GUÍA PRÁCTICA PARA CSIRTs

Volumen 2, 2023

Un modelo de negocio sustentable

OEA | Más derechos para más gente

CSIRTAmericas Network

EMPIEZA CON

POCO Y CRECE

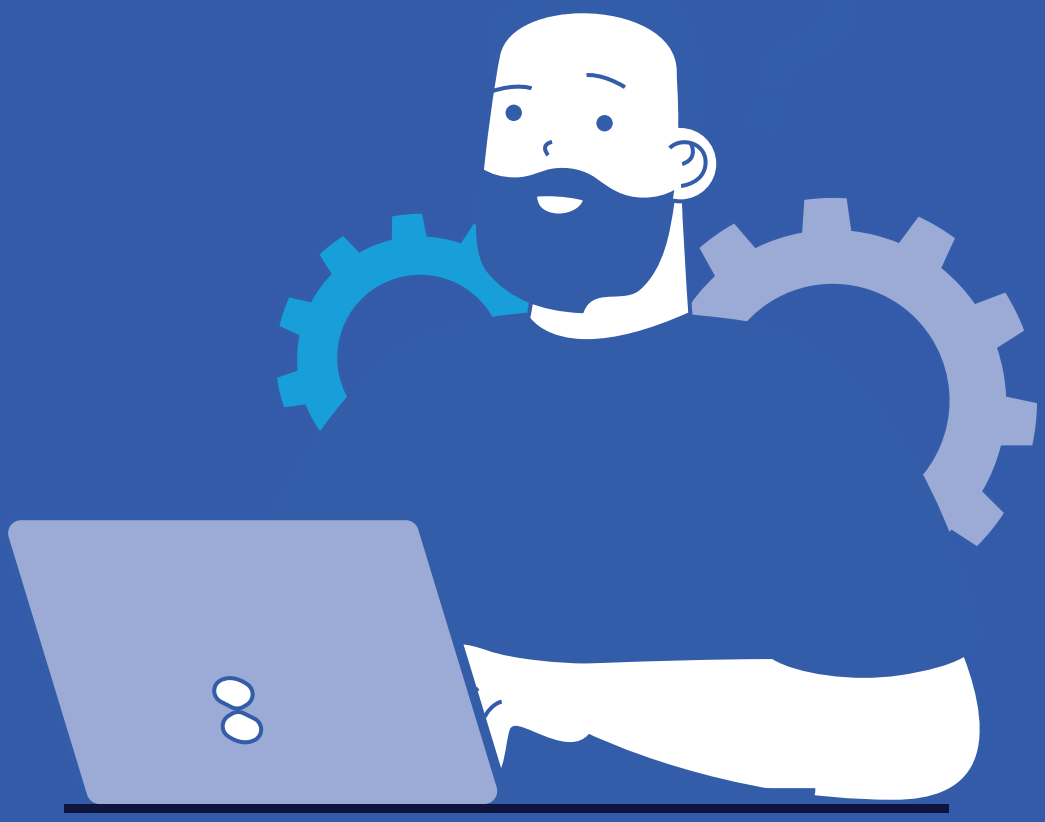
Copyright © 2023 Organización de los Estados Americanos (OEA)
Las opiniones expresadas en esta publicación son de los autores y no necesariamente reflejan las opiniones del Secretario General de la Organización de los Estados Americanos o de los Estados Miembros.

GUÍA PRÁCTICA PARA CSIRTs

Volumen 2, 2023

Un modelo de negocio sustentable

Tabla de Contenido



0. CÓMO USAR ESTA GUÍA

Esta guía parte del documento anterior "Buenas Prácticas para establecer un CSIRT nacional"[1] elaborado por la Organización de Estados Americanos (OEA) en 2016, donde se cubren temas de planeamiento e implementación de un Equipo de Respuesta ante Incidentes Cibernéticos (CSIRT, por sus siglas en inglés), incluyendo aspectos organizacionales, de recursos humanos, capacitaciones e infraestructura, entre otros. Este segundo volumen pretende construir sobre el anterior y servir de guía direccional para un líder de proyecto, tomador de decisiones o cualquier persona interesada en crear, desarrollar, modernizar o sostener un CSIRT con un enfoque estratégico.

La guía se limita a CSIRTs del ámbito público, con especial foco en América Latina y el Caribe, y se basa en la experiencia de más de 15 años y el conocimiento de la OEA en la materia, y datos estadísticos reales obtenidos de la Red CSIRTAmericas[2] del CICTE/OEA. Adicionalmente, toma consejos y experiencias de referentes en la región y a nivel global que fueron entrevistados y citados con propósitos puramente educativos para la elaboración de este documento.

Esta guía presenta recomendaciones generales, por lo que es importante comprender que al evaluar las mejores prácticas es indispensable contextualizar el espacio, tiempo y recursos disponibles en cada situación. Cada país posee diferentes sistemas políticos, culturales, geográficos y legales, por lo que esta guía no pretende servir de modelo estático, sino ser un recurso que permita su aplicabilidad a cada condición local según sea necesario.

[1] Buenas Prácticas para establecer un CSIRT nacional. Organización de Estados Americanos, 2016.
https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2016%20-%20Buenas%20Practicas%20CSIRT.pdf

[2] La Red CSIRTAmericas es la red de Equipos de Respuesta ante Incidentes Cibernéticos (CSIRTs) gubernamentales de los Estados Miembros de la OEA.
Más información: https://csirtamericas.org/

1. POR QUÉ ES NECESARIO UN CSIRT

Hace apenas algunos años, eventos como el que una región sufriera el desabastecimiento de combustible, que un organismo de gobierno sufriera la exposición de su información, o que un ciudadano sufriera una suplantación de su identidad en línea, podían considerarse eventos aislados sin relación alguna. Hoy en día, dado el avance exponencial de los sistemas de información, conectividad, complejidad en la tecnología híbrida, intercambio de datos y ecosistemas empresariales ampliados, sabemos que existe un posible factor común en escena, origen de estos y muchos otros escenarios, los ”incidentes de ciberseguridad”.

Resulta primordial y necesario, entonces, que una organización sea capaz de detectar, contener, mitigar y así recuperar lo más pronto posible la prestación de sus servicios o, en otras palabras, tenga la capacidad de prevenir y responder a un incidente de ciberseguridad.

Vivimos en un mundo digitalizado donde las comúnmente llamadas infraestructuras críticas —cadenas de distribución, transporte, comunicaciones, servicios esenciales como electricidad y agua, por nombrar algunas— conviven en el ciberespacio y, por ende, necesitan de protección adecuada, por lo tanto, podemos decir que la ciberseguridad atraviesa e interpela todas las áreas de nuestra vida y permite el correcto funcionamiento y operación de gobiernos, empresas y ciudadanía.

Como fue mencionado anteriormente, ante un escenario adverso es necesario que cada organización prevenga y responda a un incidente de ciberseguridad. Sin embargo, la realidad es que muchas veces la organización no cuenta con el conocimiento ni la experiencia, por lo que contar con un Equipo de Respuesta a Incidentes Cibernéticos o, en inglés, Computer Security Incident Response Team (CSIRT) puede marcar la diferencia en la respuesta coordinada y eficiente frente a un ataque, y así ayudar a mitigar las consecuencias de este.

En palabras simples, un CSIRT **brinda servicios de ciberseguridad para prevenir, detectar, mitigar y responder a incidentes cibernéticos en una comunidad definida.** Un CSIRT cuenta con una estructura organizativa con procesos establecidos y un catálogo de herramientas tecnológicas, además de un presupuesto, mandatos, catálogo de servicios, personal especializado, red de contactos, plan de comunicaciones, un marco legal habilitante que le permita actuar, y muchos otros elementos que conforman la base para la gestión de incidentes cibernéticos de una comunidad atendida definida, así como para apoyar dicha comunidad de la mejor manera.

Tanto organismos públicos como empresas privadas, entidades militares, academia y otras organizaciones que se consideran infraestructuras críticas se enfrentan a incidentes cibernéticos y, en muchos casos, no cuentan con procedimientos formales para responder a un incidente y, en otros, con una orientación clara de cómo abordar un incidente. Ante este escenario es importante preguntarnos, **¿es necesario un CSIRT?**

Esa es una pregunta común a la que se enfrentan los tomadores de decisiones que tienen a su cargo elaborar políticas, lineamientos y estrategias nacionales, así como quienes gestionan presupuestos, administradores de proyectos, líderes de industria, empresas privadas, fuerzas del orden y academia. La respuesta no suele ser lineal y sencilla por la

falta de claridad respecto a lo que puede o debe hacer un CSIRT; sin embargo, un país o sector que cuente con un CSIRT podrá:

• **Responder a un incidente** con procedimientos estandarizados y mayor preparación para su atención.

• **Coordinar el apoyo** con colaboradores técnicos de otras instituciones nacionales o internacionales para la resolución de un incidente.

• **Tener amplia visibilidad de los riesgos** actuales de su sector o país.

• **Anticiparse a la materialización de un incidente** con estrategias de inteligencia de amenazas y sistemas de alertas tempranas.

• **Alertar a la comunidad atendida** sobre indicadores de compromiso (IoC), indicadores de ataque (IoA) o vulnerabilidades identificadas a nivel nacional e internacional.

• **Desarrollar y coordinar operaciones de respuesta** a incidentes cibernéticos que requieran la actuación de otras áreas u organizaciones con fines de entrenamiento y preparación.

• **Apoyar la generación de una cultura ciudadana** en temas relacionados con la ciberseguridad.

• **Servir como referente en la construcción de estrategias** sectoriales o nacionales de ciberseguridad.

• **Detectar y promover talentos en ciberseguridad** en el sector educativo, de comunidades o de un país.

• **Establecer estrategias** que permitan la alineación de las capacidades de prevención, detección y respuesta para gestionar, mitigar y superar los ciberataques.

• **Impulsar el desarrollo del ecosistema de ciberseguridad a nivel nacional,** por medio del consumo y generación de servicios provistos desde y hacia los sectores público, privado y academia.

• **Servir como entidad coordinadora de la ciberseguridad nacional** a nivel país, desde un marco legal de respeto a derechos humanos.

Dada la importancia de un CSIRT y su alcance, en esta guía expondremos —a partir de testimonios de especialistas de ciberseguridad que han trabajado en CSIRTs de Latinoamérica y el Caribe— las mejores prácticas para la creación, operación y sostenibilidad de un Equipo de Respuesta a Incidentes Cibernéticos.

2. CUÁL ES LA DIFERENCIA ENTRE UN **CSIRT NACIONAL Y UNO SECTORIAL**

Actualmente en Latinoamérica y el Caribe observamos un aumento de CSIRTs en los ámbitos militar, gobierno, salud y bancario, entre otros, y aunque hay similitudes, también hay diferencias **entre un CSIRT nacional y un CSIRT sectorial.**

Un CSIRT nacional actúa como punto único internacional y nacional para la coordinación de la atención a incidentes cibernéticos que afectan a un país. Su ámbito de competencia abarca centralizar el análisis situacional, articular acciones de coordinación rutinaria y en circunstancias de crisis (por ejemplo, eventos electorales o deportivos, conflictos sociales, cumbres regionales), brindar recomendaciones desde el punto de vista técnico, promover iniciativas legislativas de ciberseguridad en su país, crear y fomentar una comunidad y cultura en ciberseguridad, así como coordinar la atención de incidentes cibernéticos con otras instancias, por ejemplo, con otros CSIRTs sectoriales y organismos internacionales y desarrollar sus capacidades cibernéticas.

Por su parte, un CSIRT sectorial brinda asistencia para la resolución de incidentes cibernéticos en comunidades concretas, muchas veces con tecnologías especializadas que demandan un tratamiento específico. Por ejemplo, el sector militar muchas veces hace uso de tecnologías clasificadas como sistemas de rutas de vuelo o controles de mando de embarcaciones que necesitan de un nivel de experticia para la atención de un incidente. Esta situación es diferente al hablar de un CSIRT perteneciente a una empresa del sector privado, ya que aglutina a organizaciones del sector de comercio minorista o financiero, por ejemplo, donde no solo su tecnología sino sus intereses son completamente diferentes. Como se menciona en el capítulo 0, para los propósitos de esta guía nos enfocaremos en los CSIRTs del sector público.

Como se muestra en la imagen inferior (imagen 1), una buena práctica en un ecosistema donde coexista un CSIRT nacional y múltiples CSIRTs sectoriales es aquella donde se genera un ambiente colaborativo de coordinación continua e intercambio de información, que permita a un CSIRT nacional tener un panorama real y actualizado de las amenazas de ciberseguridad que enfrenta un país en todos sus sectores, generando una ciberseguridad con un enfoque nacional, siendo este parte de la Gobernanza Digital. Sin embargo, para que este panorama ideal ocurra en la realidad es necesario contar con elementos clave que recopilamos y describimos en esta guía.

