación y coordinación:

Establecer canales de comunicación efectivos con partes interesadas internas y externas, incluyendo equipos de TI, la alta dirección, proveedores de servicios y otros CSIRT.

Coordinar y colaborar con otras organizaciones en respuesta a incidentes.

Capacidad de respuesta y recuperación:

Establecer planes de respuesta a incidentes detallados para diferentes

2.2 PLANIFICACIÓN DEL MARCO DE TRABAJO

La planificación es un proceso fundamental en la implementación de un equipo de respuesta a incidentes informáticos, pues nos permitirá determinar a quienes se brinda acompañamiento, identificar los propios recursos, analizar las debilidades del equipo, determinar los diferentes servicios disponibles y la disponibilidad de estos.

Para ello a continuación se desarrollan cada uno de los elementos necesarios para implementar el marco de trabajo del equipo de respuesta, además en el ***Anexo 1*** encontrará una plantilla para poder desarrollar su propio marco de trabajo.

2.3 MISIÓN: La misión es fundamental en el funcionamiento de un centro CSIRT aquí se explica de forma clara el propósito de este, los objetivos del equipo y como recomendación se debe redactar de forma compacta en unas 2 o 3 oraciones.

Ejemplo Misión de la línea de ayuda de Access Now:

> La Línea de Ayuda de Seguridad Digital de Access Now trabaja con individuos y organizaciones de todo el mundo para mantenerlos seguros en línea, Si usted está en riesgo, podemos ayudarle a mejorar sus prácticas de seguridad digital para mantenerse fuera de peligro. Si ya está bajo ataque, proporcionamos asistencia de emergencia de respuesta rápida.

2.4 GRUPO OBJETIVO O CONSTITUENCY: La comunidad objetivo también se conoce en inglés con el término Constituency es el grupo de individuos que utilizarán los servicios del CSIRT, es fundamental identificar el grupo objetivo al que se le brindará asistencia, pues esto servirá para identificar de forma clara sus necesidades.

Ejemplo grupo objetivo Access Now:

> Somos un recurso gratuito para la sociedad civil en todo el mundo. Ofrecemos asistencia técnica y asesoramiento directo en tiempo real a grupos y activistas de la sociedad civil, organizaciones de medios de comunicación, periodistas y bloggers, y defensores de derechos humanos.

2.5 EQUIPO: El equipo que conforma el CSIRT deberá tener conocimientos técnicos que le permitan abordar los incidentes de forma eficiente. Lo más importante es que si la persona no cuenta con los conocimientos técnicos necesarios esté dispuesto a adquirirlos, algo fundamental también es que todos los miembros del equipo deberán motivarse por las causas sociales de la organización.

Algunos de los perfiles que podrían considerarse dentro del equipo son (Barbosa. 2021):

Dirección de Tecnología: La dirección, con mayor jerarquía y responsabilidad, es la encargada de tomar decisiones que puedan impactar o mejorar las condiciones del CSIRT, también establecen un compromiso total y realizan una planificación estratégica tanto de la operación como de cara a los clientes. y los medios de comunicación, por lo que los procedimientos y actividades del CSIRT deben ser transparentes.

Jefe de operaciones: Supervisa la operación del CSIRT y establece la planificación estratégica, ocupa este puesto, que es el más jerárquico en términos de la operación del CSIRT, es responsable de asegurar que los procesos y actividades del CSIRT, así como el escalamiento de infraestructura crítica e incidentes de seguridad de alto impacto, sean claros para los clientes de la operación.

Coordinador de ciberseguridad: Supervisa un equipo de especialistas, analistas y técnicos de ciberseguridad. También establece la estrategia de planificación y coordinación con miras al funcionamiento del área de ciberseguridad. Es quien toma las decisiones respecto de los incidentes de seguridad de la información internos y externos, así como los relacionados con la informática forense.

Security incident handler: Este perfil es fundamental dentro del equipo de respuesta pues es la persona encargada del manejo de los incidentes y brindar acompañamiento a los individuos u organizaciones que soliciten un servicio.

Indicente Response Coordinator: En caso de que el equipo de respuesta sea grande y se cuente con recursos se podría pensar en un Coordinador del equipo de respuesta, el mismo tendrá un rol de liderazgo en el equipo.