Imagen 1

Ejemplo de estructura colaborativa de CSIRT nacional y CSIRTs sectoriales

Fuente: Organización de Estados Americanos, 2023.

3. PANORAMA DE LOS CSIRTs EN LATINOAMÉRICA Y EL CARIBE

3.1 ¿Dónde se han ubicado los CSIRTs nacionales?

Ante el incremento de incidentes cibernéticos de relevancia nacional en países de Latinoamérica y el Caribe, y la necesidad de los gobiernos de reaccionar ante ellos, a partir de 2003 el rol del CSIRT toma relevancia, por lo que se dan las condiciones para la creación y asignación de presupuestos necesarios para la conformación de CSIRTs en la región, lo que condujo a que con el paso del tiempo no solo se constituyeran CSIRTs nacionales sino también sectoriales.

En algunos casos, los CSIRTs se crearon por una Estrategia de Ciberseguridad Nacional y, en otros, por proyectos de ley o la emisión ministerial o presidencial de decretos o política pública; pero independientemente del origen, el surgimiento de los *Equipos de Respuesta a Incidentes Cibernéticos* ha dotado a la región de elementos para hacer frente a los incidentes cibernéticos.

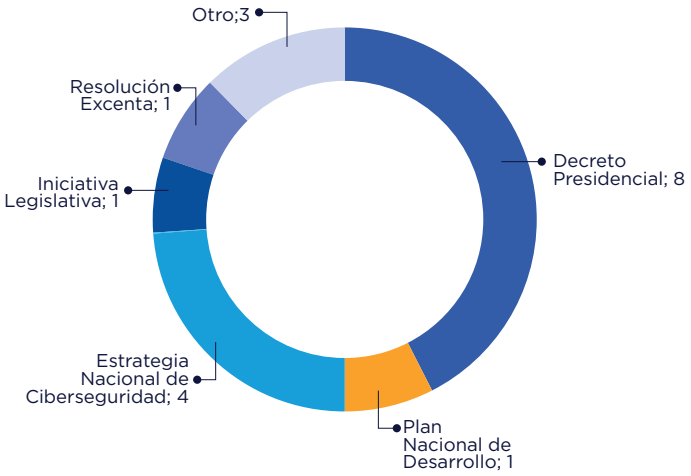
La creación del CSIRT requiere de un proceso de formalización que, normalmente, depende de un mandato derivado de una instancia de gobierno. En Latinoamérica y el Caribe los mandatos se han promovido, entre otros, por medio de:

- Decreto Presidencial
- Plan Nacional de Desarrollo
- Estrategia Nacional de Ciberseguridad
- Iniciativa Legislativa
- Resolución Exenta
- Acuerdo Ministerial

La gráfica 1 muestra el procedimiento normativo por el cual fueron constituidos los CSIRTs públicos de la región de la OEA y que forman parte de la Red *CSIRTAmericas*[3] , mientras que en la tabla 1 se observa que no hay un estándar definido para ubicarlos; todo dependerá del país, mandato, economía, estructura organizativa legal y contexto político y sociocultural donde se desenvuelve.

Gráfica 1

Procedimiento normativo por el cual fue creado el CSIRT de tipo nacional en la Red CSIRTAmericas



Fuente: Información de la red CSIRTAmericas de la Organización de los Estados Americanos (OEA), 2023.

[3] La Red CSIRTAmericas es la red de Equipos de Respuesta ante Incidentes Cibernéticos (CSIRTs) gubernamentales de los Estados Miembros de la OEA. Más información: https://csirtamericas.org/

Tabla 1

Ubicación institucional de CSIRTs de la región
(Información con base a las respuestas oficiales recibidas a la encuesta realizada por la red CSIRTAmericas)

PAÍS	CSIRT	NOMBRE OFICIAL	ADSCRITO A
Argentina	CERT.ar	Equipo de Respuesta ante Emergencias Informáticas Nacional - CERT.ar	Jefatura de Gabinete de Ministros (Oficina de Presidencia/Gobierno Estatal o Local)
Argentina	BA-CSIRT	Centro de Ciberseguridad de la Ciudad Autónoma de Buenos Aires	Gobierno Estatal o Local
Barbados	CIRT-BB	CIRT-BB	Ministerio de Industria, Innovación, Ciencia y Tecnología
Bolivia	CSIRT-Bolivia	Centro de Gestión de Incidentes Informáticos (CGII)	Ministerio de la Presidencia
Brasil	CTIR Gov	Computer Security and Incident Response Team (CTIR Gov)	Gabinete Presidencial
Chile	CSIRT-CL	Equipo de Respuesta ante Incidentes de Seguridad Informática de Chile	Ministerio del Interior y Seguridad Pública
Colombia	ColCERT	Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT	Ministerio de Tecnologías de la Información y las Comunicaciones
Colombia	CSIRT-CCOCI	CSIRT - Comando Conjunto Cibernético	Ministerio de Defensa Nacional (FF.AA.)
Costa Rica	CSIRT-CR	CSIRT-CR	Ministerio de Ciencia y Tecnología
Estados Unidos	US-CERT	Cybersecurity and Infrastructure Security Agency (CISA)	Departamento de Seguridad Nacional
Guatemala	CRIC-GT	Centro de Respuestas a Incidentes Cibernéticos (CRIC) del Ejército de Guatemala	Ministerio de Defensa (FFAA)
Guyana	CSIRT.GY	CSIRT.GY	Oficina del Primer Ministro – Autoridad Nacional de Gestión de Datos

Tabla 1

Ubicación institucional de CSIRTs de la región
(Información con base a las respuestas oficiales recibidas a la encuesta realizada por la red CSIRTAmericas)

Jamaica	Ja-CIRT	Jamaica Cyber Incident Response Team (Ja-CSIRT)	Ministerio de Ciencia, Energía y Tecnología
México	CSIRT-SEMAR-MX	CSIRT-SEMAR-MX	Ministerio de Defensa (FFAA)
México	CSIRT-SEDENA-MX	CSIRT-SEDENA-MX	Ministerio de Defensa (FFAA)
Paraguay	CERT-PY	CERT-PY	Ministerio de Tecnologías de la Información y Comunicaciones (MITIC)
Perú	CSRIT-MGP	CSIRT – Marina de Guerra de Perú	Ministerio de Defensa (FFAA)
República Dominicana	CSIRT-RD	Equipo Nacional de Respuesta a Incidentes Cibernéticos (CSIRT-RD)	Ministerio de la Presidencia
República Dominicana	CSIRT-Defensa	Equipo de Respuesta a Incidentes Cibernéticos de Defensa (CSIRT-Defensa).	Ministerio de Defensa (FFAA)
Suriname	SurCSIRT	SurCSIRT	Agencia de Seguridad Nacional
Trinidad y Tobago	TTCSIRT	Trinidad and Tobago Cyber Security Incident Response Team	Agencia de Seguridad Nacional
Uruguay	DCSIRT-UY	DCISRT-UY	Ministerio de Defensa (FFAA)
Uruguay	CERTuy	Centro Nacional de Respuesta a Incidentes de Seguridad Informática	AGESIC / Presidencia de la República

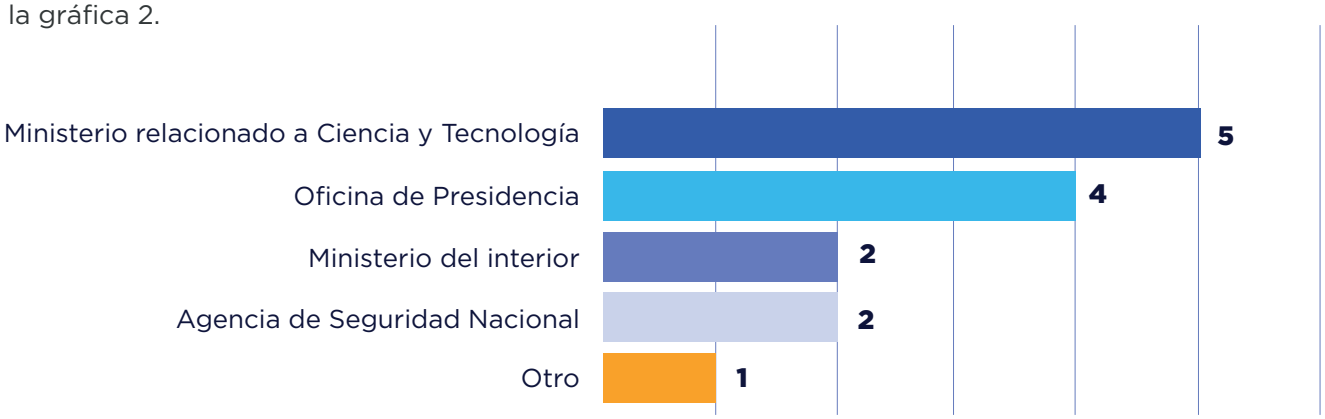
Fuente: Información con base a las respuestas oficiales recibidas a la encuesta realizada por la red CSIRTAmericas de la Organización de los Estados Americanos (OEA), 2023.

| Para información completa sobre los CSIRTs miembros de la red, visite: https://csirtamericas.org/es/member_teams

Cuando se plantea la creación de un CSIRT nacional surge la pregunta **¿dónde lo ubico?** En Latinoamérica y el Caribe predominan como organismos promotores los ministerios orientados a Ciencia y Tecnología, del Interior, de la Defensa, así como agencias o departamentos adscritos a la presidencia, entre otras posibilidades que se pueden observar en la gráfica 2.

Gráfica 2

Institución de gobierno a la que se encuentra adscrito un CSIRT de tipo nacional en la Red CSIRTAmericas



Fuente: Información de la red CSIRTAmericas de la Organización de los Estados Americanos (OEA), 2023.

Para seleccionar un organismo promotor y definir dónde (en qué institución) se ubicará dicho CSIRT nacional es recomendable responder a las siguientes preguntas:

¿Es un organismo que genera confianza en los organismos del sector?

¿Es un organismo con capacidad de coordinación, atención y acceso a todos los organismos de un sector?

¿Es un organismo con una base financiera sólida para mantener y fortalecer las operaciones del CSIRT?

Para responder estos cuestionamientos es importante tener en cuenta que **la principal característica y habilidad de un CSIRT debe ser la generación de confianza en las organizaciones que forman parte de la comunidad atendida;** las instituciones a las cuales brindará servicios no deben sentir temor al reportar un incidente o solicitar apoyo, sobre todo en momentos de crisis, ya que un CSIRT es un organismo que, principalmente, provee apoyo, recomendaciones y mentoría, pero no impone, juzga o regula.

> Se realizó una evaluación antes de la creación del CSIRT y la conclusión fue que debían encontrar un lugar donde se generara la confianza necesaria para brindar los servicios. Finalmente quedó dentro de la Oficina de Presidencia

República Dominicana
CSIRT-RD, CSIRT nacional

Otras dos características por considerar son que **el área donde se encuentre ubicado el CSIRT deberá entender la importancia de priorizar la protección de la información, además de tener la capacidad de apoyar y coordinar a cualquier miembro de la comunidad atendida.** Es decir, un CSIRT debe contar con una capacidad inmediata de convocatoria y respuesta para la coordinación multisectorial y, a su vez, tener recursos financieros sólidos para la operación diaria, formación de personal, creación y sostenimiento de servicios, así como disponibilidad de fondos en momentos de emergencia o crisis circunstanciales que se presentan en la comunidad atendida, y contar con el apoyo político del más alto nivel para poder gestionar los incidentes a nivel nacional.

Algunos expertos consideran que para ubicar al CSIRT también se debe tomar en cuenta la importancia de la **autonomía e independencia** que el CSIRT requiere para realizar su trabajo. Ambas características se logran con base en la confianza, una correcta priorización de la protección de información y la capacidad de convocatoria para trabajar codo a codo con cada uno de los miembros de su comunidad atendida, sabiendo que todos tienen un mismo fin: la resolución del incidente.

Adicionalmente, al definir la ubicación de un CSIRT nacional dentro de un ministerio, entidad o secretaría se recomienda tener en cuenta que el CSIRT puede aprovechar los servicios internos disponibles necesarios (como recursos humanos, finanzas, infraestructura, etcétera) para la creación de su estructura.

Por último, es importante contar con el apoyo del ministerio, entidad o secretaría anfitriona para que el CSIRT opere con **velocidad y flexibilidad** (necesarias ante los retos actuales) mientras se sostiene y crece en el tiempo.

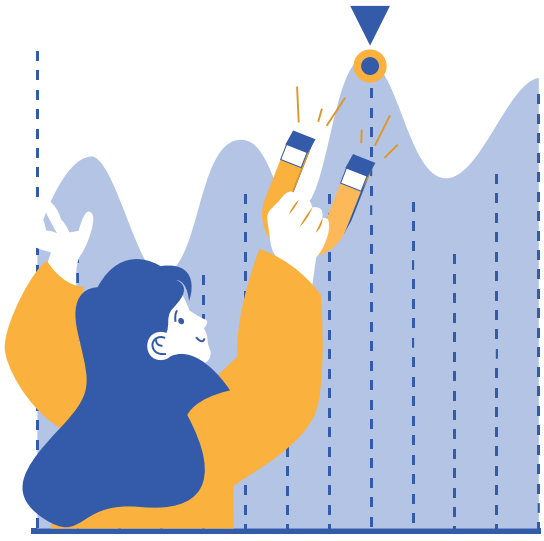
3.2 Asegurando la continuidad de los CSIRT en Latinoamérica y el Caribe

Para lograr la continuidad, así como la consolidación y sostenibilidad de un CSIRT a lo largo del tiempo se debe sopesar un conjunto de factores que impactan en una gestión de incidentes cibernéticos efectiva, como el talento humano, el desarrollo de la confianza, el establecimiento de procesos y la obtención de los presupuestos necesarios (que no sólo se destinarán a los recursos humanos, infraestructura, capacitación y oficinas para operaciones normales, sino también para proyectos de mejoramiento que resulten necesarios).

Muchos de los especialistas de la región entrevistados para la realización de este documento coinciden en que **un factor que puede contribuir al éxito de un CSIRT es comenzar en pequeño; construir a partir de un plan sencillo, con acciones o servicios concretos, y realizar evaluaciones periódicas que permitan conocer los avances y, si fuera el caso, proponer cambios.**

Proponer cambios implica un proceso de transformación que se logra al identificar y analizar estratégicamente qué requiere la comunidad en cuanto a servicios, el número y características de recursos humanos que participa en la operación, y la tecnología necesaria para cubrir los servicios que se ofrecen. Esto requiere por parte del CSIRT una **escucha activa** y poner al "cliente" en el centro de la operación. Se recomienda que entre los servicios básicos iniciales se ofrezcan los siguientes: un sistema de tickets[4], un servidor de correo electrónico, línea telefónica, una página web y, por lo menos, un servicio adicional como la emisión de boletines de alertas. No es recomendable lanzar servicios

"EMPIEZA CON **POCO Y CRECE"**



[4] Sistema automático de registro de casos para el correcto seguimiento y priorización de las solicitudes de una comunidad.

porque otros CSIRTs los tienen o por una recomendación fuera de contexto, ya que cada comunidad es diferente, por lo tanto, será necesaria la evaluación estratégica mencionada del valor que aporta cada uno de los servicios a la comunidad y sus necesidades específicas. Se recomiendan pequeñas acciones pero de gran impacto que permitan ir afianzando con logros el trabajo del CSIRT.

Respecto al talento humano, es recomendable iniciar con el personal mínimo necesario para operar los servicios mencionados. Según la ENISA, el número promedio de personal trabajando en un equipo pequeño es de 3 a 7[5], sin embargo, este número dependerá de los servicios definidos con anterioridad. En muchas ocaciones al comienzo se contrata personal *junior* o con poca o nula experiencia en ciberseguridad, lo que hace que muchos de los cimientos del CSIRT no queden sólidos. A pesar de que esto puede mejorar con el tiempo, resulta más costoso en comparación con hacerlo al inicio. Una buena recomendación en este sentido sería contratar personal con la experiencia suficiente o contratar servicios de consultoría.

Con el personal definido, los servicios acotados y el establecimiento de procesos necesarios será posible gestionar las expectativas que se establezcan ante los tomadores de decisiones y la comunidad atendida al inicio de la operación del CSIRT. Atender estas recomendaciones también permitirá crecer orgánicamente y dar respuesta a los incidentes que se presenten.

Así como el inicio de la operación de un CSIRT en general se lleva a cabo con una serie de servicios básicos acotados, uno con un alto nivel de madurez puede estar atendiendo telefónicamente a los llamados de notificación de incidentes cibernéticos de instituciones afectadas, desplegar personal para la atención en sitio de un incidente relacionado a una fuga de información, monitorear y analizar patrones de amenazas cibernéticas, capacitar a organizaciones de la comunidad, hacer pruebas en el laboratorio de un nuevo servicio para la mitigación de ataques de Denegación de Servicio Distribuida (DoS), actualizar reglas de un *Web Application Firewall* (WAF)[6], analizar logs, participar en comités para el desarrollo y actualización de estrategias de ciberseguridad, coordinar mesas de trabajo para la protección de algún evento de alcance nacional, realizar *hardening*[7] en servidores y muchas otros de los que se encuentran en el catálogo de servicios del FIRST[8] el cual se basa en las siguiente cinco áreas:

- Gestión de incidentes de ciberseguridad.
- Gestión de vulnerabilidades.
- Concientización.
- Transferencia de conocimientos.
- Gestión de eventos de ciberseguridad.

Un CSIRT no solamente se debe enfocar en responder a incidentes cibernéticos cuando una institución lo requiere; un CSIRT juega un rol fundamental en la coordinación de ciberseguridad en eventos de impacto social

[5] ENISA, December 2020. How to set up CSIRT and SOC, Good Practice Guide. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc
[6] Web Application Firewall: Firewall de Aplicación Web
[7] Hardening: consiste en el proceso de reducción de vulnerabilidades en las aplicaciones o sistemas.
[8] FIRST: Forum of Incident Response and Security Teams. https://www.first.org/

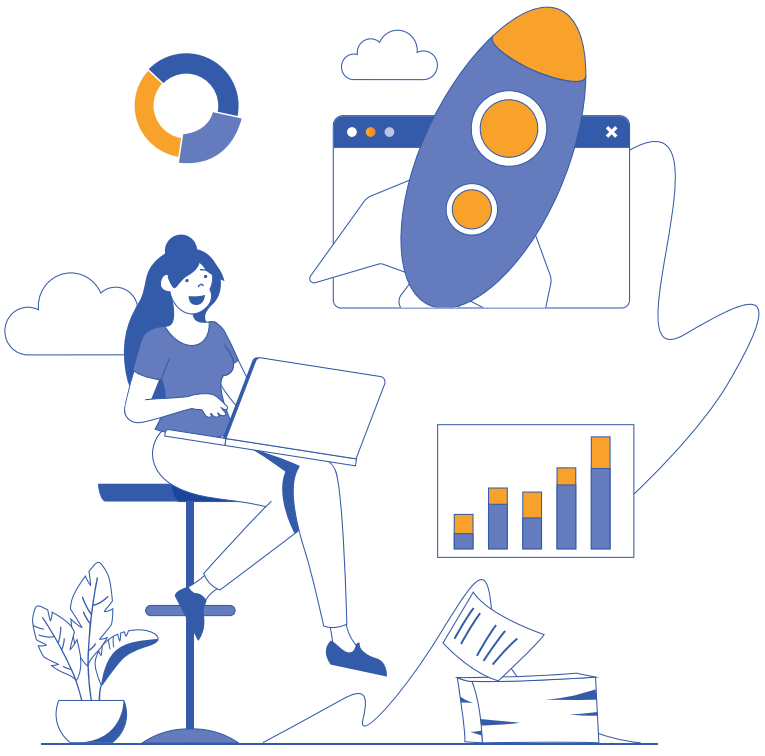
y económico de un país, razón por la que deberá desarrollar confianza más allá de los decretos y acuerdos existentes. **Es por medio de la confianza y la generación de valor que un CSIRT puede ubicarse del lado del afectado y ayudarlo, y no en su contra.**

> "La normativa establece que el CERTuy tiene la potestad de intervenir en incidentes de seguridad informática, sin embargo gracias a la confianza generada su participación nunca tuvo que ser forzada, todo lo contrario"
>
> **Uruguay**
> **CERTuy, CERT nacional**

Los CSIRTs de Latinoamérica y el Caribe han tenido un rol protagónico en la coordinación de eventos e iniciativas relacionadas a la ciberseguridad que ha requerido que incluyeran nuevos servicios; algunos de esos eventos o iniciativas son:

- Jornadas electorales
- Juegos deportivos nacionales y regionales
- Ejercicios intersectoriales
- Elaboración de Estrategias Nacionales de Ciberseguridad
- Situaciones de escalada de conflictos sociales
- Cumbres regionales o nacionales
- Coordinación de contenido de cátedras y programas con las universidades

El desarrollo de los CSIRTS y su continuidad en la región ha llevado a la incorporación de servicios que normalmente prestaría un *Security Operations Center (SOC)*, esto puede ser de gran valor para la comunidad, pero será importante revisar el mandato que se tiene para determinar si es un servicio que puede ser brindado por el CSIRT o no. En el ANEXO 1 se describen las características y diferencias entre un CSIRT, un CERT y un SOC, pero en general será el mandato que dio origen al CSIRT el que defina sus ámbitos de operación.



3.3 El Reto: Escenarios impredecibles, recursos humanos, presupuesto y tecnología

Uno de los grandes desafíos y oportunidades que tiene un CSIRT es enfrentarse cada día a un escenario impredecible que puede incluir: olas de ataques, aparición de nuevos patrones, nuevos grupos de ciberdelincuencia cada vez más sofisticados, y tensiones políticas o ciclos electorales, que llevan a un CSIRT a poner al límite sus capacidades de atención, respuesta y gestión de incidentes. En la región este ritmo de fenómenos ha producido una serie de desafíos que empiezan por la limitación de los presupuestos asignados para las operaciones diarias, cambio de rumbo por contextos políticos variables, demoras en la adquisición de herramientas de ciberseguridad, así como el riesgo de la continuidad en la prestación de servicios (establecidos y nuevos) a la comunidad.

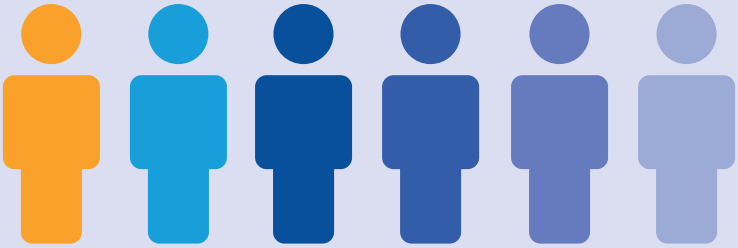
Asimismo, el riesgo de continuidad tiene dos vertientes. La primera es la alta rotación de personal que tiene su origen en el conocimiento adquirido en el CSIRT y el interés de la iniciativa privada de hacerse de recursos capacitados para afrontar sus desafíos de ciberseguridad.

Para entender el panorama en cuanto al personal, actualmente el promedio de personas que trabajan en un CSIRT público de Latinoamérica y el Caribe es de seis, de las cuales el 74% son hombres y el 26% mujeres. Esta distribución varía en cuanto a posiciones de liderazgo como se muestra en la gráfica 3.

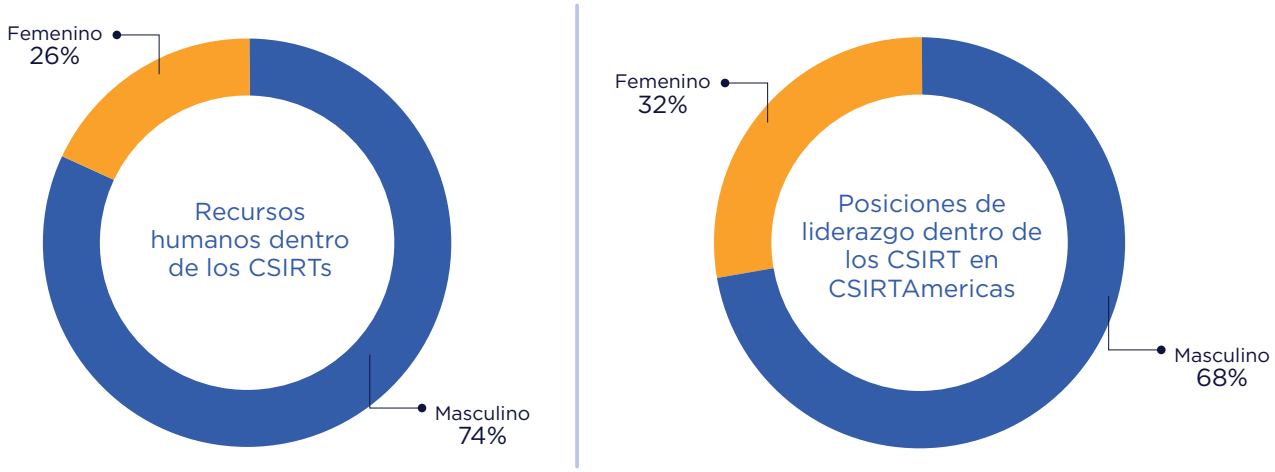
> “Después de 18 o 24 meses de trabajar en un CSIRT una persona se convierte en un candidato muy atractivo para la iniciativa privada. Para evitar tener una alta rotación del equipo es importante mantener a las personas motivadas, capacitadas y comprometidas con la misión”
>
> **República Dominicana**
> **CSIRT-RD, CSIRT nacional**

Gráfica 3

Recursos Humanos y los CSIRTs en la Red CSIRTAmericas



6 Miembros por CSIRT en promedio



Fuente: Red CSIRTAmericas, Organizaciones de los Estados Americanos, 2023.