Digital Security Trainer: Es fundamental para las actividades preventivas contar con un entrenador de seguridad digital, pues los procesos de formación deben ser permanentes en la sociedad civil.

2.6 DISPONIBILIDAD: La disponibilidad de los servicios se verá directamente relacionada con el tiempo laboral de los miembros del CSIRT, en algunos casos la mayoría pueden ser voluntarios que brinden apoyo solo en horarios específicos o cuando se cuente con incidentes reportados.

2.7 RELACIONES INTERNAS Y EXTERNAS: Las relaciones internas del equipo de respuesta servirán para fortalecer sus servicios, en algunas ocasiones si la organización es más grande se deberán generar algunas estrategias conjuntas con otros departamentos como, por ejemplo: Comunicación, TI, Proyectos, etc.

En el caso de relaciones externas servirán para escalamiento de casos o para vincularse a espacios de entrenamiento o mejorar las capacidades de la organización, algunas organizaciones externas con las que se podría realizar alianzas estratégicas son:

CiviCert: Es una red de equipos de respuesta a emergencias informáticas (CERT), equipos de respuesta rápida y proveedores de servicios y contenido de Internet independientes que ayudan a la sociedad civil a prevenir y abordar problemas de seguridad digital.

Línea de ayuda de Access Now: La Línea de Ayuda de Seguridad Digital de Access Now trabaja con individuos y organizaciones de todo el mundo para mantenerlos seguros en línea.

2.8 SERVICIOS: Los servicios brindados por un centro de respuesta a incidentes informáticos para la sociedad civil pueden clasificarse en servicios preventivos y reactivos, ahora se destallan los servicios que pueden brindarse.

Servicios preventivos:

- Difusión y capacitación
- Emisión de boletines y alertas

Servicios reactivos

- Auditorías de seguridad digital
- Análisis de vulnerabilidades
- Detección de incidentes
- Análisis forense

Servicios Proactivos

- Mensajes y anuncios.
- Observatorio de tecnología.
- Auditorías o evaluaciones de seguridad.
- Creación de herramientas de seguridad.
- Servicios de detección de intrusos.
- Aplicaciones para el control de listas de configuración seguras para sistemas TIC
- Monitoreo de redes

Todos estos servicios podrán ofertarse con base en los recursos de la organización y su misión, pero el servicio fundamental que no debería faltar será el de atención de incidentes.

2.8 INFRAESTRUCTURA Y HERRAMIENTAS

Las instalaciones del CSIRT y la infraestructura tecnológica son recursos que tienen que garantizar la seguridad de la información manejada y además la seguridad del equipo del CSIRT.

Consideraciones sobre seguridad física: En caso de contar con un espacio físico, la documentación del CSIRT debe almacenarse en un espacio seguro al que no puedan acceder personas no autorizadas.

Se debe mantener un control de acceso a las instalaciones físicas.

Consideraciones sobre equipamiento TI: Se deben implementar mecanismos de comunicación seguros y sistemas endurecidos, incluyendo las computadoras usadas para la atención de casos. Se deberá implementar salas de monitoreo, salas de pruebas y demás especificaciones que integran el CSIRT, entregando un esquema general de la estructura física y gráfica del centro de atención de incidentes. Las salas de los centros de datos deberán contar con sistema de aire acondicionado, sistemas contra incendio, así como todas las medidas de seguridad para el acceso a las mismas únicamente por personal autorizado.

Consideraciones sobre herramientas específicas CSIRT: Dentro de las herramientas específicas se debe tomar en cuenta lo siguiente:

Sistema de gestión de tickets

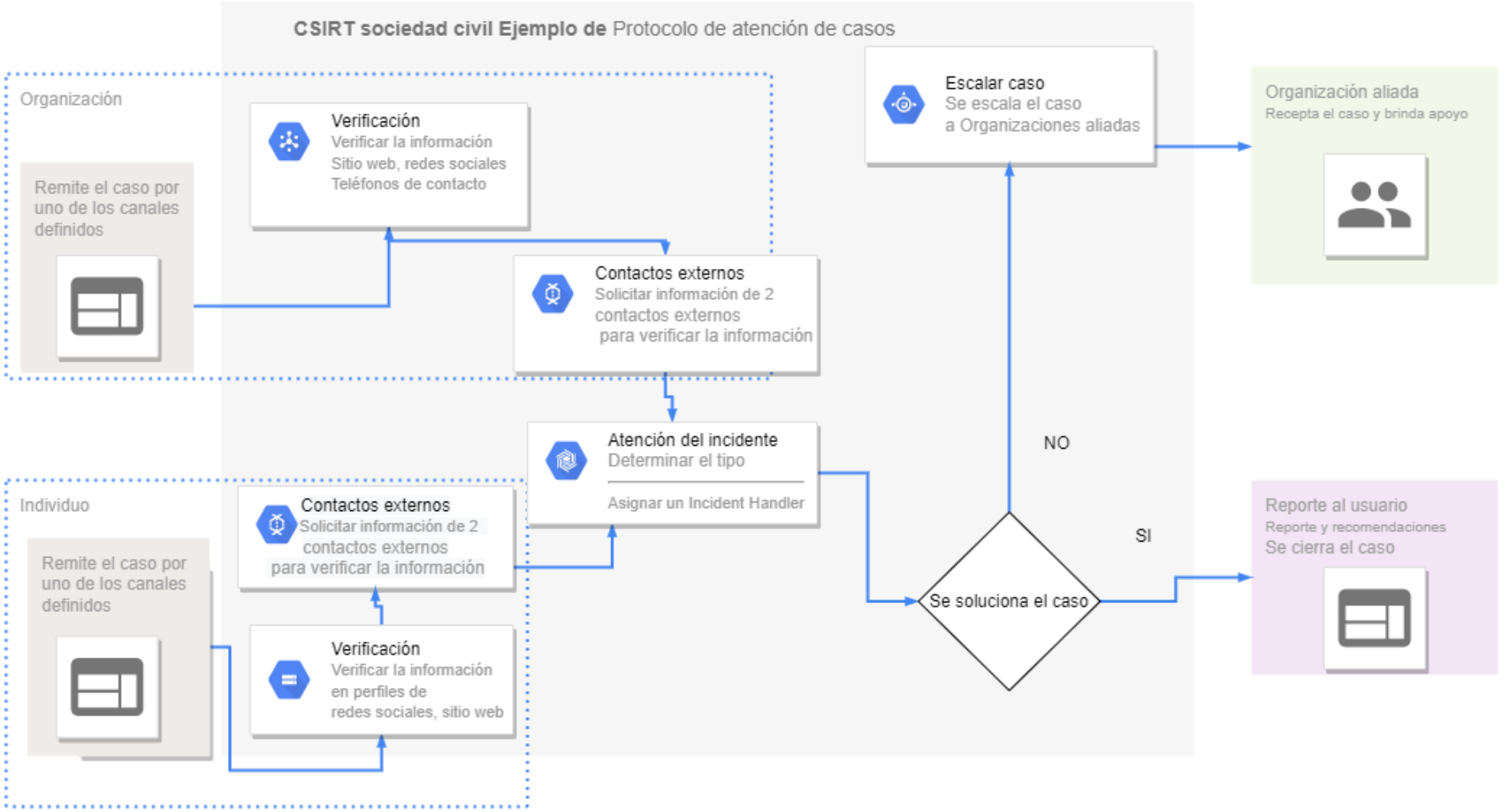
Base de datos de contactos

Herramientas de seguridad digital como software antivirus, firewall, servidores proxy, escáner de vulnerabilidades, sistema de prevención de intrusos.

2.9 **PROTOCOLO DE ATENCIÓN DE CASOS Y VERIFICACIÓN DE IDENTIDAD**:

Mantener un protocolo de atención a casos que nos permita en primera instancia verificar la identidad de las personas es fundamental, además es importante determinar todos los procesos para la atención del incidente, incluyendo el escalado a organizaciones externas que puedan brindar apoyo, a continuación se

presenta un diagrama de ejemplo que podría ser utilizado para la recepción de casos:


CSIRT sociedad civil Ejemplo de Protocolo de atención de casos
Organización
Remite el caso por uno de los canales definidos
Verificación
Verificar la información
Sitio web, redes sociales
Teléfonos de contacto
Contactos externos
Solicitar información de 2 contactos externos para verificar la información
Atención del incidente
Determinar el tipo
Asignar un Incident Handler
Escalar caso
Se escala el caso a Organizaciones aliadas
Organización aliada
Recepta el caso y brinda apoyo
NO
SI
Se soluciona el caso
Reporte al usuario
Reporte y recomendaciones
Se cierra el caso
Individuo
Remite el caso por uno de los canales definidos
Contactos externos
Solicitar información de 2 contactos externos para verificar la información
Verificación
Verificar la información en perfiles de redes sociales, sitio web