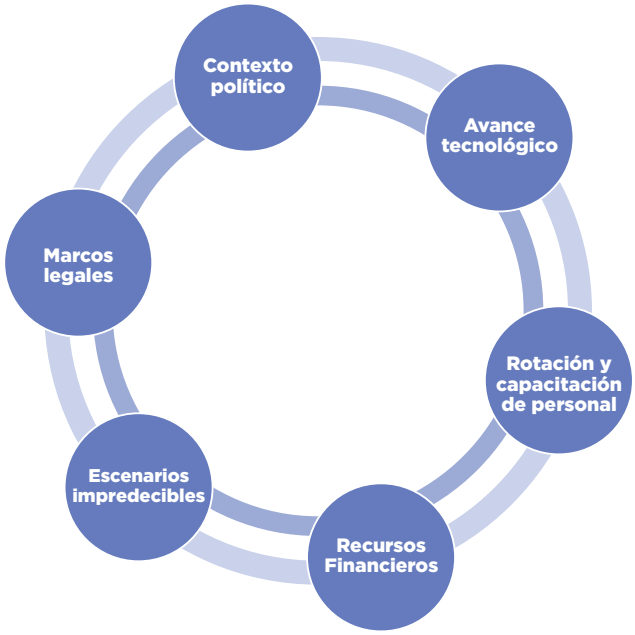
La segunda vertiente está relacionada con el **presupuesto**, en la región, es un fenómeno periódico la creación de CSIRTs sin presupuestos fijos asignados, conformación de equipos con préstamo de personal de otras áreas de la institución o de entidades externas, perfiles salariales no compatibles con el CSIRT, cambios de gobierno, procesos de compras demorados, actividades extraordinarias, migración de tecnologías y fenómenos de deuda tecnológica terminan erosionando considerablemente la operación sostenible de un CSIRT. En este sentido, es fundamental contar con un presupuesto asignado, flexible que contemple la adquisición de nuevas herramientas y licencias, su renovación y actualización, consultorías de migración de soluciones, jornadas especiales de desplazamiento de personal, formación, expansión de servicios, entre otras. En el Anexo B puede encontrarse un presupuesto que contiene consideraciones importantes y puede servir de referencia para el armado de un presupuesto inicial.

En cuanto a la **tecnología**, los CSIRTs atesoran una gran ventaja en el uso e implementación de soluciones de software libre que son desarrolladas y compartidas por comunidades de ciberseguridad a lo largo del mundo. Sin embargo, es importante considerar que la arquitectura tecnológica debe instrumentarse de forma estratégica con una mezcla adecuada entre software libre y software adquirido con fines específicos. En este sentido, es importante tener en cuenta que, por la naturaleza cambiante de las tecnologías asociadas a la operatividad y atención de incidentes, resulta imprescindible adecuarse a esta realidad, a través de la evaluación de nuevas soluciones, actualizaciones y ajustes frecuentes en tecnologías asociadas a servicios. Este y otros aspectos se abordarán en la siguiente sección con recomendaciones específicas para el sostenimiento del CSIRT.

Como se observa, existen retos y actividades diarias que conforman la esencia de un CSIRT, desde aspectos políticos hasta los retos más técnicos. Dichos retos afectan al CSIRT en distintos grados y niveles, y conviven interconectados por el ciclo de vida de un CSIRT, como se representa en el diagrama a continuación.

Gráfica 4

Retos de continuidad para CSIRTs públicos



Para hacer frente a los retos de continuidad, resulta útil visualizar a un CSIRT como un modelo de negocio que requiere ser rentable en términos de generación de valor para cierta comunidad atendida. Adicionalmente, algunos CSIRT de la región consideran estratégicas las siguientes acciones:

- Reclutar personal con habilidades blandas más que técnicas; es decir, personas con pensamiento crítico, analíticas, orientadas al riesgo o con mente estratégica, ya que es más difícil desarrollar las capacidades blandas que enseñar las técnicas.

- No centralizar las responsabilidades en un único recurso.

- Crear compromiso y sentido de pertenencia.

- Realizar acuerdos con empresas privadas para la formación del personal que labora en el CSIRT.

- Establecer con universidades acuerdos de pasantías con carreras asociadas a ciberseguridad.

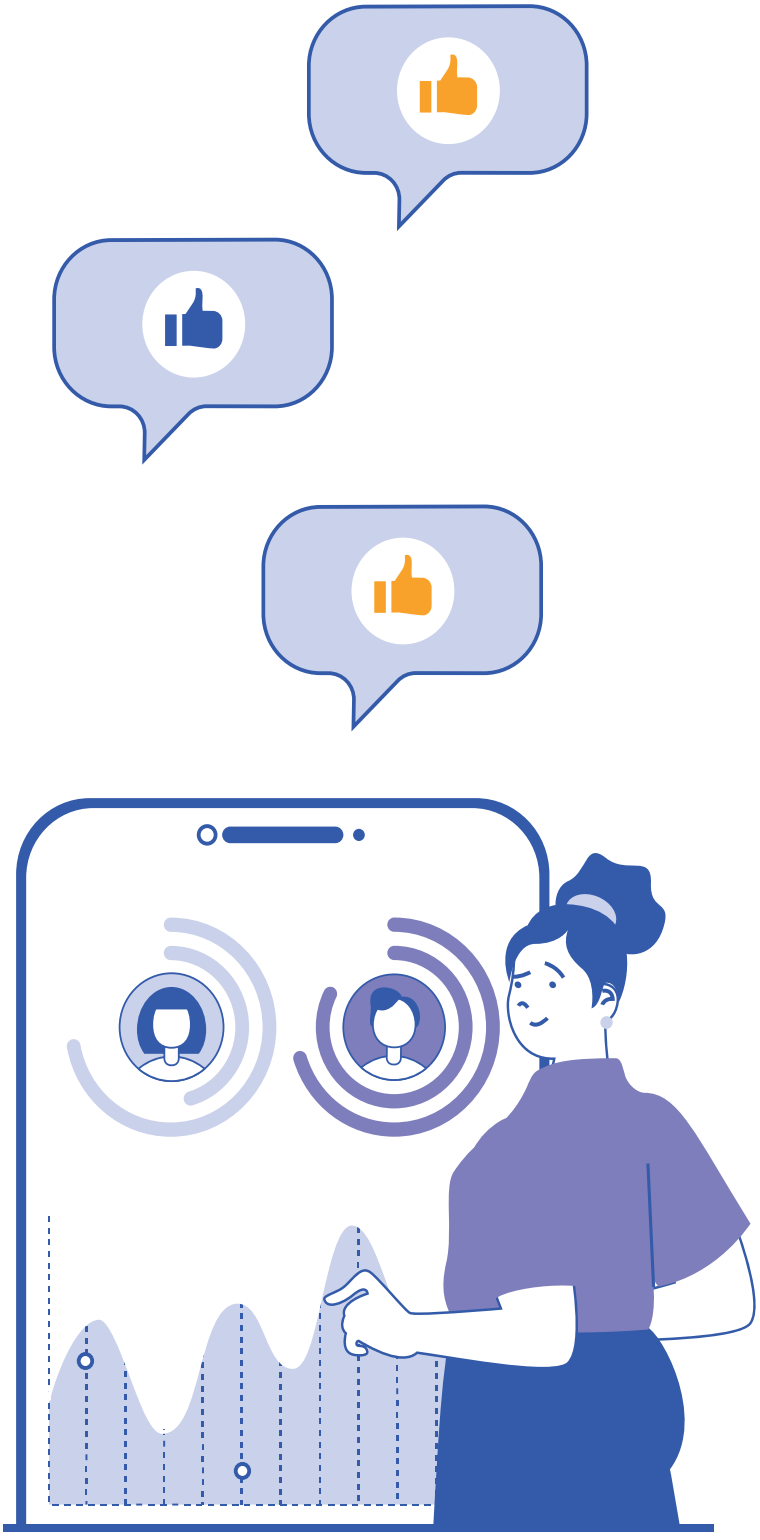
- Implementar proyectos especiales como la creación de nuevos servicios apoyados por fondos de organismos internacionales.

- Buscar fondos nacionales orientados a proyectos de tecnología y ciberseguridad.

- Desarrollar programas, competencias y actividades que tengan por objeto conocer, y como fin reclutar, talento emergente.

- Suscribir convenios internacionales que permitan la capacitación y entrenamiento bidireccional de personal del equipo de respuesta, así como poder compartir información de valor sobre amenazas.

- Generar alianzas estratégicas con la industria nacional, academia y sociedad civil a fin de desarrollar estrategias sectorizadas que cuenten con la capacidad de despliegue y difusión.



"Al principio el CERT Nacional de Colombia - colCERT y el CSIRT de las Fuerzas Militares de Colombia - CCOCI adscritos al Ministerio de Defensa Nacional fue integrado por personal militar y civil al que se capacitó a través de convenios internacionales; posteriormente se desarrolló un plan interno de gestión del conocimiento que permitió fortalecer las capacidades de los funcionarios de la entidad"

Colombia
colCERT, CSIRT de Fuerzas MIlitares - CCOCI

"Con el entendido de que la mejor fórmula para dar resultados es tener la información más el poder de acción, el CSIRT realizó eventos en las universidades para reclutar alumnos que cursaban los últimos semestres y tenían flexibilidad para trabajar y terminar su tesis. Incluso se propuso que hicieran su tesis de algo relevante para el CSIRT"

Chile
CSIRT-CL Nacional

"En la primera fase del CSIRT se reclutaban alumnos, ofreciendo ventajas como trabajo remoto, para tener un diferenciador entre otros empleos"

Argentina
CERT.ar, CSIRT Nacional

4. UN CSIRT COMO UN **MODELO DE NEGOCIO**

Como se ha indicado, la gestión de incidentes cibernéticos va mucho más allá de un procedimiento técnico. La región cuenta con muchos casos de éxito de creación de CSIRTs, pero también casos en donde el CSIRT solo queda en papel y no ve la luz.

Por ello, **antes de la puesta en marcha de un CSIRT es importante planearlo y diseñarlo con una visión de largo plazo y crecimiento sostenido.** Esta visión permitirá identificar los elementos clave para cumplir con los objetivos del CSIRT, así como **contar con indicadores claros y medibles que al cumplirse demuestren la efectividad del CSIRT y justifiquen su existencia.**

En otras palabras, una buena práctica al momento de crear un CSIRT es formarlo como un modelo de negocio ajustado a las oportunidades y limitaciones cambiantes, teniendo presente que no necesariamente va a generar rentabilidad monetaria, pero sí será un diferenciador al contribuir a tener sistemas más seguros, mayor confianza de la ciudadanía y minimización de impactos de gravedad ante incidentes cibernéticos. Es por ello que esta guía aborda la creación de un CSIRT desde la concepción de un modelo de negocio, haciendo uso de un modelo CANVAS.

Esta sección ha sido inspirada en la guía *"Getting started with a National CSIRT"*[9] que presenta un modelo de negocio para un CSIRT (Global Forum on Cyber Expertise, GFCE. Mayo, 2021).

[9]Getting Started with a national CSIRT. Cybersecurity Capacity Building – Global Forum on Cyber Expertise (GCFE), 2021. https://cybilportal.org/wp-content/uploads/2021/06/TNO-2021-Getting_started_with_a_national_CSIRT_FINAL.pdf

4.1 Definición del CANVAS

Un modelo de negocio es una herramienta que permite modular, describir y definir la forma en que una organización orquesta elementos y actividades para lograr sus objetivos; es decir, la forma en que se crea y se entrega el valor para el cual fue concebida dicha organización.