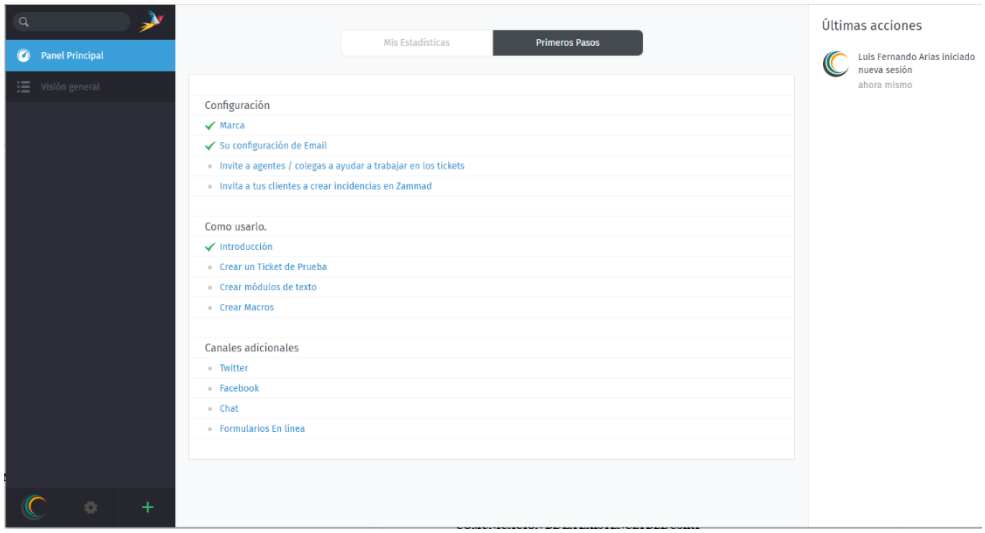
3. PUESTA EN MARCHA DEL CSIRT

3.1 IMPLEMENTACIÓN DE HERRAMIENTAS TECNOLÓGICAS

Sistemas de gestión de tickets y seguimiento de incidentes: Con el objetivo de mantener organizada la información sobre los incidentes atendidos se recomienda la implementación de un Sistema de Seguimiento de Incidentes, para lo cual en esta guía se recomienda la aplicación Zammad aunque podrían usar cualquiera que permita mantener organizada la información en forma de tickets.

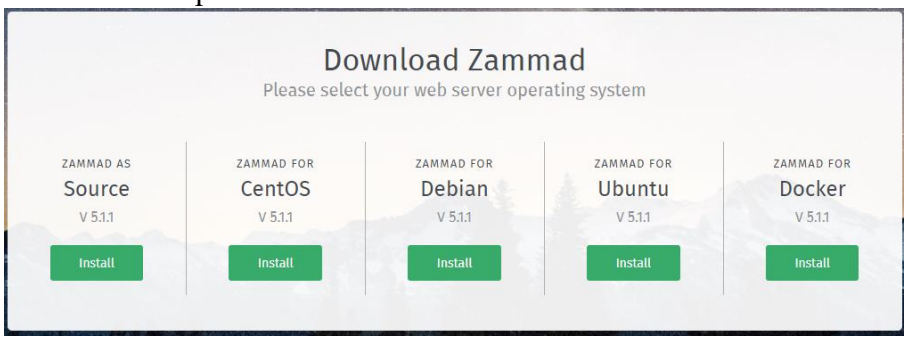
Link de la aplicación: https://zammad.org/

Zammad es una herramienta de Código Abierto y basada en web que permite gestionar tickets y brindar soporte, permite conectar varios canales de comunicación para brindar soporte desde su pantalla principal.



Pantalla principal de Zammad

Instalación: El proceso de instalación se realiza sobre un sistema operativo basado en Linux y existen varias opciones:



Una de las formas más sencillas de realizar la instalación es usando un script el mismo que se puede encontrar en el siguiente link: https://github.com/rsysadmin-com/zammad_installer

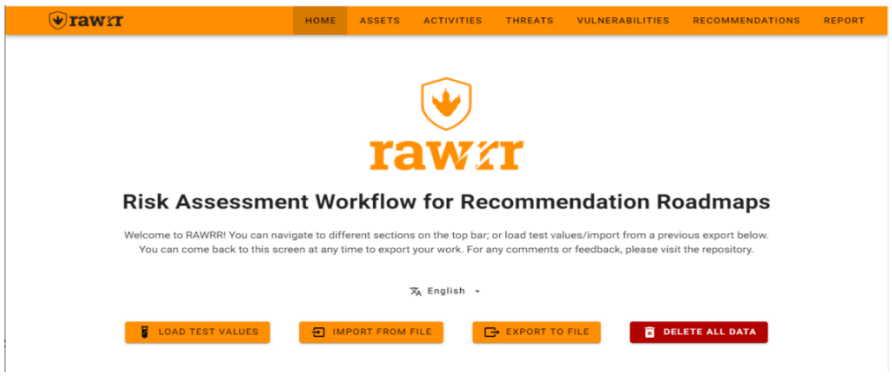
El script funciona en las siguientes distribuciones: CentOS, Ubuntu, Debian y Suse.

El uso de la herramienta es bastante intuitivo y se puede acceder a una documentación detallada en: https://zammad.org/documentation

Aplicación para evaluación de riesgos: La evaluación de riesgos es una actividad que no debería estar lejos de las actividades de un CSIRT de la sociedad civil, pero en la mayoría de ocasiones documentar eficientemente estas evaluaciones puede ser tedioso, para ello la recomendación es utilizar la herramienta: RAWRR (Risk Assessment Workflow for Recommendation Roadmaps) es una aplicación local y multiplataforma que asiste a auditores y otros especialistas de seguridad, facilitando la recopilación de información y posterior generación de reportes.

Link de la aplicación: https://conexo.org/project/rawrr/

Documentación: https://documentacionrawrr.netlify.app/



Ventana principal de RAWRR

3.2 COMUNICACIÓN DE LA EXISTENCIA DEL CSIRT

Cuando el CSIRT esté listo para brindar acompañamiento se deberá comunicar a la comunidad objetivo sobre su existencia, además de iniciar un proceso de difusión de los servicios que brindará, canales de atención y que se puede esperar del mismo.

Para la comunicación de la existencia del CSIRT se puede utilizar la plantilla: RFC 2350

3.3 RECURSOS PARA MEJORAR EL ACOMPAÑAMIENTO EN SEGURIDAD DIGITAL

Para brindar un acompañamiento adecuado en seguridad digital a miembros de la sociedad civil es fundamental utilizar recursos que ya han sido creados por la comunidad, en esta sección se presentan algunos de estos recursos:

- **Kit de Primeros Auxilios Digital:** Es un recurso para situaciones de emergencia creado por la Red de respuesta rápida que sirve para dar soporte ante una situación de emergencia que limite la seguridad digital (RaReNet) y CiviCert (CiviCERT, 2020).
  https://digitalfirstaid.org/es/about/
- **Guía de autodoxing de Access Now:** Esta guía contiene recursos para explorar la inteligencia de fuentes abiertas en uno mismo y prevenir que actores maliciosos utilicen la información pública en contra de los usuarios, además permite mejorar las prácticas de seguridad digital para mantenerse fuera de

peligro y en el caso de estar bajo ataque pueda tener una respuesta de asistencia rápida (Access Now guia línea de ayuda, 2019).

https://guides.accessnow.org/self-doxing.html

- **Totem Project:** Es un sitio web que contiene cursos en formato MOOC(Massive Open Online Course) de diferentes temáticas como: Seguridad de dispositivos móviles, ¿cómo proteger tu identidad online?, Navegación privada, salud mental, vigilancia de comunicaciones, contraseñas seguras, etc (Totem Project, 2022).

  https://totem-project.org/

3.4 MIDIENDO LA MADUREZ DEL CSIRT

Debido a los cambios drásticos de la ciberseguridad, un CSIRT se ajusta a las nuevas necesidades de su comunidad objetivo, por tal motivo es muy importante medir la madurez del CSIRT para poder tener una idea clara sobre el estado actual y principalmente las acciones necesarias para que los procesos mejoren.

SIM3

SIM3 es un acrónimo de las siglas en inglés de Security Incident Management Maturity Model.