Una forma gráfica de representar un modelo de negocio es a través de un CANVAS (Osterwalder-Pigneur, 2010). Esta metodología resulta útil para líderes de proyecto, gerentes y directores para explicar de manera clara el valor y la necesidad de un CSIRT en un contexto dado, a todos los actores relevantes.

A continuación, se muestra un CANVAS que representa el modelo de negocio genérico de un CSIRT nacional, el cual se puede adaptar a necesidades particulares, incluso a un CSIRT sectorial.

Gráfica 5

Modelo CANVAS
para un CSIRT

El CANVAS normalmente tiene un orden para crearlo, así como para leerlo, por lo que se presenta en dicho orden. En este caso, para iniciar el camino del modelo de negocio operativo y estratégico, lo más importante es definir a la comunidad atendida. Al final de este capítulo veremos cómo se comunica el modelo CANVAS.

4.1.1 Segmento de mercado. ¿A quién atiende el CSIRT?

Este elemento del CANVAS describe a la comunidad atendida, elemento fundamental al momento de empezar a planear la creación o actualización de un CSIRT. Esto define a los colectivos, organismos o entidades a las que se le ofrecerán los servicios del CSIRT.

Para el caso de un CSIRT nacional, esa comunidad se forma en primer lugar de entidades públicas del estado, ya que una función primordial es apoyarlos a identificar, prevenir y mitigar incidentes cibernéticos. Entre estas entidades se encuentran los poderes ejecutivo y judicial, las instituciones electorales y las Fuerzas Armadas que deben considerarse como segmentos a los que se atenderá y para quienes se cubrirán necesidades referentes a la propuesta de valor. Pero también debemos tomar en cuenta a las organizaciones públicas y privadas que podrían identificarse como infraestructura crítica.

Un CSIRT sectorial tendría una comunidad más acotada que un CSIRT nacional. Por ejemplo, las Fuerzas Militares de un país podrían conformar un CSIRT sectorial que coordine y preste servicios de gestión de incidentes cibernéticos a sus distintos componentes (Fuerza Aérea, Ejército Nacional, etc.).

Tipos de CSIRTs sectoriales según la comunidad atendida:

- Infraestructuras críticas. Organizaciones públicas y privadas que administran sistemas físicos o virtuales que son considerados vitales para el país, debido a que su incapacitación o destrucción tendría un efecto debilitante en la seguridad económica nacional, la salud, la seguridad pública nacional o cualquier combinación de las anteriores

- Proveedores de Internet (ISP) o *Internet Exchange Points (IXP)*. Organizaciones encargadas de la interconectividad de Internet

- Fuerzas Militares

- Sector Financiero (puede ser coordinado por medio de asociaciones)

- Servicios de salud

- Comercios minoristas o sectores puntuales

- Academia (universidades o instituciones educativas)

- Gobiernos locales o de provincia

- Sociedad civil

- Sectores de la Iniciativa privada

4.1.2 Propuesta de valor. ¿Qué necesidades satisface el CSIRT?

Este elemento es la columna vertebral del modelo, en él se define la propuesta para resolver el problema o la necesidad de la comunidad definida.

Lograr identificar a tiempo un servidor en producción comprometido, recopilar logs para analizar trazas de un ataque de malware, recuperar un servicio en línea, defender un activo crítico de un ataque de denegación de servicio, recibir formación en temas de ciberseguridad, detectar credenciales expuestas o responder a una fuga de información sensible, son algunas de las posibles necesidades que puede presentar una comunidad atendida por un CSIRT.

En este sentido, la comunidad tiene como expectativa contar con un ecosistema que articule procesos, herramientas, personas y servicios que los apoye en la resolución de incidentes cibernéticos.

Por tanto, la propuesta de valor principal que hace un CSIRT a su comunidad atendida es "identificar, prevenir, responder y mitigar incidentes cibernéticos". Asimismo, el CSIRT ofrecerá una serie de servicios que aportarán valor *"asistiendo y asesorando a la comunidad atendida"* en temas de ciberseguridad. Esta propuesta deberá estar alineada al mandato, misión y visión específicos que ese CSIRT tenga definidos.

4.1.3 Canales. ¿Cómo tendrá contacto y entregará los servicios?

En este bloque se define cómo se entregarán los servicios del CSIRT a su comunidad atendida. Este tema es fundamental, ya que el CSIRT es una organización que entra a una dinámica de contacto permanente con distintas organizaciones dentro y fuera de su comunidad atendida. Los canales del CSIRT deben estar siempre disponibles y de fácil acceso para la comunidad.

Los canales representan puentes que habilitan el acercamiento de la comunidad al consumo de los servicios del CSIRT y, por ende, al establecimiento de una red de confianza entre la comunidad y el CSIRT.

Es importante contar con un equilibrio entre la automatización de canales de respuesta y la interacción directa con miembros del CSIRT. Esto siempre es bien recibido por parte de la comunidad, ya que ayuda a estrechar vínculos de confianza con las personas que interactúan en la gestión de un incidente.

No hay que olvidar que la correcta promoción en redes sociales y otros foros, como conferencias especializadas en ciberseguridad, permiten posicionar, referenciar y dar visibilidad al trabajo que realiza el CSIRT. Los canales de atención deben de ser amigables y segmentados de acuerdo con la comunidad.

Cuando un CSIRT se comunica a la población general por medio de redes sociales o conferencias debe procurar un lenguaje simple minimizando el exceso de tecnicismos.

Una estrategia que adoptan los CSIRTs en casos de crisis circunstanciales o de gran repercusión mediática es utilizar un punto único de comunicación a través del uso de una página de estado status page que permite informar, actualizar y mantener el histórico de acciones realizadas en un caso sin comprometer la confidencialidad de la gestión del incidente. Esto permite controlar la distorsión de información falsa, manejo de expectativas de la comunidad y trazabilidad de la información, además garantiza transparencia y mantiene informadas a todas las partes involucradas en un caso.

Es importante definir y publicar el documento RFC 2350 (Expectativas para la respuesta a incidentes de seguridad informática) para presentar a la comunidad atendida las políticas y procedimientos del equipo de respuesta, la colaboración para gestionar incidentes, la relación entre el CSIRT con otros homólogos, los servicios y demás información relevante de la entidad.

Algunas opciones de canales para tomar en cuenta son las siguientes:

- Sitio web
- Sistema de *tickets*
- Lista de distribución/email
- Teléfono
- Sistema de notificación de alertas
- Conferencias y eventos
- Redes sociales
- *Status pages* o páginas de estado
- Plataformas de intercambio de información (por ejemplo, MISP[10])
- Grupos de mensajería y comunicación en medios como WhatsApp, Signal o Telegram

[10] MISP: Malware Information Sharing Platform.

4.1.4 Relaciones. ¿Qué tipo de relacionamiento mantendrá con la comunidad atendida?

La relación deriva de lo que se acuerde en el mandato que tenga el CSIRT. Por lo tanto, el mandato jurídico del CSIRT será fundamental para ajustar la propuesta de valor.

Entre las principales formas para captar a la comunidad atendida y generar lazos que deriven en relaciones de confianza están las siguientes:

- Asistencia y soporte a incidencias
- Asesorías
- Formaciones
- Red de contactos

> “Se realizaron mesas de trabajo directamente con la comunidad atendida para escuchar sus ideas, intereses y dudas. Esto permitió definir de mejor manera los servicios que realmente requería la comunidad”
>
> **Chile**
> **CSIRT-CL Nacional**

4.1.5 Fuentes de ingreso. ¿Cómo conseguir fondos para la operación?

Las fuentes de ingreso es un tema crucial para la sostenibilidad y crecimiento de un Equipo de Respuesta a Incidentes Cibernéticos. Muchos CSIRTs nacionales no monetizan la prestación de sus servicios a la comunidad, por lo que lograr captar atención financiera se vuelve una tarea creativa.

Usualmente, un organismo aloja a un CSIRT y es quien a través de un presupuesto público garantiza el soporte de las operaciones generales del CSIRT y de los empleados que trabajan en él. Sin embargo, para expandir o crear nuevos servicios, según la demanda diaria de la comunidad atendida, se requieren recursos humanos y financieros para su ejecución. Muchas veces estos servicios quedan fuera del radar de los presupuestos fijos asignados por el organismo que aloja al CSIRT.

En este sentido, aparte del presupuesto público existen algunas alternativas para encontrar financiamiento. Se listan a continuación:

- **Fondos de organismos internacionales:**
  - »Apoyos en la creación de nuevos servicios
  - »Capacitación y formación
  - »Obtención de recursos para sostenimiento

- **Consultoría de proyectos (en el caso de estar permitido):**
  - »Brindar servicios específicos remunerados

- **Iniciativas del sector privado:**
  - »Soporte en la formación de la comunidad
  - »Desarrollo de laboratorios

»Servicios pro-bono
»Donación de herramientas
»Invitación a foros y eventos

•Iniciativas con asociaciones civiles:
»Capacitación en herramientas de software libre a sus creadores
»Promoción e invitación a eventos de sus comunidades

•Iniciativas con universidades y centros académicos:
»Capacitación
»Programas de pasantías
»Apoyo con investigadores para casos complejos

•Sector Fuerzas Armadas y agentes de la ley:
»Capacitación
»Programas de apoyo por medio de personal comisionado

En la región se han dado estas alternativas; sin embargo, es importante identificar aquellos organismos o grupos que están disponibles en cada uno de los países fuera de los listados en este documento.

4.1.6 Actividades clave. ¿Qué actividades requiere hacer un CSIRT para cumplir con su propuesta de valor?

En este apartado se definen las actividades para materializar la propuesta de valor. En esencia este bloque constituye el catálogo de servicios a ofrecer; es decir, cada CSIRT revisará las necesidades que desea cubrir y el alcance de éstas (definidas en su propuesta de valor) y, derivado de ello, ofrecerá determinados servicios. Según el marco de servicios del FIRST[11] consideramos:

•Gestión de incidentes cibernéticos

•Análisis de vulnerabilidades

•Análisis situacional de ciberseguridad

•Transferencia de conocimientos

•Gestión de eventos de seguridad

Como se mencionó en el capítulo anterior: “empieza con poco y crece”. En sus primeros años, un CSIRT no debe ni puede operar ni ofrecer todos los servicios que se encuentran en el marco; hacerlo (o intentarlo) es una de las principales causas de la insostenibilidad de un CSIRT, ya que cada uno de los servicios listados implica costos operativos y recursos humanos

[11] FIRST CSIRT Services Framework version 2.1. FIRST, 2019. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Framework_v2.1.0_bugfix1.pdf

que muchas veces no pueden ser costeados por presupuestos públicos asignados a un CSIRT recién creado.

Por lo tanto, **una buena práctica es empezar con servicios fundamentales, de alto impacto y alcance, para la comunidad atendida.** Como se explicó con anterioridad, uno de ellos es el servicio de gestión de incidentes cibernéticos, que es el corazón de un CSIRT. Por otro lado, un servicio de fácil operación y entendimiento es la distribución de alertas a la comunidad a través de la comunicación de reportes y recomendaciones sobre situaciones que pueden o están afectando los recursos tecnológicos de una organización atendida. En este mismo orden, la generación de campañas de concientización y organización de entrenamientos son formas que acercan al CSIRT a la comunidad y generan vínculos de confianza al inicio de las operaciones.

Seleccionar cómo se ofrecerán los servicios es tan importante como los servicios mismos. Es importante contar con esquemas de turnos y guardias (turnos especiales en los que se está al pendiente de cualquier eventualidad) para cubrir y mantener un nivel de servicio adecuado las 24 horas del día, los 7 días de la semana. Ofrecer un servicio defectuoso, o aquel para el que no se tiene la capacidad, generará una pérdida de confianza que perjudicaría al CSIRT.

Como se mencionó anteriormente, un aspecto que es interesante destacar es que la descripción y en especial el alcance de los servicios tienen que estar muy bien definidos. Se debe saber cuáles aspectos cubre y cuáles no, ya que una definición incorrecta en el alcance puede generar falsa sensación de seguridad.

Cuando hablamos de valor hay diferentes formas de ofrecerlo a través de los servicios, una de ellas es proporcionar alertas sobre vulnerabilidades existentes o indicadores de compromiso (IOC). Otro servicio de valor podría ser proporcionar capacitación a la comunidad atendida sobre cómo hacer uso de la información que se envía constantemente; esto puede resultar del análisis de la madurez de la comunidad atendida.

Una idea que compartieron especialistas de la región (CSIRT-CL en Chile y TT-CSIRT en Trinidad y Tobago) es centrarse en generar la confianza necesaria para intercambiar capacitaciones o alertas que normalmente no son accesibles de forma pública, para así posicionar la marca CSIRT. A la vez, se recomienda realizar convenios con empresas de diferentes sectores para distribuir los contenidos. Este accionar permitió informar de primera mano y generar un valor para aquellos que recibían la información. Al final, propició que fueran las mismas empresas las que reportaran directamente los incidentes al sistema de *tickets.*

4.1.7 Recursos Clave. ¿Qué recursos son necesarios para desarrollar la propuesta de valor?

En este bloque se listan aquellos recursos que son fundamentales para que el CSIRT produzca, entregue y gestione los servicios y otras actividades fundamentales. Los recursos planteados son los indispensables para llevar a cabo los servicios descritos en el bloque anterior:

•**Recursos organizacionales.** Agrupan lo necesario para que el CSIRT opere tales como lugar físico, mobiliario, líneas telefónicas, servidores, automóviles oficiales de desplazamiento, servicios generales, instalaciones especiales (war room[12]), salas de juntas, organigramas, procesos y procedimientos descritos.

•**Información accionable.** Es la información que puede ser usada sin realizar un procesamiento mayor adicional para comunicar o validar dicha información. En este sentido, según la Agencia de la Unión Europea para la Ciberseguridad (ENISA[13]) , este tipo de información debe presentar relevancia, oportunidad, precisión, integridad y digestibilidad que ayuden al CSIRT a la toma de acciones para identificar, prevenir, responder y mitigar incidentes cibernéticos. Estos pueden ser, por ejemplo, feeds[14] de ciberinteligencia, inteligencia de amenazas, indicadores de compromiso indicadores de ataque e incluso información obtenida directamente de la comunidad.

> “La inteligencia de amenazas no se trata únicamente de implementar herramientas para la ingesta de feeds. Las herramientas no son más que aplicaciones y un par de líneas de código. Se trata de una filosofía, una metodología, una operación de prevención y respuesta basada en el consumo, procesamiento y análisis de los datos”
>
> **República Dominicana**
> **CSIRT-RD, CSIRT nacional**

Indicadores de compromiso	•Direcciones IP’s, nombres de dominio, URL’s •Hashes o valores de integridad, entradas de registro vinculadas a un código malicioso •Nombres y ubicaciones de archivos
Alertas	•Vulnerabilidades •Actualizaciones •Exploits[15] •Patrones de comportamiento •Alertas internacionales

[12] War room: Espacio para reunir a los tomadores de decisiones del Equipo a Respuesta a Incidentes que permite coordinar de mejor manera al equipo. A veces se le conoce como Salas de Situación, Salas de Control o Centro de Comando.
[13] European Union Agency for Cybersecurity (ENISA), 2023. https://www.enisa.europa.eu/
[14] Contenido que puede exportarse a otros sitios también conocidos como flujos de datos.
[15] Exploit: Programa de software o código que aprovecha una vulnerabilidad en una aplicación o sistema informático.

•**Herramientas.** Agrupan la tecnología necesaria para apoyar la propuesta de valor, los canales y las relaciones con las organizaciones de la comunidad atendida. Un ejemplo es un sistema de tickets a través del cual se puedan atender peticiones y reportes. También todo el set de herramientas orientadas a la prevención, detección y resolución de incidentes cibernéticos, servicio telefónico y de correo electrónico. Los CSIRTs pueden optar por tener un balance entre soluciones de código abierto y propietarias para soportar sus servicios, teniendo en cuenta los presupuestos (en muchos casos anual) que implica cada una de ellas para mantenerlas actualizadas.

•**Recursos humanos.** Constituyen el recurso más importante de este bloque. Sin talento no hay prestación de servicios ni mucho menos construcción de lazos de confianza. Por lo tanto, es el recurso más valioso dentro de un equipo. Son distintos los perfiles que se necesitan para formar el equipo. En los reportes del GFCE[16], FIRST[17] y ENISA[18] podrán encontrar los perfiles adecuados para conformar un CSIRT.

A pesar de que los roles técnicos son fundamentales dentro de un equipo, cada día toma más relevancia contar con especialistas de comunicaciones en ciberseguridad. El incremento de los incidentes cibernéticos y su impacto directo en la afectación de servicios esenciales de los ciudadanos demandan información oportuna digerible por parte de los ciudadanos. Ataques que afectan sistemas bancarios, entidades de identificación y servicios de salud se convierten rápidamente en crisis que demanda información centralizada, oportuna y adaptada a cada tipo de comunidad. Además, estos perfiles pudieran apoyar al equipo técnico en la socialización de la comprensión de los beneficios ofrecidos por un CSIRT.

[16] Getting Started with a national CSIRT. Cybersecurity Capacity Building – Global Forum on Cyber Expertise (GCFE), 2021. https://cybilportal.org/wp-content/uploads/2021/06/TNO-2021-Getting_started_with_a_national_CSIRT_FINAL.pdf

[17] CSIRT Roles and Competences (Addendum). FIRST, 2023. https://www.first.org/standards/frameworks/csirts/FIRST_CSIRT_Services_Roles_and_Competencies_v_0.9.0.pdf

[18] How to set up CSIRT and SOC. ENISA, 2020. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

4.1.8 Asociaciones clave. ¿Quiénes son los socios o proveedores clave?

La respuesta abarca a los socios, proveedores o entidades que juegan un rol estratégico o contribuyen de forma significativa para que un CSIRT funcione de manera adecuada. Algunos de los proveedores o socios clave de un CSIRT nacional son:

•**Proveedores de internet (ISPs).** Son quienes pueden apoyar con información y, en algunos casos, ante algunos incidentes cibernéticos. Un claro ejemplo es la contención de ataques de denegación de servicios distribuidos donde una relación de confianza entre un ISP y el CSIRT permite la ejecución inmediata de acciones de bloqueos y contención. Otro ejemplo común es la realización de operativos de ciberhigiene en dispositivos del Internet de las Cosas infectados bajo el segmento de un ISP. Esta es una clara relación que permite generar valor bidireccional.

•**Fuerzas del orden.** Los CSIRTs y las fuerzas del orden deben tener una comunicación fluida y permanente por la estrecha relación entre los incidentes cibernéticos y los casos de cibercrimen que propician un terreno común de colaboración e intercambio de información constante entre estas organizaciones. Un CSIRT puede mantener actualizados a los cuerpos del orden sobre las últimas técnicas y patrones de compromiso de cuentas de correos electrónico de interés o de acceso a paneles administrativos de infraestructuras virtuales expuestas en internet, que quizás pudieran facilitar la resolución de un caso de cibercrimen en el que estén actuando los organismos de la ley, por ejemplo. Una iniciativa de colaboración entre un CSIRT nacional con fuerzas militares es la realización de ejercicios de simulación en conjunto para medir las capacidades de respuesta ante incidentes cibernéticos de un país o región.

•**Poder legislativo.** Es un cliente potencial del CSIRT y, a la vez, un referente para la promoción de aspectos legislativos relacionados a la ciberseguridad. Por ejemplo, un CSIRT nacional puede suministrar indicadores del número de sistemas comprometidos de gobierno que pudieran impulsar instrumentos legislativos para el robustecimiento y monitoreo de sistemas de alta criticidad, incluyendo la adopción de mecanismos de doble factor de autenticación, limitación de cuentas administrativas, etc.

•**Poder judicial.** Alguna atención de incidentes cibernéticos puede requerir la intervención del poder judicial. En esos casos los CSIRTs podrían actuar como colaboradores activos en procesos judiciales que requieren el testimonio de un experto en materia de ciberseguridad.

•**Organizaciones internacionales.** Los organismos internacionales juegan un rol clave en la operatividad de un CSIRT. La relación podría darse de varias formas, entre ellas:

»Coordinación regional.
Organismos internacionales pueden apoyar la coordinación de incidentes cibernéticos que requieran apoyo regional o de contactos internacionales. Un ejemplo de referencia regional es la Red CSIRTAmericas, red hemisférica de Equipos de Respuesta ante Incidentes Cibernéticos (CSIRTs) gubernamentales de los estados miembros de la Organización de Estados Americanos (OEA) que actúa como el impulsor principal del Programa de Ciberseguridad del CICTE/OEA en el fortalecimiento de las capacidades de respuestas ante incidentes

cibernéticos de la región de la OEA y sirve de plataforma para el intercambio de información sobre amenazas cibernéticas 24/7; brinda programas de asistencia técnica y ofrece oportunidades de desarrollo profesional a sus miembros.

»Fondos de proyectos.
Los CSIRTs pueden elevar proyectos de creación de nuevos servicios, programas de capacitación o programas de concientización de gran impacto a organizaciones internacionales para explorar opciones de financiamiento.

»Capacitaciones y eventos.
Los miembros de un CSIRT pueden verse beneficiados por los entrenamientos y eventos de ciberseguridad organizados por organismos internacionales que permiten formar a los especialistas del equipo y también visibilizar las iniciativas trabajadas por un CSIRT.

•**Universidades e instituciones de educación superior.** La asociación con universidades es estratégica debido a que un problema que suele enfrentar un CSIRT es la escasez de recursos con perfiles adecuados que tengan la formación básica para ejecutar actividades dentro de un CSIRT. Con la universidad se pueden establecer relaciones que permitan capacitar desde las aulas a los alumnos que pudieran ser invitados a formar parte de la plantilla laboral del CSIRT, a través de programas como *Creando una trayectoria profesional en ciberseguridad*, iniciativa impulsada por la OEA con el apoyo de *CITI Foundation* que busca entrenar e inspirar a jóvenes talentosos con el fin de consolidar una fuerza laboral regional. Este programa tiene un componente que relaciona directamente a las universidades y otras instituciones de educación superior con los CSIRTs brindando oportunidades a estudiantes de la región para crear soluciones a CSIRTs miembros de la red CSIRTAmericas.

El sector académico también puede colaborar con un CSIRT nacional en la preparación e impartición de entrenamientos de interés para la comunidad atendida, así como colaborar en investigaciones de incidentes cibernéticos de alta complejidad.

•**Empresas privadas de ciberseguridad.** Las empresas privadas tienen interacción con un CSIRT de varias maneras. Las más comunes son a través de:

»La provisión de equipamiento, licencias o soluciones tecnológicas que soporten los servicios brindados por el CSIRT.

»El establecimiento de convenios y mecanismos para el reporte de alertas o incidentes cibernéticos detectados por empresas privadas que afectan la comunidad atendida por el CSIRT.

»La organización de entrenamientos y programas de desarrollo de capacidades en ciberseguridad de interés para la comunidad atendida.

»Tercerizar la contratación de talento humano en caso de ser necesario.

Es importante recordar que en el caso de CSIRT Nacionales se debe contar con un marco legal que habilite este accionar como lo son contar con Memorandum de Entendimientos (MoU).

•**Asociaciones civiles.** Las organizaciones civiles promueven e influyen en la generación de una cultura de ciberseguridad en una región o sector. Un CSIRT y las asociaciones civiles pueden trabajar cercanamente en proyectos como:

»Organización y promoción de entrenamientos en ciberseguridad de interés para la comunidad atendida.

»Explorar la creación de programas de *bug bounty*[19] para el reporte de vulnerabilidades asociadas a organizaciones de la comunidad atendida.

»Facilitar la ubicación de expertos en temas especializados de ciberseguridad que pudieran apoyar la resolución de algún caso particular de incidente cibernético.

»Participación en ejercicios de simulación organizados por el CSIRT.

•**Otros CSIRT.** La naturaleza de un CSIRT es proveer asistencia técnica y realizar acciones de coordinación multisectorial. Por eso es importante consolidar acuerdos de colaboración e intercambio de información con otros CSIRTs a nivel nacional e internacional. La colaboración podrá beneficiarse de la asistencia mutua en casos de incidentes cibernéticos, apoyo con experticia, intercambio de información accionable, integración de soluciones para la detección y mitigación de incidentes cibernéticos e intercambio de experiencias y buenas prácticas.

4.1.9 Estructura de costos. ¿Qué partida de gastos debe tener en cuenta un CSIRT?

Este bloque nos ayuda a definir gastos e inversiones necesarias para operar un CSIRT. Cabe mencionar que, si en algún punto el equipo decide crecer para ofrecer nuevos servicios, o si amplía su propuesta de valor será necesario replantear el CANVAS antes de revisar la estructura de costos, la cual puede segregarse en diferentes categorías como costos fijos y costos variables. Algunos costos asociados son:

•**CapEX (Gastos en capital).** Se debe considerar la inversión en recursos materiales como oficina y su equipamiento, compra de servidores y otras inversiones en capital de activo no corriente. Se debe tener en cuenta tanto inversiones nuevas necesarias para crecer los servicios, como aquellos gastos para la actualización o mejora de equipo y oficinas.