El sitio web institucional de la "Open CSIRT Foundation", organización que lo promueve, lo describe de la siguiente manera:

"La madurez de un CSIRT es un indicativo de qué tan bien un equipo gobierna, documenta, ejecuta y mide su función. La madurez de un CSIRT se mide con el Modelo de Madurez de la Gestión de Incidentes de Seguridad, también llamado SIM3."

El modelo está compuesto por 44 parámetros, organizados en 4 categorías y 5 niveles de madurez.

Modelo SIM3

Niveles de Madurez

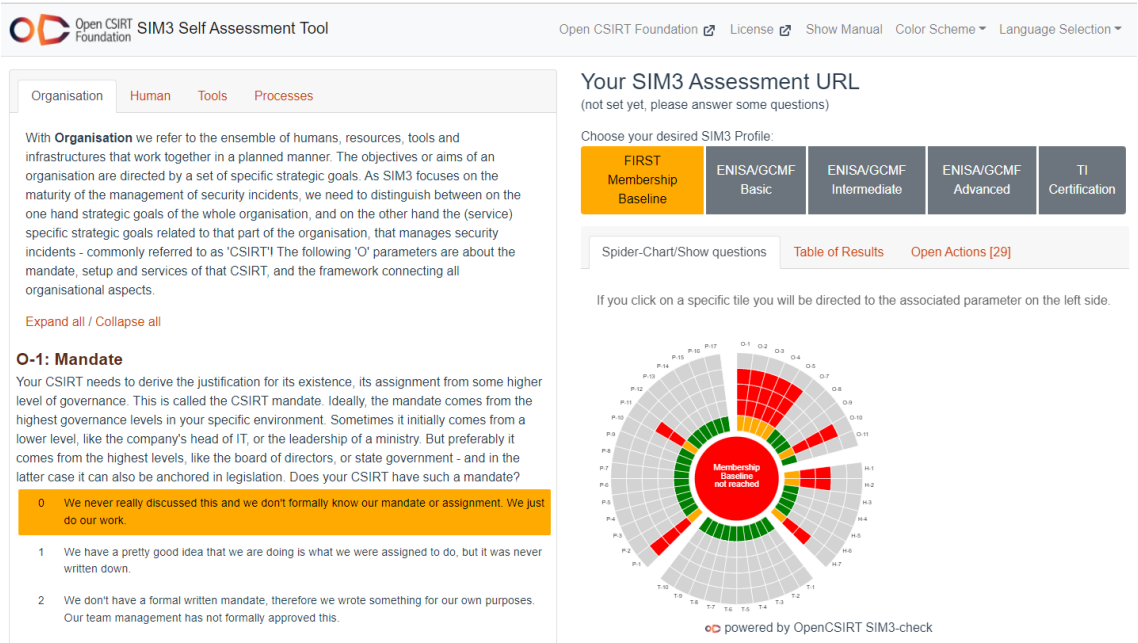
Nivel 0- No disponible/No conozco/No existe: No se tiene conocimiento de que este parámetro, aplique a la institución, no existe o no ha sido definido dentro de la institución.

- ✓ **Nivel 1-** Implícito: Se conoce/está considerado este parámetro dentro de la institución, pero no hay nada escrito sobre él. Es un acuerdo, práctica o procedimiento informal o de palabra.
- ✓ **Nivel 2-** Explícito, interno: El parámetro está escrito, pero no está formalizado. Incluso puede ser algo escrito en una base de conocimiento o sitio web interno (ej: página de wiki).
- ✓ **Nivel 3-** Explícito, formalizado: El parámetro está escrito y es conocido y ha sido aprobado por el director del CSIRT. Incluso puede ser algo escrito en una base de conocimiento o sitio web interno (ej: página de wiki). Si el documento forma parte de la organización o de niveles más altos que el CSIRT y ha sido aprobado por niveles superiores a este, es considerado automáticamente válido, aunque se recomienda que el director del CSIRT avale el documento.

- ✓ **Nivel 4-** Idéntico al 3 pero auditado explícitamente por niveles superiores al de la dirección del CSIRT. Estas auditorías deben realizarse con cierta frecuencia (ej: anual, bianual, etc).