•**Opex (Gastos de operación).** Considera las siguientes opciones:

»Infraestructura tecnológica.
Se mencionó en el bloque de recursos clave la importancia de este punto que soporta la operación y la prestación de servicios del CSIRT.

»Licencias de Inteligencia de Ciberamenazas (CTI, por sus siglas en inglés).
Las licencias para la obtención de *feeds* (flujos de datos) son clave para la operación de un CSIRT, ya que proveen información real accionable

[19] Programa que permite que "hackers éticos" accedan a la seguridad técnica de una plataforma tecnológica (web o móvil) para descubrir fallas o vulnerabilidades a cambio de una remuneración dependiendo de la gravedad de lo encontrado.

sobre posibles amenazas a infraestructuras tecnológicas de la comunidad atendida. En concreto, pueden contener información sobre infraestructuras críticas expuestas a internet, correos electrónicos comprometidos, credenciales expuestas y fugas de información sensible, entre otros. Tomando como referencia el ejemplo anterior, la información compartida a través de la *Red CSIRTAmericas* permite a los CSIRTs miembros identificar amenazas que podrían afectar la seguridad de las organizaciones, las infraestructuras críticas y la ciudadanía de su país, lo que constituye el primer paso para prepararse y defenderse de los ataques. Es decir, a través de la obtención (sin costo) de grandes volúmenes de datos de ciberinteligencia el CSIRT puede identificar, gestionar y notificar directamente a instituciones gubernamentales afectadas por un ciberataque, lo que fortalece directamente su servicio de Gestión de Eventos de Seguridad de la Información.

»Recursos humanos y administrativos.
Este rubro puede consumir un porcentaje alto de la estructura de gastos de operación, tanto en salarios como en las capacitaciones constantes del personal. También deben incluirse gastos operativos por esquemas de trabajo fuera de horario, transporte, hospedaje y otros gastos recurrentes. No podemos olvidar que en todos los casos la capacitación constante para el recurso humano no puede ser obtenida sólo por donaciones o invitaciones.

»Membresía a foros internacionales de seguridad.
Son costos asociados que tienen como finalidad que representantes del CSIRT puedan tener acceso a una serie de recursos como asistencia técnica y planes de formación para el equipo.

4.2 ¿Cómo comunicar el modelo de negocio de un CSIRT de forma eficiente?

Comunicar de forma eficiente y acertada un CANVAS es tan importante como su propia definición y diseño de sus componentes. Por ello el CANVAS tiene una estructura definida para su lectura que recomienda una técnica de contar una historia para explicar y transmitir el modelo de forma atractiva; esto es, contar la historia a través de la perspectiva de la comunidad atendida, sus problemas y necesidades. Se puede realizar de la siguiente forma:

1. La comunidad atendida es la protagonista de la historia. Se debe hablar de los retos que enfrenta y las labores que debe llevar a cabo haciendo énfasis en los aspectos donde el CSIRT será relevante.

2. Posteriormente se debe explicar cómo el CSIRT crea valor para esta comunidad y describir sus servicios, enfatizando en cómo cada servicio responde a una necesidad específica de la comunidad. Como parte de la historia, también debe contarse qué recursos y actividades sostendrá la puesta en valor del CSIRT.

Como se mencionó anteriormente, esta metodología sirve a líderes de proyecto, gerentes y directores en su misión de explicar de manera simple y cercana el valor necesario de un CSIRT ante todos los actores relevantes.

5. CLAVES PARA TENER UN CSIRT EFICIENTE

Esta sección intenta presentar de manera simple y concreta las experiencias y consejos de los autores de este documento y de los especialistas entrevistados según categorías específicas, y no pretende expresar las consideraciones técnicas para el funcionamiento y operaciones de un CSIRT.

Mandato

•Es importante mantenerse dentro de las funciones y lineamientos descritos en el mandato oficial del CSIRT. A medida que un CSIRT se da a conocer por su trabajo, en muchas en ocasiones son consultados para situaciones de apoyo fuera de su mandato. El CSIRT debe canalizar esas peticiones a las instancias correspondientes.

•Será importante gestionar las expectativas de la alta gerencia y comunidad atendida al inicio de la operación del CSIRT. Contar con un CSIRT no significa que los incidentes cibernéticos desaparecerán al día siguiente de arrancar, implica que se someterán a un proceso de gestión formal.

•Definir la normatividad a la que el CSIRT debe ajustarse. Documentar procedimientos, procesos y responsabilidades.

Recursos humanos

•En caso de tener un pequeño *pool* de especialistas, se recomienda asignar varios roles dentro del CSIRT; también rotar sus posiciones en los diversos departamentos.

•Es necesario interactuar con universidades para concretar iniciativas para la captación de talento humano y estructurar programas de formación.

•Se deben implementar políticas de flexibilidad laboral que ayuden a mitigar la rotación de personal.

•Es importante aprovechar los programas de formación que ofrecen los organismos internacionales, pero con la condición de que quienes acudan a la capacitación regresen al CSIRT a documentar y transmitir el conocimiento.

•Se requiere formar al personal en el manejo de comunicaciones en escenarios públicos o de prensa.

•Es importante documentar los procesos para que la curva de aprendizaje entre los nuevos miembros del grupo sea menor.

LA CURVA DE APRENDIZAJE DE UN NUEVO RECURSO HUMANO PUEDE SER LARGA; DOCUMENTAR LOS PROCEDIMIENTOS AYUDA A TENER EFICACIA EN LA OPERACIÓN.

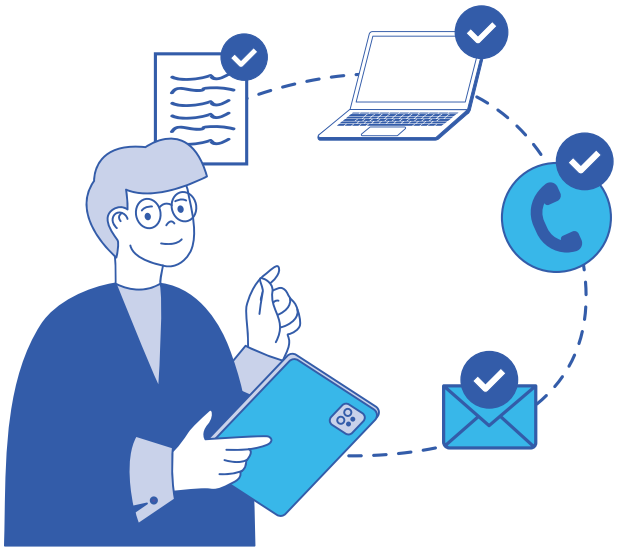
Servicios

•Empezar con el servicio principal de un CSIRT: la gestión de incidentes cibernéticos y luego agregar servicios que tengan un beneficio amplio en toda la comunidad y sean simples de operar.

•Al diseñar y ofrecer un nuevo servicio a la comunidad es necesario pensar primero en la posible utilidad para la comunidad. Los servicios deben mantenerse simples y evitar que sean una alta carga adicional a los usuarios de la comunidad.

•Para la implementación de las herramientas tecnológicas esenciales de un CSIRT (página web, lista de distribución, herramienta de gestión de tickets, correo electrónico, línea telefónica) se pueden apoyar en tecnologías open-source que ayudarían a priorizar y orientar los costos, así como al fortalecimiento de los servicios que ofrecen; la elección entre herramientas open-source o de desarrollo propio dependerá de presupuestos, necesidades y recursos disponibles del equipo.

•Al momento de lanzar un nuevo servicio, debe siempre tenerse en cuenta que cada CSIRT es diferente y debe priorizar aquellos servicios que generen mayor valor a su propia comunidad atendida, que dependerá de la demanda, el contexto nacional, la habilitación legal y el nivel de madurez, entre otros factores.



GENERO VALOR AGREGADO A QUIEN ME NOTIFICA UN INCIDENTE SI UTILIZO LA VÍA TÉCNICA, LA COMUNICACIÓN, ASESORÍA LEGAL Y UNA ESTRATEGIA DE PREVENCIÓN. CON ESTO EL CSIRT NO SOLO RESPONDE, TAMBIÉN ACOMPAÑA.

Comunidad

•Un error común es medir la cantidad de tickets que se reciben y atienden, generando la percepción de que más personas de la comunidad conocen al CSIRT; tener más tickets no significa que se está realizando mejor el trabajo.

•Es necesario que la comunidad reconozca el trabajo y realmente vea valor en los servicios que provee el CSIRT. Esto se logra al hacer del conocimiento de la comunidad las tareas

y servicios que han apoyado o ayudado a miembros de la comunidad.

•Se tiene que vender al CSIRT; tener visibilidad y comunicar lo que hace genera confianza y permite acercamientos a la comunidad, por lo tanto, se debe involucrar a la comunidad en lo que hace el CSIRT.

•Hay que tener presente que muchas veces un CSIRT puede generar gran impacto con servicios simples (noticias, alertas, boletines, campañas de prevención).

ENTRE LOS FACTORES CLAVES PARA EL ÉXITO SOSTENIDO DEL CSIRT EN LA COMUNIDAD ESTÁN LA INTEGRACIÓN (POR EJEMPLO, COMPARTIR INDICADORES DE COMPROMISO) Y LA CONFIANZA, TANTO PARA REPORTAR COMO PARA ESTAR ATENTO A LO QUE SE PUEDE DIFUNDIR.

Presupuesto

•Siempre se deben considerar escenarios donde se requiera algo de urgencia o no contemplado.

•Hacer que los tomadores de decisiones entiendan que el presupuesto puede cambiar con el paso del tiempo para poder ofrecer cada vez más servicios a la comunidad.

•Cada determinado tiempo, además de revisar el presupuesto, es necesario checar la forma en que se están usando las herramientas para identificar posibles cambios en productos y así eficientizar dicho presupuesto.

EL PRINCIPAL RIESGO DE UN CSIRT ES HACER SOSTENIBLE LA OPERACIÓN, PRINCIPALMENTE POR LOS RECURSOS ECONÓMICOS, POR ESO SE RECOMIENDA NO INICIAR CON UNA INVERSIÓN CUANTIOSA O HACERSE DEPENDIENTE DEL LICENCIAMIENTO O PLATAFORMAS QUE REQUIERAN OBLIGATORIAMENTE UNA RENOVACIÓN O UNA FUERTE INVERSIÓN.

Apoyo político

•Entregar resultados medibles y que demuestren la razón por la cual el CSIRT otorga valor a la comunidad.

•Tomar decisiones basadas en datos, reportes, cuadros de mando e información relevante.

•La confianza en la comunidad permitirá que los tomadores de decisiones tengan más herramientas para mantener la continuidad del CSIRT.

•Aliarse con organizaciones internacionales tiene beneficios como incrementar funcionalidades y servicios del CSIRT sin necesidad de una inversión adicional.

Comunicación

•El CSIRT debe ser capaz de articular, negociar y definir con organismos distintos temas relacionados con su misión; esto requiere involucrar a los tomadores de decisiones en el modelo de negocio que se ha presentado para lograr éxitos visibles para el CSIRT.

•Establecer un área, responsable y plan de comunicación o prensa para notificar incidentes de carácter mediático o de conocimiento público.

•Definir canales de comunicación y estrategias según los interlocutores. Por ejemplo, al comunicarse con el público general el lenguaje debe ser simple y cercano, mientras que al hablar con un público técnico el lenguaje debe ser preciso, confiable y accionable.

6. EL CSIRT DEL **FUTURO**

El CSIRT de hace una o dos décadas era un equipo que giraba en un nicho puramente técnico. Los incidentes cibernéticos, en su mayoría, se atendían a partir del reporte de una organización afectada. Actualmente, la diversidad de plataformas y el aumento explosivo de servicios expuestos a Internet que forman parte de la vida diaria de la sociedad ha hecho que los CSIRTs transiten de un enfoque técnico a un enfoque integral alineado a los objetivos sociales, económicos, tecnológicos y ambientales de un país.

ES POR ELLO QUE LOS CSIRTS EN LA REGIÓN DEBEN CONSTRUIR LOS SERVICIOS OFRECIDOS A LA COMUNIDAD ALINEADOS A LAS POLÍTICAS PÚBLICAS DE UN PAÍS O DE UN SECTOR. EN ESTE SENTIDO, EL CSIRT DE LOS PRÓXIMOS AÑOS PODRÍA:

1. Ser el coordinador nacional de una plataforma de intercambio de indicadores de compromiso entre su comunidad y otros CSIRTs sectoriales.