La forma más práctica de comprender cómo funciona el modelo es utilizando la herramienta en línea proporcionada por Open CSIRT Fundation:

https://sim3-check.opencsirt.org



Pantalla principal SIM3 Check

Anexo 1

Plantilla para implementar el marco de trabajo del centro de respuesta a incidentes informáticos para la sociedad civil

Adaptación de: Establishing a csirt - ThaiCERT

Nombre del equipo:	
Misión:	
Grupo objetivo o Constituency:	
Equipo:	
Disponibilidad:	
Relaciones internas y externas:	
Servicios	
Preventivos	**Reactivos**
Infraestructura y herramientas	
Elementos físicos:	
Equipamiento de TI:	
Herramientas específicas:	

Bibliografía

Access Now guia línea de ayuda. (2019). Recuperado el 15 de 04 de 2022, de https://guides.accessnow.org/self-doxing.html

Aguilar, J. (2019). Hechos ciberfísicos: una propuesta de análisis para ciberamenazas en las Estrategias Nacionales de Ciberseguridad. *URVIO Revista Latinoamericana de Estudios de Seguridad*, 24-40.

Apolinario, J. (2022). Propuesta de creación de Centros de respuesta a incidentes de Seguridad informática como estrategia de Cyberseguridad para medios de pagos digitales (Master's thesis, Universidad de Guayaquil-Facultad de Ciencias Matemáticas y Físicas-Carrera de Ingenierí.

Benavides, E., Fuertes, W., Sanchez, S., & Nuñez-Agurto, D. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología, 13*(1), 97-104.

Bernal, P. (2021). Introducción a la Creación de CSIRT. *Cursos del Grupo Técnico de Seguridad 2021*.

CiviCERT. (2020). *Digital First Aid Kit*. Recuperado el 15 de 03 de 2022, de https://digitalfirstaid.org/es/about/

Dias, R., & Borges, F. (2018). Entrevista. *Polifonia*, 160-170.

Espinoza, E. (2020). Reflexiones sobre las estrategias de investigación acción participativa. *Conrado*, 342-349.

Fernández, D., & Martínez, G. (2018). *Ciberseguridad, ciberespacio y ciberdelincuencia.* Thomson Reuters Aranzadi.

Flórez, j. (2021). Diseño administrativo de un centro de respuesta a incidentes cibernéticos para la empresa Cibersecurity de Colombia LTDA.

Fojón, E., & Sanz, A. (18 de Junio de 2010). *Real Instituto Alcano*. Recuperado el 21 de Noviembre de 2021, de http://biblioteca.ribei.org/id/eprint/1879/1/ARI-102-2010.pdf

Inostra, C., Lara, A., Bernal, P., Pérez, E., Alexandro, Y., Lima, E., & anchez, R. (2020). Experiencias, oportunidades y retos de los CSIRT en los nuevos entornos digitales de las Redes Académicas. *Días Virtuales del grupo técnico de Seguridad*.

LACNIC. (2012). *LACNIC.* Recuperado el 10 de 12 de 2021, de https://csirt.lacnic.net/wp-content/themes/warpnew/docs/manual_basico_sp.pdf

Martínez, G. (2022). LACNIC Implementación de SIM3 para los CSIRT Institucionales.

Mikly Melo, J. C., & Siegert Cerezo, E. (2020). Diseño del CSIRT para la Dirección Nacional de Inteligencia DNI.

Ocampo, H. (2019). Diseño documental de un centro de respuestas e incidentes informáticos-CSIRT. Obtenido de https://repository.unad.edu.co/handle/10596/51484

Ríos, E. (2022). Desarrollo de un sistema web prototipo para generar y gestionar documentos necesarios en el proceso de creación de CSIRT académicos.

Tanczer, L. M., Brass, I., & Carr, M. (2018). CSIRT s and global cybersecurity: How technical experts support science diplomacy. *Global policy, 9*, 60-66. doi:https://doi.org/10.1111/1758-5899.12625

Torres, A., & García, A. (2020). Organizaciones Culturales de la Sociedad Civil: Modelos de gestión cultural y administrativa. *Estudios sobre las culturas contemporáneas*(50), 49-74.

Totem Project. (2022). *Totem Project*. Recuperado el 15 de 04 de 2022, de https://totem-project.org/

Unión Internacional de Telecomunicaciones. (2019). *UIT Academy.* Recuperado el 21 de Noviembre de 2021, de https://academy.itu.int/training-courses/full-catalogue/manejo-y-respuesta-incidentes-de-ciberseguridad