2. Identificar al usuario final como eje central en el diseño y desarrollo de servicios.

3. Lograr que los usuarios tengan un entendimiento (dependiendo de su contexto) del impacto y beneficio que tiene el trabajo de un CSIRT.

4. Tener un enfoque de datos en las operaciones o toma de decisiones basado en la interpretación y análisis. Es imperativo que un CSIRT se alimente de información accionable en cada uno de los servicios que ofrece a la comunidad. Un CSIRT con información accionable y oportuna podrá aumentar su capacidad de respuesta y resiliencia.

5. Involucrarse como colaborador activo en la creación, ejecución y actualización de las estrategias nacionales de ciberseguridad, de Gobernanza y Transformación Digital, y políticas públicas que beneficien a todo el ecosistema. Un CSIRT colecta y centraliza información sobre patrones de ataques, sectores más afectados y capacidad de respuesta de instituciones que es vital para la priorización de lineamientos a nivel nacional o sectorial.

6. Desarrollar capacidades de respuesta a incidentes a nivel nacional, incluyendo a todos los sectores.

7. Orientar los procesos y procedimientos a metodologías ágiles que permitan mejorar los tiempos de respuesta en la atención de incidentes cibernéticos.

8. Desarrollar alianzas flexibles con organizaciones aliadas para, por ejemplo, contar con mecanismos de intercambio de inteligencia de amenazas cibernéticas y consecución de acciones de respuesta con proveedores de servicios de internet (ISPs), reguladores o autoridades gubernamentales.

9. Involucrarse en la creación de servicios que permitan identificar los riesgos antes de su desarrollo y aplicación. El relacionamiento temprano genera más y mejores beneficios para el CSIRT y la comunidad que atiende.

10. Buscar alternativas laborales para los especialistas para evitar la rotación de personal con el objetivo de fortalecer la sostenibilidad de las operaciones del CSIRT.

11. Aprovechar el momento exponencial que existe en cuanto a nueva tecnología y nuevos modelos para reaccionar ante incidentes.

12. Desarrollar capacidades de comunicación no solo de forma interna y hacia los tomadores de decisiones, sino también hacia la comunidad para desarrollar la confianza.

13. Ser líderes en el sector, logrando el reconocimiento con base en los resultados.

14. Generar y gestionar procesos sólidos que puedan ser auditados.

7. CONCLUSIONES

Los CSIRT enfrentan retos que varían según diferentes circunstancias en tiempos y espacios determinados, pero todos tienen en común un único objetivo: velar por la seguridad de su comunidad atendida. Es por eso por lo que existen consejos, recomendaciones y mejores prácticas que sirven en todos los ámbitos y que se describen en este documento.

El enfoque de modelo de negocios puede permitir a un CSIRT ser creado desde su concepción de manera sostenible y eficiente. Para ello es fundamental definir claramente dónde se ubicará y cuáles serán los servicios que le darán el mejor valor a la comunidad atendida. Sin embargo, siempre se debe tener presente la posibilidad de parar, revisar y replantear actividades, servicios o formas con las que opera un CSIRT ya establecido.

El eje fundamental que siempre debe estar presente es la confianza, la cual es el recurso clave para asegurar las operaciones de un CSIRT y permitir la sustentabilidad y el desarrollo necesario que se sustenta en 10 puntos que son los fundamentos para el CSIRT del futuro.

Es importante recordar que nos encontramos dentro de marcos democráticos de acción por lo que los CSIRT deben actuar apegados a las normativas y recordando el accionar en el contexto de derechos humanos.

Por último, es fundamental destacar que los CSIRT son parte de un ecosistema a nivel de los países donde conviven otras instituciones con diferentes competencias, por lo que tener claro alcance y acciones de cada uno es fundamental para las diferentes acciones y para apoyarse entre todas.

Tabla 2

10 Fundamentos para la creación de un CSIRT

1 ORIGEN Y ESTRUCTURA	2 NECESIDAD	3 COMUNIDAD ATENDIDA	4 RECURSOS HUMANOS	5 MODELO DE NEGOCIOS
Un CSIRT brinda servicios de ciberseguridad para prevenir, detectar, mitigar y responder a incidentes cibernéticos en una comunidad definida. Cuenta con una estructura organizativa con procesos establecidos y un catálogo de herramientas tecnológicas, además de un presupuesto, mandatos, catálogo de servicios, personal especializado, red de contactos y plan de comunicaciones.	Tanto organismos públicos como empresas privadas, entidades militares, academia y otras organizaciones que se consideran infraestructuras críticas se enfrentan a incidentes cibernéticos y, en muchos casos, no cuentan con procedimientos formales para responder a un incidente y, en otros, con una orientación clara de cómo abordar un incidente. Ante este escenario es necesario un CSIRT.	La comunidad atendida son los colectivos, organismos o entidades a las que se le ofrecerán los servicios del CSIRT. Definirla es fundamental al momento de empezar a planear la creación de un CSIRT o al actualizarlo. Entre las principales formas para captar a la comunidad atendida y generar lazos que deriven en relaciones de confianza están: asistencia y soporte a incidencias; asesorías; formaciones; y red de contactos.	Algunas acciones estratégicas son: Reclutar personal con habilidades blandas más que técnicas; es decir, personas con pensamiento crítico, analíticas, orientadas al riesgo o con mente estratégica, ya que es más difícil desarrollar las capacidades blandas que enseñar las técnicas. No centralizar las responsabilidades en un único recurso. Crear compromiso y sentido de pertenencia. Realizar acuerdos con empresas privadas para la formación del personal que labora en el CSIRT.	Antes de la puesta en marcha de un CSIRT es importante planearlo y diseñarlo con una visión de largo plazo y crecimiento sostenido. Esta visión permitirá identificar los elementos clave para cumplir con los objetivos del CSIRT, así como contar con indicadores claros y medibles que al cumplirse demuestren la efectividad del CSIRT y justifiquen su existencia. Es importante, tener presente que no necesariamente va a generar rentabilidad monetaria, pero sí será un diferenciador al contribuir a la minimización de impactos de gravedad ante incidentes cibernéticos.
6 ACTIVIDADES	**7 FINANCIAMIENTO**	**8 RECURSOS CLAVE**	**9 ELEMENTOS DE VALOR**	**10 COMUNICAR**
"Piensa en grande, empieza con poco y crece". En sus primeros años, un CSIRT no debe ni puede operar ni ofrecer muchos servicios pues hacerlo (o intentarlo) es una de las principales causas de su insostenibilidad, ya que cada uno de los servicios listados implica costos operativos y recursos humanos ante presupuestos públicos limitados. Se puede iniciar con: servicios fundamentales, de alto impacto y alcance, para la comunidad atendida como proporcionar alertas sobre vulnerabilidades existentes, indicadores de compromiso (IOC) o publicación de guías de buenas prácticas.	Muchos CSIRTs nacionales no monetizan la prestación de sus servicios a la comunidad, por lo que lograr captar atención financiera se vuelve una tarea creativa. Usualmente, un organismo aloja a un CSIRT y es quien a través de un presupuesto público garantiza el soporte de las operaciones generales del CSIRT y de los empleados que trabajan en él. Sin embargo, para expandir o crear nuevos servicios, existen algunas alternativas para encontrar financiamiento como: Fondos de organismos internacionales; consultoría de proyectos (en el caso de estar permitido); iniciativas del sector privado, entre otros.	Son los recursos indispensables para que el CSIRT produzca, entregue y gestione los servicios y otras actividades fundamentales. Los indispensables son: Recursos organizacionales; Información accionable (es la que puede ser usada sin realizar un procesamiento mayor adicional para comunicar o validar la información debe presentar relevancia, oportunidad, precisión, integridad y digestibilidad que ayuden al CSIRT a la toma de acciones para identificar, prevenir, responder y mitigar incidentes cibernéticos); herramientas para apoyar la propuesta de valor o servicios, los canales y las relaciones con las organizaciones de la comunidad atendida; y recursos humanos.	La propuesta de valor principal que hace un CSIRT a su comunidad atendida es identificar, prevenir, responder y mitigar incidentes cibernéticos. Para ello, el CSIRT ofrecerá una serie de servicios que aportarán valor asistiendo y asesorando a la comunidad atendida en temas de ciberseguridad. Los servicios deberán estar alineados al mandato, misión y visión que se tenga y también ser diseñados de acuerdo con la comunidad atendida.	Se debe contar una historia para explicar y transmitir el modelo de negocio de forma atractiva; esto es, abordando desde la perspectiva de la comunidad atendida, sus problemas y necesidades. La comunidad atendida es la protagonista de la historia. Se debe hablar de los retos que enfrenta y las labores que debe llevar a cabo haciendo énfasis en los aspectos donde el CSIRT será relevante. Posteriormente se debe explicar cómo el CSIRT crea valor para esta comunidad y describir sus servicios, enfatizando en cómo cada servicio responde a una necesidad específica de la comunidad. Como parte de la historia, también debe contarse qué recursos y actividades sostendrá la puesta de valor del CSIRT.

8. CRÉDITOS

Luis Almagro
Secretario General de la Organización de Estados Americanos

Equipo técnico de la OEA
Luis Fernando Lima Oliveira
Alison August Treppel
Kerry-Ann Barrett
Diego Subero
Sofía Hunter
Volker Esteves

Editores
Andrés Velázquez - MaTTica
Laura Jácome - MaTTica

Expertos contribuidores
Angus Smith
Carlos Landeros
Carlos Leonardo
Gabriela Ratti
José Callero
Katherina Canales
Lia Molinari
Roberto Lemaître
Samuel Maroon
Wilson Prieto

Diseño y diagramación
María Paula Lozano

Agradecimientos a

Canada

DEPARTMENT OF STATE
UNITED STATES OF AMERICA

9. ANEXOS

9.1 ANEXO A: Diferencias entre CSIRT, CERT y SOC

CSIRT – Computer Security Incident Response Team

Un CSIRT, de acuerdo con la European Union Agency for Cybersecurity (ENISA),[20] es un nombre genérico que se le da a un equipo que provee un conjunto de servicios tanto preventivos como reactivos que incluyen: compartir información, concientizar, gestión de incidentes cibernéticos (servicios core o principales), monitoreo, gestión de vulnerabilidades y del conocimiento en ciberseguridad. Sin embargo, esta definición puede adecuarse al momento en el que se encuentra el CSIRT, el tamaño y los servicios específicos que va a brindar.

CERT – Computer Emergency Response Team

CSIRT también es definido por el CERT/CC de la Universidad de Carnegie Mellon[21] como una organización de servicios que es responsable de recibir, revisar y responder a los reportes y actividades de incidentes cibernéticos; los servicios que prestan son para un grupo definido de organizaciones: una empresa, gobierno, una región o país o una red de investigadores. CERT es, entonces, una marca registrada desde 1997.

SOC – Security Operations Center

SOC normalmente es un grupo de personas dentro de una organización que cuentan con procesos y tecnología que permite monitorear la seguridad desde una perspectiva técnica. Cuando lo vemos desde la perspectiva de comparación con un CSIRT, un SOC podría ser un servicio que brinda un CSIRT para apoyar a prevenir, detectar y analizar posibles incidentes cibernéticos o para, a partir de la información con la que cuenta, responder a un incidente de ciberseguridad.

9.2 ANEXO B: Consideraciones para la creación de presupuesto

Costos generales
Personal
Salarios
Costos extraoficiales
Programas incentivos
Sistemas de información
Equipamiento (HW)
Licencias
Mantenimiento, soporte y mejora
Comunicaciones
Entrenamientos
Nacionales
Internacionales
Otros entrenamientos
Gastos generales
Gastos de renta
Acondicionamiento y mantenimiento
Muebles y oficina
Insumos generales
Servicios externos
Consultorías, Soporte especializado
Membresías, certificaciones, impuestos
Comunicaciones, promoción y eventos
tercerización de servicios
Otros gastos
Seguros, operativos especiales

[20] CSIRT Capabilities. How to assess maturity? Guidelines for national and governmental CSIRTs. ENISA, 2015. https://www.enisa.europa.eu/publications/csirt-capabilities/@@download/fullReport

[21] CSIRT Frequently Asked Questions - FAQ. Software Engineering Institute. Carnegie Mellon University, 2017. https://resources.sei.cmu.edu/asset_files/WhitePaper/2017_019_001_485654.pdf

EMPIEZA CON

POCO Y CRECE

GUÍA PRÁCTICA PARA CSIRTs

Volumen 2, 2023

Un modelo de negocio sustentable

OEA | Más derechos para más gente

CSIRTAmericas Network